F6

Киберугрозы в России и Беларуси. Аналитика и прогнозы 2025/26

Оглавление

Введение

Валерий Баулин, CEO компании F6

Привет! Перед вами аналитический отчет от команды F6, в котором мы подводим итоги 2025 года и делимся прогнозами на 2026 год.

В 2025 году ландшафт киберугроз в России напоминал плато: впервые за последние три года не наблюдалось взрывного роста кибератак, массового появления новых преступных групп, антирекордов по утечкам данных. Кажется, что атакующие выдохлись или занимались перегруппировкой сил. С массовых атак фокус сместился на нанесение максимального ущерба: остановку бизнеса, получение многомиллионных выкупов, кражу чувствительных данных.

Продолжались коллаборации прогосударственных групп, хактивистов и киберкриминала. Вымогатели заимствовали тактику APT-групп, а прогосударственные группировки приобретали на хакерских форумах **0-day**-эксплойты, инструменты и доступы в инфраструктуру. Все это, несомненно, усложняло исследователям реагирование и атрибуцию.

В отличие от общемирового тренда, когда атакующие стараются без лишнего шума закрепиться в инфраструктуре, чтобы незаметно шпионить за жертвой или готовиться к будущей масштабной диверсии, прошлогодние атаки на российские транспортные компании и торговые сети были очень громкими. Они сопровождались публикацией утечек данных, информационными вбросами и кампаниями по дискредитации пострадавших.

Одним из самых эффективных векторов в 2025 году оставались атаки по модели **Supply chain** (через цепочку поставок) и **Trusted relationship** (через доверительные отношения). Они стали более точечными и разрушительными. В этих условиях компаниям важно следить не только за состоянием собственной инфраструктуры, но и за киберустойчивостью своих подрядчиков и партнеров.

Несмотря на хайп вокруг темы искусственного интеллекта, нейросети в 2025 году, к счастью, пока еще не стали супероружием в руках злодеев. При этом ИИ-инструменты уже сейчас позволяют киберпреступникам автоматизировать и удешевить создание фишингового контента и дипфейков, упростить масштабирование атак, улучшить процессы разведки.

Случаи реального применения ИИ в сложных целевых атаках пока остаются единичными. Однако недавний эксперимент по созданию шифровальщика PromptLock с ИИ-компонентами на борту наглядно продемонстрировал разрушительный потенциал цифрового кибероружия нового поколения. Вероятно, уже в ближайшее время мы можем столкнуться с полностью автономными ИИ-атаками.

Над этим отчетом работали сразу несколько департаментов нашей компании: аналитики киберразведки, эксперты Лаборатории цифровой криминалистики, специалисты Центра кибербезопасности и Департамента защиты от цифровых рисков. Уверен, что подготовленные нашими экспертами тренды, прогнозы и рекомендации станут ценным источником стратегических и тактических данных об актуальных киберугрозах для CISO и руководителей групп кибербезопасности, специалистов по реагированию на инциденты, аналитиков SOC, CERT, Threat Intelligence. Как мы уже неоднократно убеждались, все наши прогнозы имеют обыкновение сбываться.

Ключевые выводы

В 2025 году эксперты F6 фиксировали активность **27** прогосударственных APT-групп, атакующих Россию и СНГ. Для сравнения: в 2024 году были зафиксированы атаки на Россию и СНГ **24** группировок. Из выявленных 27 групп **24** атаковали компании в России, 8 — белорусские организации. Семь новых APT-групп были раскрыты впервые: **Silent Lynx**, **Telemancon**, **Mythic Likho**, **NGC6061**, **NGC4141**, **SkyCloak**, **NGC5081**. Большая часть из них начала проводить атаки в предыдущие годы, но выявлены они были лишь в 2025 году.

Среди топ-5 российских индустрий, которые атаковали APT-группы в 2025 году, оказались госучреждения (их атаковали **13** групп), промышленность (**11** групп), НИИ (**9** групп), предприятия ВПК (**8** групп), ТЭК (**7** групп).

Прогосударственные атакующие использовали в атаках против России **0-day**-эксплойты, вероятно, приобретенные на андеграундных форумах, что довольно уникально для APT-групп.

В 2025 году количество атак программ-вымогателей выросло на **15%** по сравнению с предыдущим годом (в 2024 году рост количества атак составил **44%**). При этом в **15%** подобных инцидентов, связанных со средними и крупными предприятиями, целью киберпреступников был не выкуп, а диверсия — разрушение инфраструктуры и нанесение максимального ущерба жертве (в прошлом году на подобные атаки приходилось **10%**).

Эксперты F6 отмечают рост уровня консолидации проукраинских группировок.

Наиболее активными проукраинскими группами в этом году стали **Bearlyfy/ЛАБУБУ** (не менее 55 атак), **THOR** (не менее 12 атак), **3119/TR4CK** (не менее 4 атак), **Blackjack/Mordor** (не менее 4 атак), **Shadow** (не менее 4 атак).

Чаще всего в 2025 году вымогатели атаковали производственные и инжиниринговые компании (**17,1%**), организации из сфер оптовой (**14,3%**) и розничной торговли (**12,9%**), ИТ (**7,1%**), транспорта и логистики (**7,1%**).

Рекорд по сумме первоначального выкупа в 2025 году поставила группировка **CyberSec's**, потребовавшая **50** BTC (около 500 млн руб. на момент атаки). В среднем суммы первоначального выкупа за расшифровку данных в 2025 году колебались от **4 млн** до **40 млн** руб.

Как мы предсказывали в прошлогоднем отчете, в 2025 году продолжались атаки типов **Supply chain** (через цепочку поставок) и **Trusted relationship** (через доверительные отношения). Например, были выявлены атаки программы-вымогателя на страховые организации через компрометацию подрядной организации, а также замечены атаки, в которой сразу две прогосударственные группы находились в сети ИТ-подрядчика, а одна из них еще и атаковала клиентов.

В 2025 году, помимо групп-вымогателей, была выявлена активность более **20** финансово мотивированных группировок. Наиболее примечательные из них — **Vasy Grek**, **Hive0117**, **CapFIX**.

Возобновились атаки группы **OldGremlin** и атаки с использованием ВПО Buhtrap, как мы предсказывали. Вторые совершили несколько атак на российские компании через сервис электронного документооборота (ЭДО).

Как минимум 4 группы были замечены в 2025 году за проведением DDoS-атак: **CyberSec's**, **Himars DDOS**, **Кіберкорпус**, **IT Army**

of Ukraine. Последняя группировка уделяла основное внимание атакам на российских интернет-провайдеров, при этом не обошла стороной компании из сфер финансов, ИТ и разработки ПО, промышленности, энергетики и транспорта, а также государственные структуры. Проукраинские хактивисты, хотя и стали менее активны в Telegram-каналах, продолжили свои атаки. Они все чаще преследовали не только политические, но и финансовые цели, требуя выкуп за расшифровку данных.

Разные типы атакующих использовали легитимные инструменты и фреймворки в атаках. Так, например, в 2025 году наряду с **CobaltStrike** группа **Silent Lynx** начала применять фреймворк **AdaptixC2**, который появился годом ранее. А другая группа задействовала в атаке криминалистический инструмент **Velociraptor**.

Замечен ренессанс вредоносных программ для ОС Android: это и вариации известных ранее **CraxsRAT** и **NFCGate**, **Mamont** и новые — **LunaSpy**, **Retka**, **Lazarus stealer**, **Gorilla**.

По данным F6, на ВПО **Mamont** приходится **47%** заражений Android-устройств в России.

На протяжении 2025 года эксперты F6 фиксировали многочисленные случаи использования вредоносных версий легитимного Android-приложения NFCGate в атаках на клиентов ведущих российских банков. Общий ущерб клиентов банков от использования всех вредоносных версий **NFCGate** за 10 месяцев 2025 года составил не менее **1,6 млрд** рублей.

В 2025 году было выявлено **230** новых публикаций баз данных российских компаний, еще **10** публикаций баз данных белорусских компаний и **10** публикаций данных компаний из стран СНГ. Суммарное количество записей, попавших в открытый доступ и содержащих данные россиян, составляет **порядка 800 млн.** По Беларуси в открытом доступе оказалось **232 тыс.** записей. Помимо публикации в открытом доступе, злоумышленники используют такие данные для последующего проведения каскадных атак на крупных игроков коммерческого и государственного секторов.

Нередко злоумышленники, активно публикующие данные нескольких компаний, резко прекращают активность (например, их ресурсы блокируются администрацией площадки), но спустя время они возобновляют свою деятельность в новых источниках.

Среди выявленных угроз 2025 года, на которые приходилось реагировать специалистам Центра кибербезопасности компании F6, чаще всего встречались инциденты, связанные с управляемыми человеком атаками, — **32%**. На втором месте — майнеры (**26%**). На третьем месте — инциденты, связанные с использованием троянов удаленного доступа (**9%**).

Фишинговые письма с ВПО злоумышленники чаще всего рассылали по вторникам — на этот день приходится **25,5%** всех отправлений. Меньше всего рассылок в 2025 году было по воскресеньям — **2%**.

В 2025 году на фоне усиления борьбы с мошенничеством наблюдался переход скам-групп от фишинга к скаму. Было заблокировано **7357** скам-ресурсов на один бренд (6398 — в прошлом году) и всего **3851** фишинговый ресурс на один бренд (3714 в прошлом году). На первом месте по количеству как фишинговых, так и мошеннических атак находится ретейл.

Киберпреступники в 2025 году реже использовали доменную зону .ru из-за налаженной работы блокировки доменов в зонах .ru/.рф, чаще делая выбор в сторону других доменных зон и зарубежных регистраторов. Фишинговые и мошеннические ресурсы размещались у хостеров в США в **81%** случаев. У российских хостинг-провайдеров — **4,6%**.

ИИ массово использовался для генерации дипфейков, фишинговых рассылок и ресурсов, для разведки и сбора информации о жертвах. Выявленные случаи использования нейросетей для написания вредоносного кода, скриптов, а также непосредственного участия в атаках в 2025 году носят пока лишь единичный характер.

В 2025 году специалисты F6 наблюдали рост активности, связанной с продажей вредоносного ПО на теневых ресурсах. Наиболее заметными были объявления о продажах троянов удаленного доступа (RAT), а также несколько новых видов ВПО. Среди них Android-ботнет Maradona, а также специализированные инструменты, используемые в качестве NFC-ретранслятора. Кроме того, в андеграунде активно продавались стилеры, например Gremlin Stealer, mac.c Stealer, нацеленный на пользователей macOS-устройств, а также эксплойты уязвимостей нулевого дня для Windows и Android. Несмотря на запрет ведения деятельности по странам СНГ, нередко злоумышленники намеренно меняют функциональность вредоносных программ для проведения атак и в этом регионе.

Прогнозы-2026

Ландшафт киберугроз в России в ближайшие годы будет напрямую зависеть от политической ситуации. В условиях острого геополитического конфликта продолжатся кибератаки как политически мотивированных кибергрупп (хактивистов), так и прогосударственных APT на российские организации. Будет расти как количество групп атакующих, так и ущерб от их деятельности.

Основной целью проукраинских прогосударственных групп по-прежнему останутся предприятия **военно-промышленного комплекса** (ВПК) и **госсектор**, причем сами атаки будут выглядеть достаточно «шумно» с целью заполучить все данные сразу, не пытаясь обеспечить скрытое длительное присутствие.

Усилится тренд на коллаборацию и совместное проведение атак у политически мотивированных группировок. Помимо реальных кибератак, злоумышленники будут **проводить информационные атаки**, заключающиеся в публикации фейковых новостей, рассылках писем с угрозами и др. Причем пик таких атак будет приходиться на дни, когда публикуются громкие новости о взломах.

Будет выявлена активность новых групп из Юго-Восточной Азии, которые месяцами, а в некоторых случаях годами могут скрытно присутствовать в инфраструктурах жертв, как это было, например, в случае с группами **UNC5174** и **GOFFEE**.

Независимо от политической ситуации будет заметна активность таких финансово мотивированных групп, как **Mimic**, **OldGremlin**, **DcHelp**, а также атак с использованием **Buhtrap**. Суммы выкупов, требуемых за расшифровку после атаки программ-вымогателей, будут продолжать расти.

Чтобы осложнить детектирование атак, злоумышленники будут чаще маскироваться под деятельность **Red Team — команд**, используя легитимное ПО и инфраструктуру.

Ожидается увеличение атак с использованием **ИИ** как в части разработки ВПО, так и в части внедрения LLM для его работы в момент заражения.

Ожидается рост числа атак с использованием уязвимостей. Это обусловлено сокращением времени с момента выявления уязвимостей, в том числе критических, до публикации PoC: злоумышленники с разной мотивацией пытаются мгновенно проэксплуатировать уязвимости в непропатченных системах.

Атаки через подрядчиков и доверительные отношения будут актуальны для проведения разных типов атак как с участием программ-вымогателей, так и прогосударственных групп.

Из-за активных блокировок аккаунтов и каналов злоумышленников со стороны администрации социальных сетей и мессенджеров, а также ликвидации правоохранительными органами теневых форумов атакующие попытаются найти новые способы ведения своего криминального бизнеса на альтернативных площадках.

Количество записей, публикуемых злоумышленниками в открытом доступе, будет кратно расти или оставаться на прежнем высоком уровне. Это напрямую связано с геополитической обстановкой: политически мотивированным киберпреступникам выгодно массово распространять персональные данные пользователей из России и Беларуси для дальнейшего использования информации из утечек в мошеннических схемах и для совершения каскадных атак.

Возрастет число атак через профильные публичные системы и сервисы, подобные тем, что были обнаружены в 2025 году, когда через скомпрометированные учетные записи в системе электронного документооборота осуществлялась рассылка ВПО Buhtrap.

В связи с ужесточением законодательства и сложностями с выводом и обналичиванием похищенных средств киберпреступники продолжат усложнять свои схемы для увеличения среднего чека с одной атаки.

Скам-группы, которые проводят атаки на российских пользователей, для хищения денег с их банковских счетов будут чаще использовать реквизиты платежных карт банков СНГ в связи с тем, что использовать для этой цели реквизиты платежных карт российских банков стало сложнее и дороже.

Продолжится тенденция роста количества поддельных сайтов для распространения ВПО.

Ожидается массовое создание новых тематических Telegram-каналов злоумышленников. Несмотря на активные блокировки Telegram-каналов, ведущих публикацию и продажу незаконно полученной информации, такой как скомпрометированные базы данных, киберпреступники продолжают повторно создавать аналогичные ресурсы в этом мессенджере для максимального распространения данных.

Будут появляться новые приемы социальной инженерии и способы заражения устройств с операционной системой Android. Потенциально все больше вредоносных программ будет распространяться по модели MaaS.

Так как предыдущие вредоносные версии NFCGate, обнаруженные первоначально в других странах, использовались в атаках на российских пользователей, специалисты F6 ожидают дальнейшую модификацию RatOn для использования против клиентов российских банков.

В 2026 году основную долю критических инцидентов, с которыми будут сталкиваться команды мониторинга и реагирования, будут составлять человекоуправляемые атаки, способные обходить штатные средства защиты на этапах проникновения и развития. Не стоит сбрасывать со счетов и классические вредоносные программы — стилеры, майнеры, так как количество атак с их использованием продолжает расти.

Векторы атаки через уязвимости нулевого дня и цепочки поставок в 2026 году станут доминирующими.

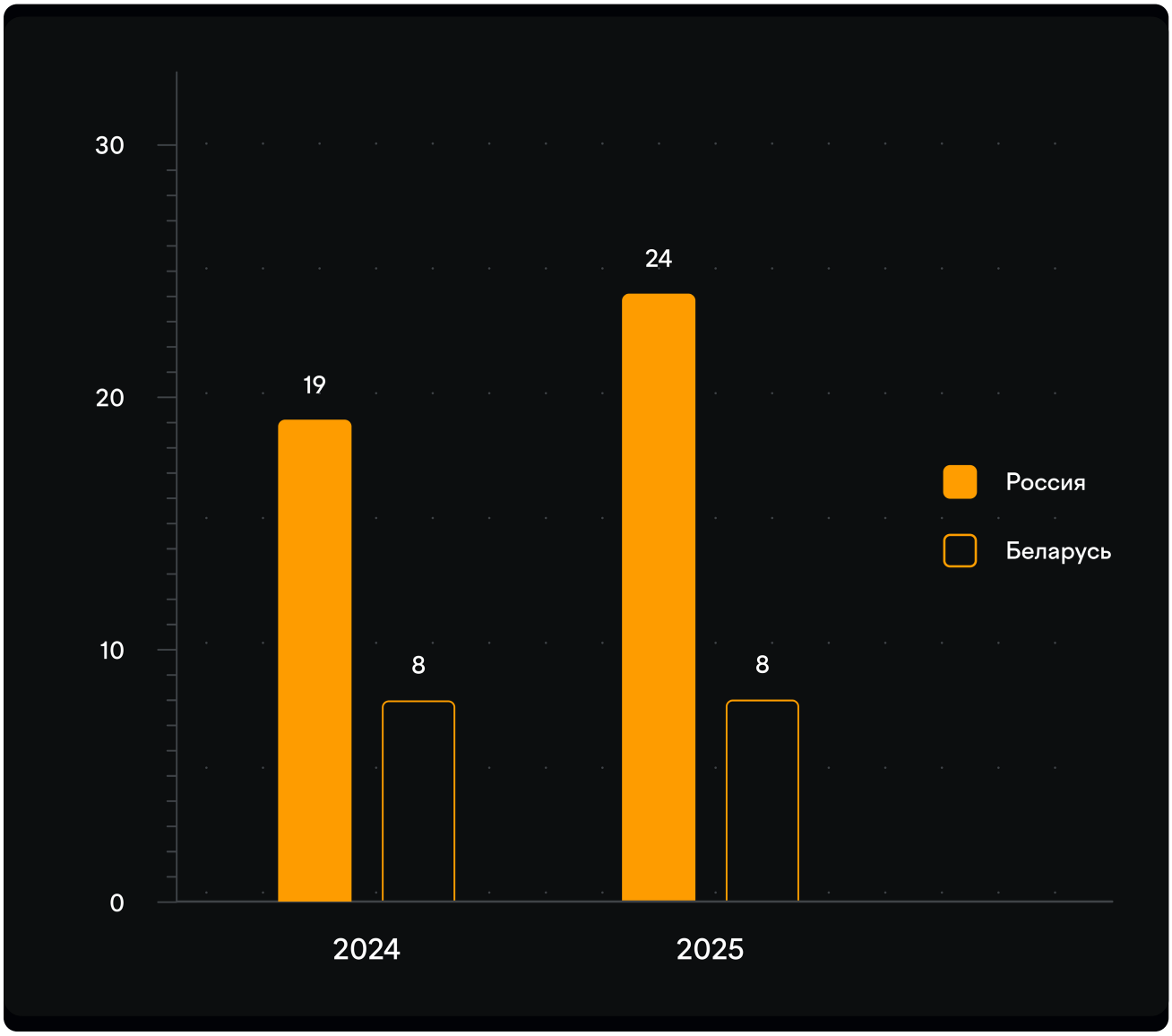
Злоумышленники продолжат активно применять целевой фишинг (Spear Phishing) с использованием искусственного интеллекта, а также компрометацию легитимных учетных записей.

Ожидается рост числа атак через скомпрометированные облачные сервисы, а также использование инструментов удаленного администрирования (AnyDesk, TeamViewer) и встроенных в ОС возможностей (Living-off-the-Land).

Прогосударственные APT-группировки

Если 2024 год был рекордным по количеству различных типов групп, нацеленных на Россию и Беларусь (напомним, что тогда выявлен почти двукратный рост по сравнению с 2023 годом), то в 2025 году мы отмечали выход на некое плато: незначительный рост числа кибератак и исчезновение с радаров некоторых групп.

Специалисты F6 фиксируют следующую статистику активности прогосударственных APT-групп:



В 2025 году были замечены всего **24**прогосударственные APT-группы, нацеленные на Россию. Минимум у **8** из них в целях, помимо российских, были и белорусские организации. В отчетном периоде мы не фиксировали активности 7 групп, которые атаковали Россию годом ранее. Но при этом 7 новых групп были раскрыты впервые: **Silent Lynx**, **Telemancon**, **Mythic Likho**, **NGC6061**, **NGC4141**, **SkyCloak**, **NGC5081**. Большая часть из них начала проводить атаки в 2024 году, однако выявлены они были лишь в 2025 году. Отдельно отметим группу **Silent Lynx**, которая, по нашим данным, действует минимум с 2022 года. Исследователи отмечают пересечения с группой **Tomiris** по целям и инструментам, в связи с чем полагают, что за ними может стоять один атакующий.

Во время исследований нередко появляются детали, позволяющие со временем объединять различные группировки в одну. Так, например, в 2025 году появились доказательства, позволяющие объединить активность двух отслеживаемых ранее по отдельности групп **Dante APT** и **TaxOff** и раскрытую в 2025 году кампанию «**Форумный тролль**».

Помимо объединения группировок, нередки случаи изменения классификации злоумышленников при появлении дополнительных данных об атаках. В частности, две группы из выявленных (**GOFFEE** и **Rezet**) ранее мы относили к категории киберпреступных, но впоследствии, исходя из характера атак, нацеленности и используемых инструментов, стали считать их прогосударственными. Активность группы **GOFFEE**, выявленная в рамках реагирований на инциденты специалистами F6 в 2025 году, позволяет заключить, что группа хорошо оснащена, для нее характерен длительный скрытый доступ к скомпрометированной инфраструктуре, что делает ее особо опасной угрозой для российских организаций.

Еще одной топ-угрозой остается **PhantomCore**. Она продолжает использовать самописное ВПО, разрабатываемое и дорабатываемое на разных языках программирования на регулярной основе. В 2025 году специалистам F6 удалось выявить инфраструктуру группы 2022 года и связанные образцы вредоносного ПО — оказалось, что группа в первых своих атаках использовала вайпер. В прошлом году в атаке группы **Head Mare** для первоначального доступа использовались письма, приводящие к установке инструментов PhantomCore — PhantomDL и PhantomRAT, а в 2025 году специалистами F6 была раскрыта новая группа вымогателей **Bearlyfy**, которая имеет пересечения в инфраструктуре с PhantomCore. Предположительно, группа PhantomCore после получения первоначального доступа и сбора необходимой информации передает доступ или иным образом взаимодействует с другим кибергруппами, нацеленными на шифрование и/или вайп инфраструктуры по политическим мотивам или с целью получения финансовой выгоды.

Полный список APT-групп, чью вредоносную деятельность мы отслеживали на территории России и Беларуси в 2025 году, приведен на стр. 12–14. Для большей наглядности таблица также включает группировки, которые были указаны в ежегодном отчете за 2024 год.

Атаки на Россию со стороны прогосударственных APT-групп в 2024 и 2025 годах

№	APT-группа	Страна источника угрозы	Атаки в 2024 г.	Атаки в 2025 г.
1.	Sticky Werewolf	Украина	⌖	⌖
2.	Cloud Atlas	Украина	⌖	⌖
3.	Core Werewolf	Неизвестно	⌖	⌖
4.	PhantomCore	Украина	⌖	⌖
5.	XDSpy	Неизвестно	⌖	⌖
6.	Dante APT	Неизвестно	⌖	⌖
	TaxOff	Неизвестно	⌖	
7.	ReaverBits	Неизвестно	⌖	⌖
8.	Sapphire Cat	Украина	⌖	⌖
9.	CloudSorcerer	Предположительно, Китай	⌖	⌖
10.	Unicorn	Неизвестно	⌖	⌖
11.	IronHusky	Китай	⌖	⌖
12.	Mysterious Elephant	Индия	⌖	⌖
13.	UNC5221	Китай	⌖	⌖
14.	UNC5174	Предположительно, Китай	⌖	⌖

№	APT-группа	Страна источника угрозы	Атаки в 2024 г.	Атаки в 2025 г.
15.	**Space Pirates**	Китай	Выявлены в 2025 г.	
16.	**Rezet**[1]	Неизвестно		
17.	**GOFFEE**[2]	Украина		
18.	**Telemancon** Обнаружена в 2025 г.	Неизвестно		
19.	**Mythic Likho** Обнаружена в 2025 г.	Неизвестно	Выявлены в 2024 г., атрибутированы в 2025 г.	
20.	**NGC6061** Обнаружена в 2025 г.	Неизвестно	Выявлены в 2025 г.	
21.	**NGC4141** Обнаружена в 2025 г.	Неизвестно	Выявлены в 2025 г.	
22.	**SkyCloak** Обнаружена в 2025 г.	Неизвестно		
23.	**NGC5081** Обнаружена в 2025 г.	Предположительно, Восточная Азия	Выявлены в 2025 г.	
24.	**Silent Lynx** Обнаружена в 2025 г.	Неизвестно	Выявлены в 2025 г.	
	Tomiris Пересечения с Silent Lynx	Казахстан		

1. Группа была переклассифицирована из киберкриминальной в прогосударственную.
2. Группа была переклассифицирована из киберкриминальной в прогосударственную.

№	APT-группа	Страна источника угрозы	Атаки в 2024 г.	Атаки в 2025 г.
25.	**Hellhounds**[3]	? Неизвестно	⊕	⊕
26.	**Mysterious Werewolf**	Украина	⊕	⊕
27.	**Lazy Koala**	? Неизвестно	⊕	⊕
28.	**Obstinate Mogwai**	BA Восточная Азия	⊕	⊕
29.	**APT37**	Северная Корея	⊕	⊕
30.	**Lazarus**	Северная Корея	⊕	⊕
31.	**Midge APT**	? Неизвестно	⊕	⊕

Атаки на Беларусь со стороны прогосударственных APT-групп в 2024 и 2025 годах

№	APT-группа	Страна источника угрозы	Атаки в 2024 г.	Атаки в 2025 г.
1.	**Sticky Werewolf**	Украина	⊕	⊕
2.	**Cloud Atlas**	Украина	⊕	⊕
3.	**Core Werewolf**	? Неизвестно	⊕	⊕
4.	**PhantomCore**	Украина	⊕	⊕
5.	**XDSpy**	? Неизвестно	⊕	⊕

3. В строках 25–31 указаны группы, которые действовали в 2024 году, но не были активны в 2025 году на территории России и Беларуси.

№	APT-группа	Страна источника угрозы	Атаки в 2024 г.	Атаки в 2025 г.
6.	**Dante APT**	? Неизвестно		
7.	**SkyCloak**	? Неизвестно		
8.	**Rezet**	? Неизвестно		
9.	**Lazy Koala**	? Неизвестно		
10.	**Midge APT**	? Неизвестно		

Таблица ниже содержит информацию об отраслях, атакованных прогосударственными группами в 2025 году в России и Беларуси. Нужно учитывать тот факт, что целевых секторов и атакующих группировок на самом деле больше. В отчете рассматривались атаки, которые попали в поле зрения специалистов F6, но не для всей раскрытой вредоносной активности удалось установить целевую организацию. Кроме того, не обо всех целевых атаках становится известно в публичном пространстве. В ряде случаев информация доступна только специалистам, проводившим реагирование на инцидент, а также пострадавшей организации, которая редко открыто освещает факт компрометации.

Атаки на отрасли России и Беларуси в 2025 году, проводимые прогосударственными APT-группами

- **Промышленность**
- **Торговля**
- **Медицина**
- **Туризм**
- **ИТ**
- **Телекоммуникации**
- **Госучреждения**
- **Военная отрасль**
- **Транспорт и логистика**
- **Энергетика**
- **Строительство**
- **Финансы**
- **Образование/НИИ**
- **ЖКХ**

Группировка/отрасль														
Sticky Werewolf	●							●	●	●	●			●
Cloud Atlas	●							●						
Core Werewolf								●	●				●	
PhantomCore	●				●	●				●	●	●	●	●
XDSpy	●						●	●					●	
Dante APT							●					●	●	
ReaverBits	●	●	●											
Sapphire Cat							●			●				
Rezet	●	●	●	●						●	●	●	●	
CloudSorcerer					●		●							
Mysterious Elephant							●							
Unicorn	●	●	●				●	●	●	●	●	●	●	●
Silent Lynx	●	●					●		●	●		●		
NGC6061							●						●	
IronHusky							●							
Telemancon	●	●						●						
GOFFEE	●	●		●	●	●	●	●	●	●	●	●	●	
UNC5174					●		●						●	
Space Pirates							●							
NGC5081					●	●								
NGC4141							●							
SkyCloak								●						
Mythic Likho	●	●				●								

В соответствии с нашей телеметрией, данными, полученными в рамках реагирований на инциденты, а также на основе исследования разного рода ресурсов мы выделяем топ-5 индустрий, на которые нацеливались прогосударственные группы в 2025 году:

Отрасль	Кол-во групп
Госучреждения	**13**
Промышленность	**11**
НИИ	**9**
Военная отрасль (включая оборонно-промышленный комплекс)	**8**
Энергетика	**7**

Направленность атакующих на ОПК распространяется не только на сами промышленные предприятия, занимающиеся производством, но также на НИИ. Это говорит о нацеленности злоумышленников на знания, свежие идеи и разработки, которые еще могли не дойти до фактического производства.

Несмотря на то что ИТ-организации не попали в топ-5, мы продолжаем наблюдать повышенный интерес у злоумышленников к ним. ИТ, да и другие подрядчики, могут использоваться злоумышленниками для масштабирования своих атак на клиентов взломанных подрядчиков.

Помимо уже атрибутированной активности, зафиксировано несколько сложных атак, которые не были приписаны конкретным атакующим. Например, в апреле 2025 года имел место инцидент с проведением сложной целевой атаки у ряда пользователей продуктов ViPNet, реализующих функции организации защищенных VPN-сетей и межсетевого экранирования. Согласно заявлению компании, атака была реализована злоумышленником, обладающим доступом к произвольному узлу ViPNet с правами администратора ОС, глубокими знаниями механизмов построения сетей ViPNet и ключом подписи действующего сертификата пространства доверия внутренней сети организации. Атака направлена на нелегитимное использование транспортного протокола ViPNet сети (MFTP) и имитирует конверты обновления программного обеспечения продуктов ViPNet.

Жертвами стали десятки российских компаний, среди которых — государственные, образовательные, консалтинговые, производственные, розничной торговли и финансовые. Эта атака — свидетельство того, что злоумышленники постоянно совершенствуют и изобретают все более изощренные способы реализации атаки. Также это очередное доказательство того, что атака на ИТ-организации или иные подрядные организации действительно актуальная угроза, для которой характерны значительные последствия для клиентов из разных индустрий.

Интересной особенностью 2025 года стали неоднократные активности, которые исследователи преподносили в публичном пространстве как новые опасные группировки, атакующие СНГ. После анализа оказывалось, что это не что иное, как легитимная Red Team — деятельность.

Так, в сентябре исследователи опубликовали информацию о группе Noisy Bear, якобы атаковавшей казахстанскую нефтяную компанию. На самом же деле, по заявлению компании, это было внутреннее мероприятие по проверке, оценке и повышению уровня осведомленности сотрудников в вопросах ИБ, а не атака. В октябре была опубликована информация о другой кампании, нацеленной на российский автомобильный сектор. Анализ связанной сетевой инфраструктуры позволил специалистам F6 сделать вывод,

что это опять же была не вредоносная кампания, а тестирование на проникновение, проводимое ИБ-компанией.

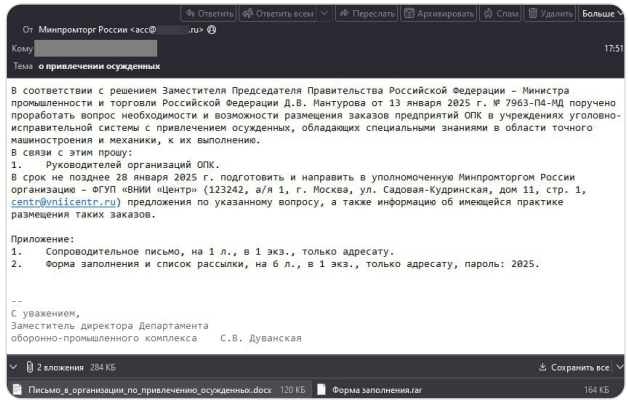
Ниже приводим описание сценариев атак и инструментов активных APT-групп, действующих с целью шпионажа против организаций в России и Беларуси в течение 2025 года.

Обзор активных APT-группировок

Sticky Werewolf	
Псевдонимы	MimiStick, Angry Likho, PhaseShifters
Начало активности	Апрель 2023 г.
Целевые страны	Россия, Беларусь
Целевые индустрии	Энергетика, промышленность, ОПК, строительство, ЖКХ, транспорт
Атакуемые платформы	Windows
Инструменты	Ozone RAT, Quasar RAT, Pulsar RAT, PowerShell Stego downloader
Особенности	• Рассылки с мимикрией под госведомства (Минпромторг России, Минобрнауки России, ФГУП «ВНИИ «Центр», Росгвардия). • Obfuscated Files or Information: Steganography; Forced Authentication
Ресурсы	https://habr.com/ru/companies/F6/news/873762/

С конца 2024-го и вплоть до середины 2025 года группа **Sticky Werewolf** проводила рассылки от имени Минпромторга России. Злоумышленники регистрировали созвучные домены и создавали убедительные приманки для проведения рассылок.

Первая зафиксированная кампания группы в 2025 году была проведена 13 января, среди целей — промышленные предприятия. Пример письма представлен на рис. 1.


Ответить Ответить всем Переслать Архивировать Спам Удалить Больше

От Минпромторг России <acc@ .ru>

Кому 17:51

Тема о привлечении осужденных

В соответствии с решением Заместителя Председателя Правительства Российской Федерации – Министра промышленности и торговли Российской Федерации Д.В. Мантурова от 13 января 2025 г. № 7963-П4-МД поручено проработать вопрос необходимости и возможности размещения заказов предприятий ОПК в учреждениях уголовно-исправительной системы с привлечением осужденных, обладающих специальными знаниями в области точного машиностроения и механики, к их выполнению.
В связи с этим прошу:
1. Руководителей организаций ОПК.
В срок не позднее 28 января 2025 г. подготовить и направить в уполномоченную Минпромторгом России организацию – ФГУП «ВНИИ «Центр» (123242, а/я 1, г. Москва, ул. Садовая-Кудринская, дом 11, стр. 1, centr@vnicentr.ru) предложения по указанному вопросу, а также информацию об имеющейся практике размещения таких заказов.

Приложение:
1. Сопроводительное письмо, на 1 л., в 1 экз., только адресату.
2. Форма заполнения и список рассылки, на 6 л., в 1 экз., только адресату, пароль: 2025.

--
С уважением,
Заместитель директора Департамента
оборонно-промышленного комплекса С.В. Дуванская

2 вложения 284 КБ Сохранить все

Письмо_в_организации_по_привлечению_осужденных.docx 120 КБ Форма заполнения.rar 164 КБ

Рис. 1 — Пример письма группы Sticky Werewolf

Письмо содержит защищенный паролем архив, внутри которого приманка и исполняемый файл — установщик NSIS. Установщик закрепляет в системе дроппер, задача которого — запустить VBS-скрипт, который, в свою очередь, выполнит команду, приводящую к загрузке PowerShell Stego downloader. Последний загружает по ссылке картинку, в которой содержится закодированная третья стадия, представляющая собой загрузчик-инжектор. Эта стадия загружает с удаленного узла финальную нагрузку в виде **Ozone RAT** и запускает ее в контексте процесса `RegAsm.exe`.

В марте злоумышленники вернулись к привычной цепочке атаки, к которой они прибегают в большинстве случаев: архив → дроппер-установщик NSIS → BAT → AutoIt script → запуск Quasar в контексте процесса `RegAsm.exe`. Стоит отметить, что домен, выступающий в роли управляющего сервера, мы выявили в декабре 2024 года и прогнозировали, что группа начнет его использовать в ближайшее время.

Sticky Werewolf имеет характерный и узнаваемый формат приманок. Например, содержимое приманки из мартовской атаки представлено на рис. 2.

Руководителям предприятий
(по списку)

МИНИСТЕРСТВО
ПРОМЫШЛЕННОСТИ
И ТОРГОВЛИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНПРОМТОРГ РОССИИ)

ЗАМЕСТИТЕЛЬ МИНИСТРА

Пресненская наб., д. 10, стр. 2, г. Москва, 125039

«_17_» __03___ 2025_ г. №1734651/25
На № _____ от _____

Уважаемый генеральный директор!

С целью разработки стратегии государственного субсидирования оборонных предприятий на 2025 год просим вас **в ответ на данное электронное письмо в срок до 21.03.2025** года предоставить информацию касательно наличия и размера долговой нагрузки на предприятие.

С уважением,

С. Цыб

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат 34BCA4A80E5F91D2090940A4177B05CB
Владелец Цыб Сергей Анатольевич
Действителен с 20.02.2025 по 20.03.2025

Рис. 2 — Пример документа-приманки группы Sticky Werewolf из мартовской атаки

В ряде случаев нам удавалось провести предварительную атрибуцию по содержимому приманки. Так, например, получилось с ноябрьской атакой, в ходе которой злоумышленники впервые использовали ВПО Pulsar RAT. Можно заметить, что сертификат электронной подписи (ЭП, выделено красным на рис. 3) в приманке из атаки от 04.11.2025 идентичен используемому в мартовской приманке (рис. 2), причем по легенде ЭП принадлежит другому пользователю.

Начальник Главного управления государственного контроля
и лицензионно-разрешительной работы Росгвардии А.А. Маликов

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат 34BCA4A80E5F91D2090940A4177B05CB
Владелец Маликов Анатолий Анатольевич
Действителен с 29.08.2025 по 02.12.2025

Рис. 3 — Фрагмент документа-приманки группы Sticky Werewolf из атаки от 04.11.2025

В мае группа стала рассылать **Quasar RAT** от лица Минобрнауки России, позднее — от имени ФГУП «ВНИИ «Центр».

Помимо типовой цепочки атаки, группа была неоднократно замечена за рассылкой специально подготовленных вложений, позволяющих реализовать сбор NTLM-хешей с зараженных устройств. Таким образом, **Sticky Werewolf** проводит разведку, собирая аутентификационные данные, которые может использовать для развития атаки.

В ноябре группа значительно изменила цепочку атаки — стала использовать технику DLL side-loading и применила **ВПО PulsarRAT**. Причем рассылка впервые проводилась от имени Росгвардии.

Cloud Atlas	
Псевдонимы	Cloud Werewolf, Inception, Blue Odin, Clean Ursa, Oxygen
Начало активности	2014 г.
Целевые страны	Россия, Беларусь
Целевые индустрии	ОПК, промышленность
Атакуемые платформы	Windows
Инструменты	CVE-2017-11882, VBShower Launcher, VBShower Cleaner, VBShower backdoor, PowerShower
Особенности	• Использование одних и тех же уязвимостей и ВПО. • Типовые доменные зоны. • Очистка следов с помощью VBShower Cleaner
Ресурсы	https://www.f6.ru/blog/cloud-atlas-field-trials/

Ранее мы отмечали, что группа Cloud Atlas — одна из самых стабильных. Она давно существует, использует старые уязвимости и одни и те же самописные инструменты на протяжении долгого времени, также придерживается определенного шаблона при регистрации доменов. Однако периодически группа отходит от привычных методов и пытается добавлять нововведения.

Мы продолжаем детектировать активность группы Cloud Atlas, выявляя различные образцы ВПО и инфраструктуру. Злоумышленники предпринимают действия, чтобы минимизировать вероятность анализа их вредоносной деятельности исследователями.

В 2025 году было выявлено и пресечено несколько атак, нацеленных главным образом на промышленный сектор. Так, 31 июля группа использовала привычную цепочку атаки, начинающуюся с рассылки фишингового письма (рис. 4).

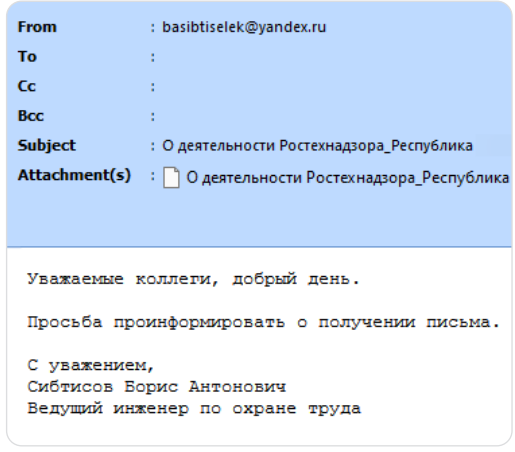


Рис. 4 — Пример письма группы Cloud Atlas от 31.07.2025

Вложенный архив содержал в себе файл «О деятельности Ростехнадзора_Республика Татарстан.doc», замаскированный под информирование об осуществлении надзорной деятельности на поднадзорных промышленных объектах. Злоумышленники эксплуатируют

уязвимость CVE-2017-11882, что приводит к последующей загрузке и запуску HTA-дроппера. Дроппер создает несколько файлов: VBShower Launcher, VBShower Cleaner, VBShower backdoor. Затем в автозапуск добавляется VBShower Launcher, который скачивает с сервера PowerShower, основная задача которого — разведка и сбор информации для проведения дальнейшей атаки. VBShower Cleaner используется для очистки содержимого всех файлов из папки `\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\` путем открытия файлов на запись. Сами файлы при этом остаются, но их содержимое стирается. Таким образом VBShower Cleaner избавляется от следов вредоносных документов и шаблонов, загруженных из сети в процессе атаки.

В октябре во время исследования атаки на агропромышленную организацию специалисты F6 обнаружили изменения в арсенале группы Cloud Atlas. Особенностью выявленных атак стало изменение доменных зон: впервые группа зарегистрировала нетипичные для нее домены в зонах `.live` и `.fr`, а также внесла незначительные изменения в ВПО. В частности, использовала дроппер `*.txt` с полезной нагрузкой VBShower. Кроме того, в нескольких более ранних атаках в 2025-м и конце 2024 года группа применяла в атаке `.lnk`-файлы.

Core Werewolf	
Псевдонимы	PseudoGamaredon, Awaken Likho, GamaCopy
Начало активности	2021 г.
Целевые страны	Россия, Беларусь
Целевые индустрии	Военная отрасль, госучреждения, НИИ
Атакуемые платформы	Windows
Инструменты	UltraVNC
Особенности	• Содержимое файлов-приманок (военная тема, документы ДСП). • Цепочка атаки, состоящая преимущественно из командных скриптов, приводящих к загрузке UltraVNC
Ресурсы	https://t.me/f6_cybersecurity/3645

В 2025 году группа Core Werewolf проводила серию кампаний по распространению писем с вредоносным вложением. Темы и приманки имитировали официальную корреспонденцию, мобилизационно-учетную документацию, наградные документы и прочие документы для служебного пользования. Злоумышленники продолжают использовать исполняемые файлы в архивах, которые после запуска инициируют цепочку выполнения командных

файлов. Несмотря на то что группа периодически обновляет промежуточные стадии, в качестве финальной нагрузки на протяжении всего года мы наблюдали использование **UltraVNC**.

29 апреля группа провела атаку на белорусское государственное учреждение. В ходе атаки злоумышленники рассылали защищенный паролем архив под видом списков на награждение.

В октябре в публичную песочницу была загружена ссылка, при переходе по которой осуществляется загрузка файла «Указания начальникам ВП об организации работы по .exe». В ходе выполнения файла на устройство сбрасывается и открывается декой. После осуществляется запуск командного файла. Затем происходит распаковка содержимого защищенного паролем архива и запуск распакованного командного файла. Последний сбрасывает конфигурационный файл и запускает еще один командный файл, содержащий команду для закрепления в системе через планировщика и запуска нагрузки в виде UltraVNC.

Еще одна версия дроппера была выявлена в ноябре, он содержал зашифрованный конфигурационный блок и защищенный паролем 7z-архив. Внутри архива — конфигурация UltraVNC, плагин для шифрования трафика, исполняемый файл UltraVNC, отвлекающая видеозапись и Batch-скрипт для их запуска. Отметим, что видеозаписи в качестве приманки редко можно видеть в арсенале группировок.

XDSpy	
Псевдонимы	Silent Werewolf, Dwarf Werewolf
Начало активности	2011 г.
Целевые страны	Россия, Беларусь, Молдова
Целевые индустрии	Госучреждения, ОПК, промышленность, НИИ
Атакуемые платформы	Windows
Инструменты	ETDownloader, Batavia, XDSpy.NSISDownloader, XDSpy.GoBackdoor
Особенности	• Письма со ссылками на вредоносные архивы. • Специфичные имена регистрируемой инфраструктуры — домены написаны транслитерацией русских словосочетаний. • Самописное ВПО. • Проверки на запуск в виртуальном окружении, если не пройдена — редирект на заглушку вместо скачивания нагрузки

В 2025 году группа XDSpy неоднократно проводила кампании, нацеленные преимущественно на российские государственные учреждения, НИИ, промышленность и ОПК.

Помимо уже характерного для группы ВПО в виде **XDSpy.GoBackdoor**, **XDSpy.NSIS Downloader**, в ходе атак в 2025 году также использовались и новые инструменты и обновленные цепочки атак.

С помощью спуфинга группа рассылала письма под видом досудебных претензий, документов, планируемых проектов, содержащие вредоносную ссылку на загрузку архива. В ряде случаев ссылка сопровождалась изображением якобы вложенного архива. Пример письма из сентябрьской рассылки представлен на рис. 5.

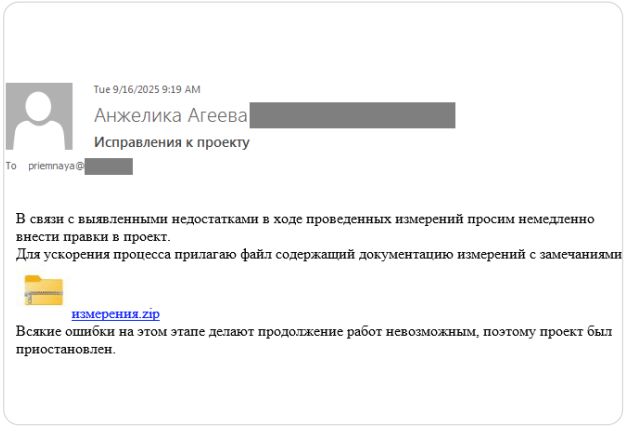


Рис. 5 — Пример письма группы XDSpy от 16.09.2025

Загружаемый по ссылке архив содержит архив с поддельным расширением (`.ini`, `.su` и др.) и `.lnk`-файл, который отвечает за запуск внедренного в него JScript.NET-кода. В свою очередь, вложенный архив содержит приманку, легитимный исполняемый файл и вредоносную библиотеку d3d9.dll, которая загружается с помощью техники DLL side-loading и классифицируется как ETDownloader. После установки загрузчик выполняет HTTPS-запрос на определенный адрес и ожидает ответ в виде зашифрованного исполняемого файла-нагрузки.

Стоит отметить, что группа реализует проверку целевой системы, чтобы избежать запуска в виртуальной среде. Так, например, если целевой хост не проходит проверку, то пользователь перенаправляется на страницу-заглушку. В ряде атак была реализована загрузка LLM-модели Llama 2. Такой подход затрудняет исследование всей атаки, в том числе позволяет атакующим обходить средства защиты. В случае успешного прохождения проверки скачивается полезная нагрузка.

С июля 2024 года и на протяжении 2025-го группа проводила кампанию против промышленных предприятий, в ходе которой распространяла ранее неизвестный бэкдор **Batavia**. Основное назначение ВПО — кража файлов с зараженного компьютера и сбор информации о нем. Также бэкдор поддерживает возможность смены командного центра, загрузки и запуска дополнительных файлов, что делает его универсальным инструментом.

Silent Lynx	
Псевдонимы	• Cavalry Werewolf, ShadowSilk. • На основании пересечений объединяют с группой Tomiris, (известна как YoroTrooper, SturgeonPhisher, Trooper Werewolf, COMRADE SAIGA)
Начало активности	2022 г.
Целевые страны	Россия, Киргизия, Туркменистан, Узбекистан, Таджикистан, Мьянма, Пакистан
Целевые индустрии	Госучреждения, финансы, энергетика, торговля, промышленность, транспорт
Атакуемые платформы	Windows
Инструменты	CVE-2018-7600, CVE-2018-7602, CVE-2024-27956, прокси-утилиты, sqlmap, WPSwpscan, FOFA, Shodan, fscan, Ggobuster, dirsearch, Metasploit, Cobalt Strike, панели JRAT и MORF Project, StallionRAT, FoalShell, ReverseSocks5, AdaptixC2, Havoc, AsyncRAT, программа для кражи криптовалюты, Tomiris Rust Downloader, Tomiris Python Discord ReverseShell, Tomiris Python FileGrabber, Tomiris Python Distopia Backdoor, Tomiris Python Telegram ReverseShell, Tomiris C# Telegram ReverseShell, Tomiris Rust ReverseShell
Особенности	• Скомпрометированные адреса электронной почты для рассылок, легитимные или скомпрометированные ресурсы для хостинга ВПО. • Использование Telegram-ботов в качестве C2. • Активно используют ПО с открытым исходным кодом, коммерческие инструменты, различные реверс-шеллы, разнообразие языков программирования

В 2025 году исследователи раскрыли кибершпионскую группу, присвоив ей имя **Silent Lynx**. Было выявлено две рассылки: в декабре 2024 года и начале января 2025-го. Они были нацелены на организации, связанные с финансами, в Киргизии и Туркменистане. Письма рассылались со скомпрометированной почты. Злоумышленник использовал Telegram-бот для выполнения команд и отправки результата, а также для загрузки файла из системы

жертвы в Telegram. Также злоумышленники использовали Google Drive для загрузки дополнительных полезных нагрузок, передавая команду на загрузку через Telegram-бот. В июне 2025 года была выявлена новая активность группы и жертвы среди правительственных структур в Центральной Азии.

30 июня была обнаружена рассылка в адрес российского государственного учреждения. Содержимое письма представлено на рис. 6.

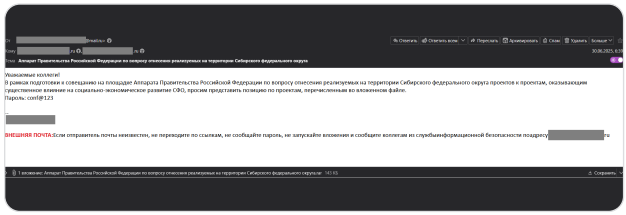


Рис. 6 — Пример письма группы Silent Lynx от 30.06.2025

Файл во вложенном архиве представляет собой бэкдор, основанный на реверс-шелле с открытым исходным кодом **Reverse-Shell-CS**. С его помощью злоумышленники загружали стилер для поиска и эксфильтрации файлов определенных расширений, а также инструмент **ReverseSocks5**. В арсенале атакующих было выявлено множество инструментов: `.bat`-скрипты, бэкдоры на C++, бэкдоры, управляемые через Telegram-бот, **FoalShell** — набор реверс-шеллов, написанных на языках Go, C++, C#. Также были обнаружены троянизированные версии легитимных программ, в которые злоумышленники внедрили вредоносный код. Атакующие создавали вредоносные модификации архиваторов, средств разработки **Visual Studio Code** и др. Такие модификации вместо основного назначения при запуске инициализируют добавленную к ним троянскую часть. Обнаруженная полезная нагрузка, распространяемая через такие «легитимные» программы, — **ReverseSocks5**, **AdaptixC2**, **Havoc**, **CobaltStrike**, **AsyncRAT**, программа для кражи криптовалюты.

Во второй половине 2025 года группа проводила кампанию, нацеленную на российские организации. Например, в одном из писем рассылали архив, внутри которого размещен исполняемый файл с множеством пробелов перед расширением для маскировки. Этот исполняемый файл — написанный на Go реверс-шелл, предоставляющий операторам доступ к выполнению команд. Пример письма, направленного в адрес государственной корпорации, представлен на рис. 7.

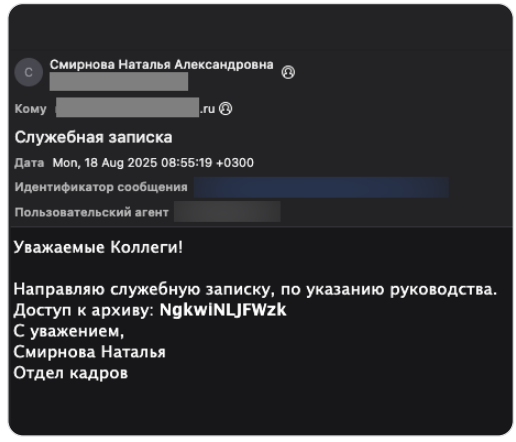


Рис. 7 — Пример письма группы Silent Lynx от 18.08.2025

Если в процессе атаки злоумышленник понимает, что ВПО запущено в виртуальной среде, то он удаляет загруженный файл и следы закрепления (добавленный ранее ключ реестра). В случае с письмом выше злоумышленники подгружали AdaptixC2.

В ряде других летних атак, в которых атакующие рассылали письма по российским организациям от имени сотрудников различных министерств Киргизии, в качестве нагрузок устанавливались FoalShell и троян удаленного доступа **StallionRAT**. Дополнительный анализ показал, что злоумышленники подгружают инструменты не только из своей инфраструктуры, но и со скомпрометированных ресурсов.

Судя по датам создания Telegram-ботов, используемых в качестве C2, группа Silent Lynx активна минимум с 2022 года. Иссле-

дователи отмечают сходства с группой **Tomiris** на основе пересекающихся целей и инструментов, поэтому объединяют эти две группы в одну. Группа Tomiris активна с 2020 года и, согласно ряду источников, действует в интересах Казахстана. Недавно было опубликовано исследование об инструментах, использовавшихся в атаках на государственные и межправительственные организации с начала 2025 года. Группировка опирается на самописные импланты, реализованные на Go, Rust, C/C++/C# и Python. Эти импланты в основном обеспечивают функциональность реверс-шеллов, в роли C2 используются Telegram и Discord, дополнительно задействуются публично доступные инструменты с открытым исходным кодом. Исследователями были получены сведения о следующих новых используемых инструментах группировки:

- **Tomiris Rust Downloader** — для сбора базовой информации о системе, отправки ее на Discord-канал злоумышленника и загрузки последующих инструментов.
- **Tomiris Python Discord ReverseShell** — выполняет команды, полученные через Discord, используется для разведки и загрузки AdaptixC2 и Tomiris Python FileGrabber.
- **Tomiris Python FileGrabber** — собирает в архив файлы с определенными расширениями.
- **Tomiris Python Distopia Backdoor** — основан на проекте dystopia-c2 с GitHub, позволяет выполнять консольные команды, загружать и выгружать файлы, завершать процессы, коммуникация через Discord.
- **Tomiris Python Telegram ReverseShell / Tomiris C# Telegram ReverseShell** — реверс-шеллы, написанные на Python и C#, соответственно, принимают команды через Telegram.
- **Tomiris Rust ReverseShell** — простой реверс-шелл, написанный на Rust и использующий командную оболочку PowerShell.

Вместе с тем в исследовании были упомянуты инструменты и связанные индикаторы, которые ранее уже публично были раскрыты как используемые группой Silent Lynx: Tomiris C/C++ ReverseShell (a.k.a FoalShell), Tomiris Go ReverseShell (a.k.a FoalShell) и Tomiris C# ReverseShell (a.k.a FoalShell), JLORAT, Tomiris PowerShell Telegram Backdoor (a.k.a. StallionRAT), Tomiris C++/Go ReverseSocks (a.k.a. BackDoor.Tunnel.41).

В большинстве случаев заражение начиналось с развертывания реверс-шеллов. На более поздних этапах жизненного цикла атаки операторы использовали фреймворки Havoc и AdaptixC2.

Dante APT	
Псевдонимы	Team46, TaxOff, Prosperous Werewolf, Insidious Werewolf, forumtroll, Форумный тролль
Начало активности	2022 г.
Целевые страны	Россия, Беларусь
Целевые индустрии	СМИ, образование/НИИ, госучреждения, финансы
Атакуемые платформы	Windows
Инструменты	CVE-2025-2783, Trinper, Dante, Tuoni
Особенности	• Коммерческое ПО компании Memento Labs. • Эксплуатация уязвимостей, в том числе нулевого дня. • Хостинг C2 в облачной инфраструктуре Fastly.net

В 2025 году специалисты в ходе реагирования на инцидент установили, что за группами **Dante** (**Team46**), **TaxOff** и **forumtroll** стоит один и тот же злоумышленник, поскольку группы использовали похожие PowerShell-команды, скрипты и паттерны URL в них, схожие по функциональным возможностям инструменты, синтаксически похожие домены с мимикрией под легитимные сервисы с дефисами в названии. Годом ранее связей между группами не было установлено, поэтому они отслеживались как две разных.

В середине марта 2025 года была обнаружена кампания «Форумный тролль». Злоумышленники использовали one-click-эксплойт уязвимости нулевого дня CVE-2025-2783 и загружали в качестве финальной нагрузки бэкдор **Trinper** (другое название — **LeetAgent**). Вредоносные письма содержали приглашения от лица организаторов научно-экспертного форума «Примаковские чтения» и были нацелены на СМИ, государственные, образовательные и финансовые учреждения в России. Заражение происходило сразу после того, как жертва открывала персональную ссылку из фишингового письма в браузере Google Chrome. Устанавливаемое на машину жертвы ВПО Trinper использует протокол HTTPs для получения и выполнения команд от сервера, в фоновом режиме выполняет задачи по отслеживанию нажатий клавиш и краже файлов.

Злоумышленники также загружали на устройство жертвы дополнительные инструменты: **7z**, **Rclone**, **SharpChrome** и коммерческое шпионское ПО **Dante**, разработанное компанией Memento Labs (ранее Hacking Team). Исследователи выделили два кластера атак с 2022 года: один с использованием Trinper, другой — с более сложным набором шпионских инструментов, который впоследствии идентифицировали как Dante. Представители Memento Labs подтвердили принадлежность обнаружен-

ного ПО Dante компании и заявили, что инциденты связаны с использованием устаревшего агента одним из государственных клиентов.

В последнем квартале 2025 года была выявлена кампания группы, направленная на ученых в области политологии из крупных российских НИИ. Рассылка велась якобы от имени научной электронной библиотеки eLibrary. Письма содержали вредоносную ссылку, по которой скачивается архив под видом отчета о проверке на плагиат. Атакующие использовали персонализированные имена архивов и ограничили его повторную загрузку. В качестве финальной нагрузки группа устанавливала коммерческий фреймворк для редтиминга Tuoni. Используя этот инструмент, злоумышленники получали удаленный доступ к устройству жертвы.

ReaverBits	
Псевдонимы	Lucky Werewolf
Начало активности	2023 г.
Целевые страны	Россия
Целевые индустрии	Торговля, промышленность, медицина
Атакуемые платформы	Windows
Инструменты	ReaverDoor, Meduza Stealer
Публикации F6	https://www.f6.ru/blog/reaverbits-new-instruments-2/

В начале года специалисты F6 обнаружили новый бэкдор в виде PHP-скрипта в арсенале группы **ReaverBits** и присвоили ему название **ReaverDoor**.

Спустя несколько дней группа провела фишинговую рассылку от имени Министерства внутренних дел Российской Федерации с темой «СК РФ Вызов на допрос», в ходе которой попыталась распространять ВПО **Meduza Stealer**.

Письмо содержит указание на необходимость перехода по ссылке для скачивания документа. Когда жертва переходила по указанной ссылке, сервер проверял язык, установленный в браузере. В случае использования русского языка жертва перенаправлялась на скомпрометированный домен, с которого на устройство загружался файл с именем «Повестка». В случае использования жертвой иного языка происходило перенаправление пользователя на официальный ресурс ведомства. Загружаемый файл представляет собой `.NET`-загрузчик, основанный на ПО с открытым исходным кодом NBTExplorer. Основное его назначение — загрузка PHP-скрипта ReaverDoor, который, в свою очередь, выполнит расшифровку полезной нагрузки и ее внедрение в память запущенного процесса `RegAsm.exe`. В качестве нагрузки используется Meduza Stealer, однако выявленный образец отличался

от более ранней версии группы следующими признаками: добавлен UAC bypass, функция самоуничтожения, конфигурация хранится в файле в зашифрованном виде. Стоит отметить, что в обнаруженном образце была реализована проверка языка системы и предусмотрено завершение работы, если он принадлежит одной из стран СНГ. Это говорит об ошибке со стороны злоумышленников при организации атаки и невозможности запуска этой нагрузки на устройствах в СНГ, а в частности в России.

Sapphire Cat	
Псевдонимы	Sapphire Werewolf, FunnyCat
Начало активности	2024 г.
Целевые страны	Россия
Целевые индустрии	Энергетика, госучреждения
Атакуемые платформы	Windows
Инструменты	FunnyCat.Stealer
Особенности	• Использование Telegram-бота и Ngrok в качестве C2. • Особый интерес к аутентификационным данным

В 2025 году группа **Sapphire Cat** распространяла вредоносные архивы под видом служебных записок и постановлений о возбуждении исполнительного производства. Среди целей была сфера энергетики.

Выявленные семплы представляют собой обновленную версию **FunnyCat.Stealer**, который злоумышленники используют с момента первых атак. В новой версии добавлена проверка на факт запуска в виртуальной среде, а также используется алгоритм Triple DES для шифрования строк. После запуска стилер отправляет информацию о системе, включающую IP-адрес и строку, является ли машина виртуальной или нет, на сервис canarytokens. Стилер собирает аутентификационные данные из браузеров, Telegram, конфигурационных файлов, документы с рабочего стола, из Telegram и внешних носителей. Собранные данные упаковываются в архив и выгружаются на C2. В качестве C2 используются **Telegram** и **Ngrok**, причем адрес **Ngrok**-сервера в обнаруженных случаях был получен из Telegram.

Unicorn	
Псевдонимы	Fairy Wolf, TA Tolik, Tolik
Начало активности	2024 г.
Целевые страны	Россия
Целевые индустрии	Строительство, медицина, торговля, финансы, транспорт, промышленность, энергетика, ЖКХ, НИИ, госучреждения, ОПК
Атакуемые платформы	Windows
Инструменты	Unicorn
Особенности	• Долгое использование одних и тех же доменов в качестве C2. • Одна цепочка атаки с минимальными изменениями: архив → HTA → .VBS-скрипт → VBS-скрипты с подгрузкой модулей из реестра = стилер Unicorn
Публикации F6	https://t.me/f6_cybersecurity/3921

2025 год показал, что группа **Unicorn** придерживается того же подхода в атаках, с чего и начинала в 2024-м: типовые рассылки, килчейн и нагрузка в виде одноименного стилера. Частота рассылок и периодами недостаточная избирательность в целевых индустриях могут охарактеризовать ее как киберкриминальную группу. Однако, исходя из ее первоначальной нацеленности на промышленность и государственные учреждения, формата рассылаемых писем (рис. 8), а также собираемой стилером информации, мы в настоящий момент относим ее к прогосударственным, которая может действовать с целью шпионажа.

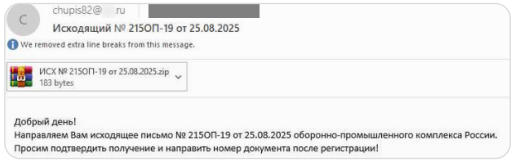


Рис. 8 — Пример письма группы Unicorn

Цепочка атаки не претерпела за год значительных изменений и состояла из следующих звеньев: архив → HTA → .VBS-скрипт → VBS-скрипты с подгрузкой модулей из реестра, образующих стилер **Unicorn**. Стилер представляет собой множество VBS-скриптов, каждый из которых отвечает за свою задачу — кражу файлов, данных браузера и Telegram, файлов со съемных носителей, и отдельный скрипт для эксфильтрации собранной информации.

В 2024 году во время исследования активности группы специалисты F6 выявили пересечения в регистрационных данных доменов злоумышленников и написали правила хантинга. Это позволило обнаружить вредоносные домены в момент их регистрации, то есть еще до начала фактического использования злоумышленниками. Спустя почти полгода, в апреле 2025-го, группа использовала эти же данные для регистрации домена,

который спустя несколько дней уже начал применяться в качестве C2. Стоит отметить, что домен использовался очень долго, вплоть до августа 2025 года. Основным изменением группы за год можно назвать октябрьское дополнение стилера возможностями трояна удаленного доступа: теперь он имеет возможность выполнения команд, получаемых от сервера.

Rezet	
Псевдонимы	Rare Wolf, Rare Werewolf, TA-927, Librarian Ghouls, Librarian Likho
Начало активности	2018 г.
Целевые страны	Россия, Беларусь, Казахстан
Целевые индустрии	Промышленность, строительство, НИИ, медицина, финансы, торговля, туризм
Атакуемые платформы	Windows
Инструменты	Mipko Employee Monitor, AnyDesk, 4t Tray Minimizer, WebBrowserPassView, Ngrok, NirCmd, blat.exe, Email Password-Recovery, Rezet.SharpGrabber, Rhadamanthys Stealer
Особенности	• Использование легитимного ПО. • Передача собранной информации через утилиту `blat.exe` (T1071.003). • Начало разработки самописного ВПО с помощью ИИ
Публикации F6	https://habr.com/ru/companies/F6/news/878320/

Группа **Rezet** характеризуется высокой активностью. Ранее мы относили ее к киберпреступной группе, однако текущая нацеленность и характер атак позволяют предположить, что основной ее мотив — шпионаж.

В 2025 году было выявлено много рассылок группы. Большая часть из них была замаскирована под коммерческие предложения, платежные поручения, договоры, выписки и другие документы. Группа начала год с рассылок от имени компании, которая специализируется на стандартизации оборонной продукции (рис. 9). Объектами атаки стали промышленные предприятия.

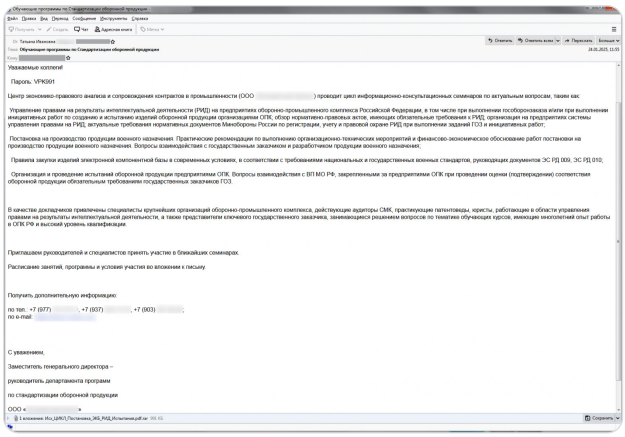


Рис. 9 — Пример письма группы Rezet

Конечной полезной нагрузкой атак обычно становятся **Mipko Employee Monitor** или **AnyDesk** — программы, которые позволяют злоумышленникам дистанционно контролировать устройства жертв, записывать с экрана и перехватывать нажатия клавиш. Rezet использует легитимную утилиту blat.exe для отправки атакующим электронных писем, содержащих собранные в процессе работы данные.

Осенью было замечено изменение цепочек атак группы Rezet. С сентября группа проводила кампанию, направленную на российские организации из сфер авиа- и радиопромышленности, в ходе которой впервые стала использовать ВПО собственной разработки **Rezet.SharpGrabber.** ВПО рекурсивно ищет файлы с расширениями .txt, .doc, .docx, .pdf, .xls и .xlsx на локальных и внешних дисках системы. Найденные файлы копируются в соответствующие каталоги с сохранением оригинальных имен, затем архивируются, разбиваются по 20 МБ и отправляются на C2 через SMTP. Исходя из особенностей оформления кода, специфического шаблона вывода отладочных сообщений и их количества, можно предположить, что разработчик для написания ВПО использовал ИИ.

В начале ноября системой F6 MXDR заблокированы рассылки в адрес организаций из сфер НИИ и развлечений. Письма содержали защищенный паролем архив. Архив содержит файл с расширением .com. Ранее группа не использовала такие файлы в ходе атак.

Позднее группа рассылала под видом коммерческого предложения в промышленные организации RAR-архив (рис. 10).

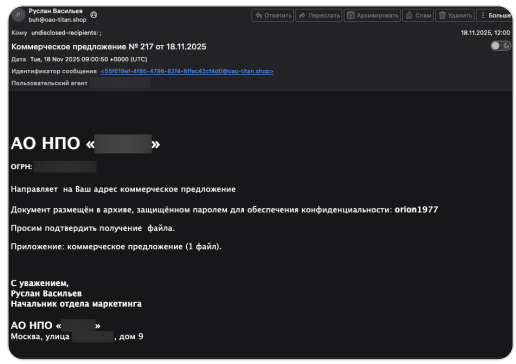


Рис. 10 — Пример письма группы Rezet

Вложение содержит исполняемый файл-дроппер. Он запускает приманку, исполняемый файл легитимного архиватора RAR и PowerShell-скрипт. Особенности оформления кода, его структура и детальность логирования позволяют предположить, что скрипт был написан при помощи ИИ (рис. 11).

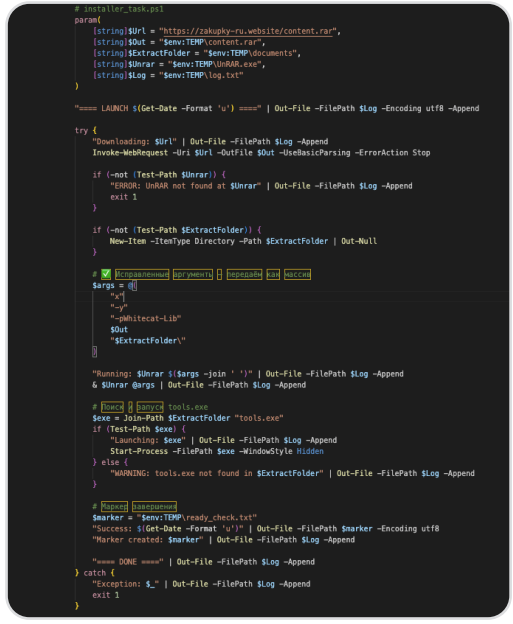


Рис. 11 — Фрагмент кода PowerShell-скрипта группы Rezet

Скрипт выполняет роль загрузчика: загружает с определенного адреса архив, распаковывает его и запускает содержимое, представляющее собой исполняемый файл `Rezet.SharpGrabber`.

Telemancon	
Псевдонимы	Herald Werewolf
Начало активности	2023 г.
Целевые страны	Россия
Целевые индустрии	Промышленность, ОПК
Атакуемые платформы	Windows
Инструменты	TMCDropper, TMCShell
Особенности	Получение адреса C2 из заметки telegra.ph
Публикации F6	https://www.f6.ru/blog/telemancon/

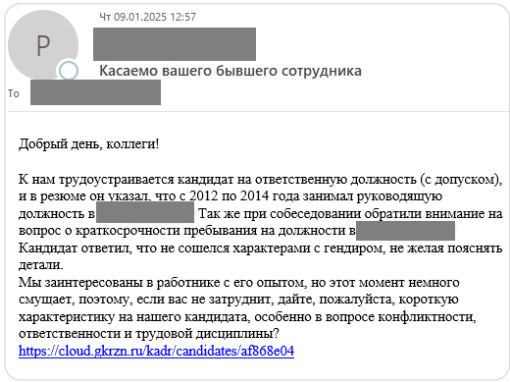
В феврале 2025 года специалисты компании F6 обнаружили новую прогосударственную группировку, которой было присвоено имя **Telemancon**. Группа имеет несколько пересечений с **Core Werewolf**, однако доказательств, чтобы сказать, что это один и тот же злоумышленник, недостаточно. В ходе исследования инфраструктуры удалось установить, что самая ранняя активность группы Telemancon датируется февралем 2023 года. Выявленные атаки были направлены на российские организации в сфере промышленности. Группа использует самописный дроппер и бэкдор, которым были даны имена соответственно **TMCDropper** и **TMCShell**.

Типовая цепочка атаки начинается с рассылки письма с вложенным архивом, содержащим вредоносный исполняемый `.scr`-файл. Этот файл был классифицирован специалистами F6 как дроппер, написанный на языке C++, позднее был переписан на C#. Дропперу было присвоено имя TMCDropper. Он выполняет три основные задачи: проверку выполнения в режиме отладки / в песочнице, извлечение и закрепление следующей стадии в виде бэкдора TMCShell, отображение документа-приманки. Для получения адреса управляющего сервера бэкдор TMCShell генерирует ссылки на страницы ресурса telegra[.]ph, при обращении к которым извлекает закодированный C2-адрес из содержимого результата запроса. TMCShell имеет возможность получать от сервера произвольные PowerShell-скрипты, выполнять их в зараженной системе и эксфильтровать результаты выполнения на C2.

Mythic Likho	
Псевдонимы	Loki, Merlin, Arcane Wolf, Arcane Werewolf
Начало активности	2024 г.
Целевые страны	Россия
Целевые индустрии	Промышленность, телекоммуникации
Атакуемые платформы	Windows
Инструменты	Merlin, Loki, Mythic, Go-дроппер, C++-дроппер
Особенности	• Использование фреймворка Mythic и агентов для него. • Фишинговые ссылки маскируются под ссылки на файлообменники организаций — отправителей писем

В 2024 году была выявлена активность, в ходе которой неустановленные злоумышленники использовали агент **Loki**, а также инструменты **Ngrok** и **gTunnel** — для организации туннелей в инфраструктуре жертвы.

В 2025 году исследователи выявили новую кампанию этого злоумышленника и присвоили ему имя **Mythic Likho**. Группа рассылала письма с вредоносной ссылкой, ведущей на загрузку архива под видом резюме. Легенда письма достаточно уникальна: оно приходит якобы от рекрутеров, которые интересуются бывшим сотрудником организации. Содержимое письма представлено на рис. 12.


Чт 09.01.2025 12:57

P [redacted]

Касаемо вашего бывшего сотрудника

To [redacted]

Добрый день, коллеги!

К нам трудоустраивается кандидат на ответственную должность (с допуском), и в резюме он указал, что с 2012 по 2014 года занимал руководящую должность в [redacted] Так же при собеседовании обратили внимание на вопрос о краткосрочности пребывания на должности в [redacted]
Кандидат ответил, что не сошелся характерами с гендиром, не желая пояснять детали.
Мы заинтересованы в работнике с его опытом, но этот момент немного смущает, поэтому, если вас не затруднит, дайте, пожалуйста, короткую характеристику на нашего кандидата, особенно в вопросе конфликтности, ответственности и трудовой дисциплины?
https://cloud.gkrzn.ru/kadr/candidates/af868e04

Рис. 12 — Пример письма группы Mythic Likho от 09.01.2025

Архив содержит несколько файлов, среди которых есть .lnk, при его открытии запускается прописанная в файле команда. Эта команда, в свою очередь, запускает скрипт, задача которого — запуск агента Merlin с помощью непрямого запуска через утилиту conhost с параметром headless.

В октябре 2025 года группа снова провела кампании, нацеленные на промышленные организации. Цепочки атаки использовались прежние, но легенда была изменена. На этот раз под видом деловой переписки злоумышленники отправляли жертвам ссылки с ВПО. Перейдя по ссылке, жертва видела страницу, замаскированную под корпоративный файлообменник, с которого загружался вредоносный ZIP-архив. Архив имел типовое содержимое для группы: в нем было несколько фотографий, а также вредоносный LNK-файл, замаскированный под служебный документ в формате PDF. Содержимое архива — на рис. 13.

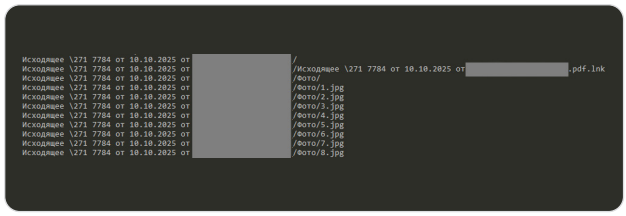


Рис. 13 — Содержимое вредоносного архива, загружаемого по ссылке из письма группы Mythic Likho

Если пользователь открывал «документ», загружался и запускался дроппер. Это вредоносная программа, которая несла в себе отвлекающий файл и еще одну вредоносную программу — загрузчик Loki. Загрузчик собирал базовую информацию о скомпрометированном хосте и отправлял ее злоумышленникам, а также загружал с сервера и запускал имплант Loki. Имплант, в свою очередь, выполнял функции трояна удаленного доступа, позволяя атакующим скрытно выполнять на устройстве жертвы различные команды. В ноябре была замечена очередная атака, но в ней использовался новый дроппер на C++ и обновленный загрузчик Loki. Главная особенность загрузчика заключается в том, что, помимо возможности получения импланта Loki от сервера, данный экземпляр содержит локальный вариант импланта Loki обновленной версии.

NGC6061	
Начало активности	2024 г.
Целевые страны	Россия
Целевые индустрии	Госучреждения, НИИ
Атакуемые платформы	Windows
Инструменты	Metasploit TCP Reverse
Особенности	• Рассылка с адресов на Yandex.ru, Mail.ru, но мимикрия отправителя преимущественно под федеральные органы, реже — под коллег жертвы. • Приманки со встроенным механизмом профилирования жертв

NGC6061 — группа, раскрытая в сентябре 2025 года, атакующая преимущественно российский госсектор. Специалисты F6 выявили рассылку группы в адрес российского НИИ. Самые ранние образцы ВПО группы были обнаружены в мае 2024-го.

В марте 2025 года группа проводит рассылки писем с защищенным паролем архивом во вложении, замаскированном под «материалы к совещанию у Министра» (рис. 14). У какого именно министра, в письме не уточняется.

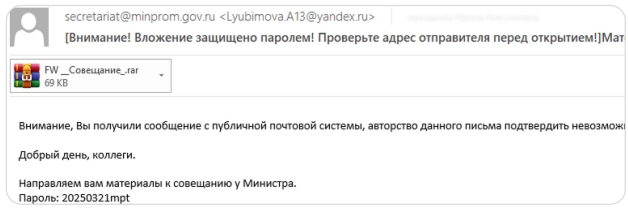


Рис. 14 — Пример письма группы NGC6061

Архив содержит `.lnk`-файл, при запуске которого будут выполнены две PS-команды. Первая команда будет парсить содержимое `.lnk` по символу обратного апострофа. Искомый блок, который является второй командой, будет выполнен через Invoke-Expression. Вторая команда снова парсит файл, только уже по символу «тильда». Искомые данные декодируются из Base64 и записываются на диск в виде двух файлов: приманки с функцией профилирования и исполняемого файла-загрузчика. Профилирование реализовано следующим образом: группировка вшивает веб-маяк через внешнее изображение (ссылка хранится в `word/_rels/document.xml.rels`). При открытии документа инициируется HTTP-запрос на контролируемый злоумышленниками узел. По такому запросу оператор получает публичный исходящий IP-адрес и метку времени каждого обращения, а также сам запрошенный URL/путь с уникальным токеном, который однозначно связывает открытие с конкретным адресатом или волной рассылки. Аналогичная техника использовалась группировкой **IAmTheKing**, поэтому часть исследователей полагает, что за этими двумя группами стоит один и тот же атакующий. Данных для подтверждения этой гипотезы в настоящий момент недостаточно.

30 марта 2025 года была обнаружена еще одна рассылка группы с темой «Форма представления сведений». Цепочка идентична: RAR→ self-extracting LNK→ дроппер полезной нагрузки и приманка → нагрузка. Здесь в качестве нагрузки распространялся **Metasploit TCP Reverse**.

В июле и сентябре 2025 года злоумышленники использовали технику DLL side-loading. Обновленная цепочка атаки: EML-письмо → RAR-архив → LNK-дроппер → PS1-дроппер → EXE — легитимный лоадер → DLL reverse shell.

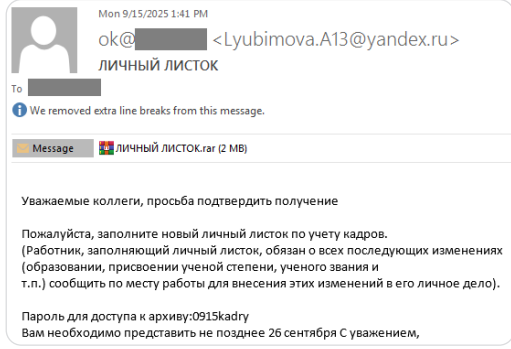


Рис. 15 — Пример письма группы NGC6061

Кроме привычных для NGC6061 писем, которые включают в себя защищенные паролем архивы с `.lnk`-файлами, злоумышленники рассылают письма с архивами без пароля, содержащими приманки с функцией профилирования. Вероятно, для разведывательных целей.

CloudSorcerer	
Начало активности	2020 г.
Целевые страны	Россия, Китай, Япония, Малайзия, Перу
Целевые индустрии	ИТ, госучреждения
Атакуемые платформы	Windows, Linux
Инструменты	AufTime, COFFProxy, VtChatter, YaLeak, CloudyLoader, OneDriveDoor, LocalPlugx, CloudSorcerer, CobaltStrike, OWOWA. SharpChrome.exe, SharpDir.exe, StickyNotesExtract.exe, Advanced IP Scanner, Tailscale VPN, Microsoft dev tunnels, Impacket
Особенности	• Использование легитимных сервисов в качестве управляющих серверов. • Пересекающееся ВПО с тремя китайскими группами (Mustang Panda, APT31 и APT27). • Многообразие утилит и ВПО. • Долгий период скрытого присутствия в сети жертвы

В июле 2024 года исследователи опубликовали информацию о предположительно китайской группе, нацеленной на российский ИТ-сектор, в особенности на компании, работающие как подрядчики для государственных органов, и присвоили ей имя **CloudSorcerer**. Примечательная особенность группы — использование легитимных сервисов в качестве управляющих серверов. В аналитическом отчете F6 «Киберугрозы в России и СНГ 2024/25» мы отмечали, что в арсенале CloudSorcerer ранее был замечен ряд уникальных инструментов, которые можно атрибутировать трем китайским группировкам: **Mustang Panda**, **APT31** и **APT27**. Ввиду этого мы продолжаем отслеживать эту группу как самостоятельную угрозу, несмотря на то что ряд исследователей объединяют ее с группой APT31.

В 2025 году исследователи фиксировали атаки группы. При расследовании инцидента в одной российской ИТ-компании в июле 2025 года специалисты установили, что злоумышленники получили доступ к инфраструктуре еще в конце 2022 года.

Другой вариант атаки был выявлен в декабре 2024 года, угроза сохранялась до апреля 2025-го. Группа использовала фишинг с сопроводительным письмом якобы от менеджера по закупкам. К письму прикреплялся вредоносный архив с LNK-файлом, запускающим документ-приманку и **CloudyLoader** — загрузчик CobaltStrike. Специалисты отмечают: несмотря на то что большая часть атак была нацелена на российские компании, также удалось найти их следы в Китае, Японии, Малайзии и Перу.

В процессе атаки злоумышленники использовали множество общедоступных утилит, известное ранее ВПО **LocalPlugx**, **CloudSorcerer**, **GrewApacha** и новые инструменты, среди которых:

- **AufTime** — бэкдор на Linux, использующий библиотеку wolfSSL для общения с C2;
- **COFFProxy** — бэкдор, загружающий Beacon-маяки формата COFFLoader. Кроме того, была обнаружена реализация этого инструмента на языке Golang с заменой загрузки маяков на выполнение аналогов команд cmd;
- **VtChatter** (также известный как **VTDoor**) — ВПО, которое использует комментарии к файлу на VirusTotal как двусторонний C2-канал;
- **CloudyLoader** — загрузчик импланта CobaltStrike, который использует прямые системные вызовы (direct syscalls) и загружает полезную нагрузку с репозитория GitHub злоумышленника;
- **OneDriveDoor** — бэкдор, использующий в качестве C2 облачное хранилище OneDrive.

Для эксфильтрации данных злоумышленники применяли инструмент YaLeak, который выгружал информацию в облачное хранилище «Яндекса».

PhantomCore	
Псевдонимы	UNG0901 Ряд исследователей отслеживают как Head Mare (Rainbow Hyena, Fairy Trickster), у нас они выделены в отдельную группу
Начало активности	2022 г.
Целевые страны	Россия, Беларусь
Целевые индустрии	ИТ, промышленность, энергетика, строительство, ЖКХ, финансы, транспорт, телекоммуникации, НИИ
Инструменты	PhantomCore.KscDL_trim, PhantomRAT, PhantomCore.PyTaskBackdoor, MeshAgent, Sliver, PhantomeCore.GreqBackdoor, PhantomCore.PollDL, PhantomTaskShell, PhantomStealer, XenAllPasswordPro, PhantomProxyLite, PhantomGoShell, PhantomDL, PhantomCSLoader, PhantomPSUpload, RSocx
Особенности	• Сложное самописное ВПО. • Поддержка разных языков программирования. • Взаимодействие с группами-вымогателями
Публикации F6	https://www.f6.ru/blog/traces-of-phantomcore/ https://www.f6.ru/blog/bearlyfy/

PhantomCore — группа, атакующая российские и белорусские компании с 2022 года, впервые обнаруженная специалистами F6 в 2024 году.

В первой половине 2025 года группа была наиболее активной, мы детектировали постоянную разработку инструментов и большое количество атак. Но во второй половине года активность стала снижаться, а под конец года мы практически совсем перестали наблюдать эту группу. Некоторые исследователи отмечают, что в группе мог произойти раскол, также не исключено, что после подробного освещения деятельности и инфраструктуры группы исследователями злоумышленники могли изменить свой почерк, чтобы снизить детектируемость.

Отличительная черта PhantomCore — использование вредоносного программного обеспечения (ВПО) собственной разработки. Причем, судя по количеству таких самописных программ, а также по количеству атак, команда разработчиков этой киберпреступной группы постоянно ищет новые решения, совершенствует свои инструменты и внимательно следит за новыми уязвимостями.

В отчетном периоде специалистам F6 удалось выявить раннюю инфраструктуру группы и связанные образцы ВПО. Оказалось, что первые атаки группа проводила в 2022 году, они были направлены на кражу, повреждение и уничтожение данных. В последние несколько лет мы наблюдаем, что атаки, в которых замечено ВПО группы PhantomCore, заканчиваются шифрованием инфраструктур жертв с целью получения финансовой выгоды.

В 2024 году мы отмечали, что для первоначального доступа и эксплуатации злоумышленники из **Head Mare** использовали фишинговые письма, содержащие архивы с ВПО группы **PhantomCore PhantomDL** и **PhantomRAT**. Для шифрования файлов группа использовала **LockBit** и **Babuk**. В 2025 году специалистами F6 была раскрыта новая группа вымогателей, получившая название **Bearlyfy**. Она использует известные программы-вымогатели семейств **LockBit 3.0 (Black)** и **Babuk**. Также были обнаружены пересечения в инфраструктуре **Bearlyfy** и **PhantomCore**.

Предположительно, группа PhantomCore после получения первоначального доступа и сбора необходимой ей информации передает доступ или иным образом взаимодействует с другими кибергруппами, нацеленными на шифрование инфраструктуры по политическим мотивам и/или с целью получения финансовой выгоды.

Периодически в арсенале группы можно увидеть оригинальные подходы к атакам. Так, в начале 2025 года злоумышленники нацеливались на ИТ- и ИБ-компании. В качестве первоначального вектора был выбран фишинг, совмещенный с техникой Rogue RDP. Атака заключалась в отправке конфигурационных файлов с расширением `.rdp` и персонифицированных учетных данных с просьбой подключиться к внешнему терминальному серверу злоумышленников, а также в использовании, предположительно, домена «зомби-компании».

Спустя несколько секунд после установления сеанса связи с терминальным сервером сессия завершается. Однако этого времени достаточно, чтобы хост жертвы был заражен вредоносной программой, классифицированной нашими специалистами как **PhantomCore.KscDL_trim**, представляющим собой урезанную версию загрузчика.

Также группа нередко использовала технику polyglot. Она рассылала фишинговые письма с вложением, которое одновременно является и архивом, и исполняемым файлом. Если его открывают из почтового клиента, файл открывается в архиваторе и распаковывает содержащийся в себе упакованный вредоносный ярлык. В результате выполнения цепочки атаки на машину жертвы устанавливалась разная нагрузка, в частности были замечены бэкдоры **PhantomCore.PyTaskBackdoor**, **PhantomCore.PollDL**.

Также исследователи отмечают, что как минимум в одной из попыток заражения вредоносный архив был загружен на компьютер жертвы через Telegram.

Все это классифицирует группу как способную приспосабливаться, быстро менять инструменты и изобретать нестандартные способы доставки ВПО до целевой организации.

GOFFEE	
Псевдонимы	Paper Werewolf
Начало активности	2022 г.
Целевые страны	Россия
Целевые индустрии	ВПК, госучреждения, ИТ, логистика, СМИ, телекоммуникации, строительство, энергетика, образование, промышленность, туризм, финансы
Атакуемые платформы	Windows, Linux
Инструменты	CVE-2025-8088, CVE-2023-20198, CVE-2024-10442, CVE-2023-22518, CVE-2017-0199, CVE-2021-4034, BindSycler, Chisel, dbuds, DQuic, Ebowla, Metasploit, MiRat, Mythic, Nmap, Owowa, Poseidon Agent, PowerRAT, PowerTaskel, QwakMyAgent, Reptile, Sauropsida, Sliver, SWATSSHD, Tiny SHell
Особенности	Постоянный мониторинг действий администраторов и сотрудников ИБ-подразделений в скомпрометированной инфраструктуре

Группа **GOFFEE** привлекла наше особое внимание в 2025 году, поскольку ей удавалось длительное время находиться в сети жертв незамеченной. Ниже приводим детали атак и разбор TTPs группы, которые удалось получать в ходе исследования и реагирования на инциденты.

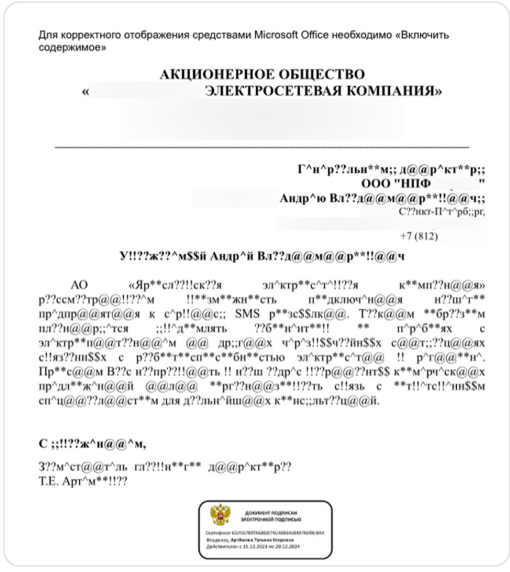
GOFFEE специализируется на проведении целевых атак против российских организаций с целью шпионажа. Группировка фокусируется на долгосрочном и скрытном присутствии в инфраструктуре жертв, вследствие чего ею используются техники, которые обеспечивают длительный и скрытый доступ к скомпрометированным системам. Активность группировки отслеживается с 2022 года.

Особенность группировки — ее постоянный мониторинг действий администраторов и сотрудников ИБ-подразделений в скомпрометированной инфраструктуре. Это позволяет злоумышленникам мимикрировать под легитимную активность и оперативно модифицировать свои инструменты для обхода правил детектирования. По мере изучения конфигурации систем, установленного на устройствах ПО и активности пользователей участники GOFFEE для выбора расположения вредоносных файлов используют наименование распространенного в инфраструктуре ПО или отдельных расширений и драйверов. В качестве полезной нагрузки атакующие используют агенты **Mythic** и SSH-бэкдоры (**ElfDoor/BindSycler** и **SWATSSHD**). После полу-

чения полного контроля над инфраструктурой атакующие применяют для распространения вредоносного ПО корпоративные репозитории с проверенным и разрешенным к использованию перечнем ПО. Они модифицируют и подменяют распространенное ПО (например, архиваторы). Таким образом, при настройке рабочей станции для нового сотрудника или при установке недостающего ПО конечный пользователь или сотрудник ИТ-службы сам загрузит и запустит инструменты атакующих.

В 2025 году группа GOFFEE провела ряд вредоносных кампаний, в том числе с использованием ранее выявленных техник и инструментов, а также значительно расширила инфраструктуру.

Так, в рамках одной из атак, проведенной в марте 2025 года, группировка продолжила начатую в 2024 году кампанию, связанную с рассылкой **PowerRAT**. Злоумышленники осуществили рассылку фишинговых писем с `.docx`-вложением, содержащим вредоносный макрос. Запуск макроса приводил к изменению текста в документе-приманке (рис. 16), а также сбросу на устройство файлов, выполнение которых приводит к заражению устройства PowerRAT.


Для корректного отображения средствами Microsoft Office необходимо «Включить содержимое»

АКЦИОНЕРНОЕ ОБЩЕСТВО
« ЭЛЕКТРОСЕТЕВАЯ КОМПАНИЯ»

У!???ж??^м$$й Андр^й Вл??д@@м@@р!!@@ч**

АО «Яр**сл???!ск??я эл^ктр**с^т^!!??я к**мп??и@@я» р??ссм??тр@@!!??^м !!**зм**жи**сть п**дключ^и@@я и??ш^г** пр^дпр@@ят@@я к с^р!!@@с;; SMS р**зс$$лк@@. Т??к@@м **бр??з**м пл??н@@р;;^тся ;;!!^д**млять ??6**н^нт**!! ** п^р^б**ях с эл^ктр**п@@т??н@@^м @@ др;;г@@х ч^р^з!!$$ч??йи$$х с@@т;;??и@@ях е!!яз??ни$$х с р??б**т**сп**с**би**стью эл^ктр**с^т@@ !! р^г@@**и^. Пр**с@@м В??с и??пр??!!@@ть !! и??ш ??др^с !!??р@@??нт$$ к**м^рч^ск@@х пр^дл**ж^и@@й @@л@@ **ри??н@@з**!!??ть с!!язь с **т!!^тс!!^ни$$м сп^ц@@??л@@ст**м для д??льн^йш@@х к**нс;;льт??и@@й.

С ;;!!??ж^н@@^м,

З??м^ст@@^ль гл???!и**г** д@@р^кт**р??
Т.Е. Арт^м**!!??

Г^и^р??льн**м;; д@@р^кт**р;;
ООО "НПФ "
Андр^ю Вл??д@@м@@р**!!@@ч;;
С??нкт-П!^г^рб;;рг;

+7 (812)

Рис. 16 — Пример документа-приманки группы GOFFEE

Несмотря на то что группировка продолжила использовать техники и инструменты, выявленные в 2024 году, она развивалась и наращивала инфраструктуру. К середине 2025 года специалисты F6 отслеживали ряд сложных атак, проводимых в отношении российских компаний из телекоммуникационной, проектной, ИТ, образовательной, аэрокосмической, оборонно-промышленной и туристических сфер. В рамках данных атак группировка осуществляла первоначальный сбор информации о компаниях путем использования следующих инструментов: **Asnmap**, **Massdns**, **Nmap**, **Subfinder**, **Dirsearch**, **FFUF**, **Metasploit**.

На следующем этапе злоумышленники осуществляли доступ в инфраструктуру жертвы с помощью эксплуатации уязвимостей в CMS-системах, сервисе OWA (Outlook Web Access), Synology Replication Service, Atlassian Confluence Data Center и Server и иных сервисах, а также проводили действия, направленные на получение доступа к базам данных и SSH (в некоторых случаях указанные действия проводились с целью развития атаки в инфраструктуре жертвы).

После получения доступа в инфраструктуру жертвы атакующие извлекали SSH-ключи и конфиденциальные пользовательские данные, которые затем перенаправлялись в контролируемую инфраструктуру. Бэкконект и туннелирование осуществлялись злоумышленниками либо посредством использования **Ligolo-ng** с агентом для скрытого TUN-доступа к сети, либо с помощью **Chisel**, используемого для проброса портов по клиент-серверной схеме. После внедрения с помощью этих инструментов проводилось сканирование внутренних ресурсов.

Кроме того, в арсенале злоумышленников было обнаружено ПО **Evilginx** с фишинг-китами, мимикрирующими под сервисы компании Yandex, что, в свою очередь, указывает на использование дополнительного вектора атак.

К середине лета 2025 года группа расширила свой арсенал, добавив в него эксплойт для уязвимости обхода пути в WinRAR (CVE-2025-8088). Фишинговые письма стали содержать вложенные архивы, при распаковке которых вредоносный файл распаковывался в указанный атакующими каталог.

В августе группировка не отставала от трендов, только вместо полноценной атаки ClickFix предлагала решить капчу Cloudflare, расположенную на ресурсе, мимикрирующем под официальный сайт МВД России (рис. 17), после чего жертва могла скачать вредоносный архив.

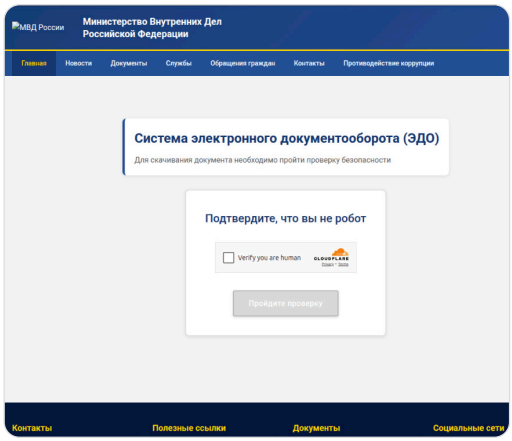


Рис. 17 — Страница, мимикрирующая под домен МВД России, используемая в атаке группы GOFFEE

При распаковке архива на устройство загружалось ВПО класса загрузчик со следующими возможностями:

- запуск дополнительных модулей, имеющихся в системе;
- загрузка следующей стадии в виде библиотек, реализованных на .NET и не сохраняемых в системе, а запускаемых в памяти;
- отображение документа-приманки.

Также исследователями F6 обнаружены аналогичные полезные нагрузки, в части из которых документы-приманки были представлены в виде резюме, а в части в качестве имен файлов были использованы названия браузеров Chrome.exe и Yandex.exe.

В октябре и ноябре 2025 года атакующие провели две фишинговые кампании, направленные на предприятия оборонной промышленности и финансовой сферы. Особенностью данной кампании стало использование атакующими механизма загрузки XLL-дополнений Excel для выполнения произвольного кода на устройстве жертвы, а также использование PowerShell-скриптов с закодированной в Base64 полезной нагрузкой, которая в ходе выполнения скрипта сбрасывалась и запускалась на устройстве (рис. 18).

Рис. 18 — Фрагмент кода группы GOFFEE

Что касается активности GOFFEE в инфраструктуре жертвы, группировка проявляет высокие навыки закрепления и уклонения от обнаружения, а также использует большой арсенал инструментов. В ходе атак на одну из российских компаний злоумышленники использовали утилиты удаленного создания временных задач планировщика Windows, а также протокол WinRM для удаленного выполнения команд на целевой системе.

Для сокрытия действий копировали легитимный файл `cmd.exe` в нестандартное место, такое как `wbem\conhost.exe`. Это позволяло скрытно исследовать окружение, а именно получить список процессов, сетевых соединений и перечень пользователей с помощью стандартных утилит.

Злоумышленники создавали процессы и запускали системные службы вручную с использованием `reg.exe`, маскируя их под легитимные исполняемые файлы, например `LBFOADMIN.exe`, `svchost.exe` с различными параметрами, `RAVBg86.exe` или `vlcmp4_x64.exe`. Работу этих служб и активные сессии проверяли командами `tasklist.exe` и `quser.exe`, а затем настраивали автоматический перезапуск при сбоях.

Кроме того, атакующие производили загрузку и установку своих сертификатов, которая выполнялась путем загрузки файла с внешнего ресурса, его распаковки с использованием 7-Zip и установки с помощью certutil.

Для сокрытия следов атакующие удаляли все записи из каталога Prefetch и подменяли временные метки файлов с использованием PowerShell. Это можно было обнаружить по подстрокам CreationTime, LastWriteTime или LastAccessTime в аргументах скрипта.

Также злоумышленники изменяли параметры автозапуска в реестре, например, подменяя AutodialDLL в службе WinSock2 или Driver в Print Monitors, указывая путь к вредоносному файлу вместо стандартного.

Тактики, техники и процедуры (TTPs) в соответствии с MITRE ATT&CK группы GOFFEE представлены в таблице ниже.

Тактика	Техника	Описание
Reconnaissance	**Active Scanning: Scanning IP Blocks** T1595.001	Атакующие проводят активное сканирование IP-адресов для выявления активных хостов и открытых портов с использованием Nmap и Masscan
	Active Scanning: Vulnerability Scanning T1595.002	Атакующие выполняют автоматизированное сканирование на наличие известных уязвимостей с помощью Nuclei, скриптов Nmap (NSE) и модулей Metasploit
	Active Scanning: Wordlist Scanning T1595.003	Атакующие используют словари для перебора директорий, файлов, параметров и поддоменов на веб-ресурсах с помощью Ffuf и Dirsearch
	Gather Victim Network Information: Domain Properties T1590.001	Атакующие собирают информацию о доменах и поддоменах с использованием Subfinder, MassDNS
	Gather Victim Network Information: IP Addresses T1590.005	Атакующие собирают информацию об IP-адресах

Тактика	Техника	Описание
Resource Development	**Acquire Infrastructure: Domains** T1583.001	Атакующие приобретают доменные имена, которые впоследствии используются для C2, хранения полезных нагрузок и промежуточных этапов атаки
	Acquire Infrastructure: Virtual Private Server T1583.004	Атакующие арендуют серверы для размещения инфраструктуры и хранения ВПО
	Compromise Infrastructure: Server T1584.004	Атакующие компрометируют легитимные веб-серверы и используют их в качестве промежуточной инфраструктуры
	Stage Capabilities: Upload Malware T1608.001	Атакующие заранее загружают вредоносные файлы на подконтрольные и скомпрометированные веб-ресурсы для последующего скачивания их с зараженных хостов
Initial Access	**Replication Through Removable Media** T1091	Атакующие используют ВПО с возможностью распространения посредством съемных USB-носителей
	Exploit Public-Facing Application T1190	Атакующие эксплуатируют уязвимости в общедоступных приложениях
	Phishing: Spearphishing Attachment T1566.001	Атакующие осуществляют рассылку фишинговых писем, содержащих вредоносные вложения
	Phishing: Spearphishing Link T1566.002	Атакующие рассылают письма с ссылками, ведущими на подконтрольные им ресурсы, с которых осуществляется загрузка ВПО

Тактика	Техника	Описание
Execution	**Windows Management Instrumentation** T1047	Атакующие используют WMI для получения информации о зараженной системе
	Scheduled Task/ Job: Scheduled Task T1053.005	Атакующие используют утилиты удаленного создания временных задач планировщика Windows (atexec и др.) для выполнения команд и запуска собственных инструментов
	Command and Scripting Interpreter: PowerShell T1059.001	Атакующие используют встроенные командные интерпретаторы ОС Windows для выполнения произвольных команд, а также закрепления на устройствах
	Command and Scripting Interpreter: Windows Command Shell T1059.002	Атакующие используют встроенные командные интерпретаторы ОС Windows для выполнения произвольных команд, а также закрепления на устройствах
	Command and Scripting Interpreter: Visual Basic T1059.005	Атакующие используют VBS для создания BAT-файлов
	Command and Scripting Interpreter: JavaScript T1059.007	Атакующие используют JavaScript для запуска ВПО
	Native API T1106	Атакующие используют ВПО, взаимодействующее с API CreateThread и VirtualAlloc
	System Services: Service Execution T1569.002	Атакующие создают системные службы Windows для разового выполнения команд на скомпрометированном устройстве
	User Execution: Malicious Link T1204.001	Фишинговые письма атакующих содержат вредоносные ссылки, при переходе по которым осуществляется скачивание вредоносных файлов

Тактика	Техника	Описание
Execution	**User Execution: Malicious File** T1204.002	Атакующие модифицируют и подменяют исполняемые файлы на корпоративном файловом хранилище с разрешенным в организации ПО (например, архиваторы). После этого пользователь сам загружает и запускает вредоносный файл. Фишинговые письма атакующих содержат вредоносные вложения, запуск которых инициирует цепочку атаки
Persistence	**Valid Accounts** T1078	Атакующие используют скомпрометированные ранее доменные и локальные учетные записи легитимных пользователей в процессе атаки
	Modify Registry T1112	Атакующие используют встроенную утилиту ОС Windows reg.exe для внесения изменений в реестр обеспечивающих автоматизированный запуск собственных инструментов (модификация параметров AutodialDLL, Print\Monitors)
	Office Application Startup: Add-ins T1137.006	Атакующие создали вредоносный XLL-файл (DLL в формате XLL), который Excel загрузил как дополнение. При открытии файла вызывается функция xlAutoOpen(), автоматически выполняющая полезную нагрузку
	Create or Modify System Process: Windows Service T1543.003	Атакующие создают системные службы Windows для автоматизированного запуска агентов Mythic и собственных бэкдоров
	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder T1547.001	Атакующие осуществляют размещение вредоносных файлов в папку автозагрузки
	Boot or Logon Autostart Execution: Port Monitors T1547.010	Атакующие модифицируют параметры реестра `SYSTEM\CurrentControlSet\Control\Print\Monitors` для обеспечения автоматизированного запуска собственных инструментов

Тактика	Техника	Описание
Persistence	**Hijack Execution Flow: Services Registry Permissions Weakness** T1574.011	Атакующие используют параметр AutodialDLL в конфигурации системной службы WinSock2 для обеспечения автоматизированного запуска собственных инструментов
Privilege Escalation	**Scheduled Task/ Job: Scheduled Task** T1053.005	Атакующие используют задачи планировщика Windows для выполнения команд и запуска собственных инструментов с правами системы
	Exploitation for Privilege Escalation T1068	Атакующий эксплуатируют уязвимость CVE-2021-4034 для повышения привилегий
	Valid Accounts T1078	Атакующие используют скомпрометированные ранее доменные и локальные учетные записи легитимных пользователей в процессе развития атаки
	Create or Modify System Process: Windows Service T1543.003	Атакующие создают системные службы Windows для выполнения команд и запуска собственных инструментов с правами системы
	Boot or Logon Autostart Execution: Port Monitors T1547.010	Атакующие модифицируют параметры реестра `SYSTEM\CurrentControlSet\Control\Print\Monitors` для запуска своих инструментов с правами системы
Defense Evasion	**Obfuscated Files or Information: Software Packing** T1027.002	Атакующие используют упаковщик Ebowla для доставки BindSycler
	Obfuscated Files or Information: Embedded Payloads T1027.009	Атакующие обфусцируют некоторые файлы с целью затруднения их анализа и обхода механизмов обнаружения

Тактика	Техника	Описание
Defense Evasion	**Obfuscated Files or Information: LNK Icon Smuggling** T1027.012	Атакующие используют ВПО, маскирующее ярлык в зависимости от расширения исходного файла
	Obfuscated Files or Information: Encrypted/Encoded File T1027.013	Атакующие шифруют полезную нагрузку, а для расшифровки используют уникальные свойства конкретного устройства (имя рабочей станции или наличие файла)
	Masquerading: Rename Legitimate Utilities T1036.003	Атакующие создают копию командного интерпретатора `cmd.exe` (`C:\Windows\System32\wbem\conhost.exe`) для противодействия правилам обнаружения, основанным на использовании конкретных файлов и утилит
	Masquerading: Masquerade Task or Service T1036.004	Атакующие используют названия и описания компонентов легитимного ПО для создания системных служб и задач планировщика
	Masquerading: Double File Extension T1036.007	Атакующие используют файлы с двойным расширением (например, `.pdf.exe`)
	Masquerading: Match Legitimate Resource Name or Location T1036.005	Атакующие используют имена различных легитимных файлов ОС Windows для сохранения собственных инструментов
	Deobfuscate/Decode Files or Information T1140	Атакующие декодируют полезную нагрузку
	Indicator Removal: File Deletion T1070.004	Атакующие удаляют файлы Prefetch для усложнения криминалистического анализа. Атакующие удаляют исполняемые файлы собственных утилит в случае частых сбоев в их работе или заменяют на другие

Тактика	Техника	Описание
Defense Evasion	**Indicator Removal: Clear Persistence** T1070.009	Атакующие удаляют созданные ранее методы закрепления в случае частых сбоев в их работе: удаляют системные службы и восстанавливают значения параметров реестра
	Indicator Removal: Timestomp T1070.006	Атакующие подменяют временные метки большинства загруженных в процессе атаки файлов
	Indicator Removal: Relocate Malware T1070.010	Атакующие изменяют шаблоны именования и расположения вредоносных файлов по мере изучения скомпрометированной инфраструктуры. При этом старые версии файлов атакующие удаляют
	Valid Accounts T1078	Атакующие используют ранее скомпрометированные доменные и локальные учетные записи легитимных пользователей, полученные в период развития атаки
	Modify Registry T1112	Атакующие вручную очищают параметры созданных ранее системных служб при помощи утилиты reg.exe
	Subvert Trust Controls: Install Root Certificate T1553.004	Атакующие добавляют собственные корневые сертификаты на скомпрометированные устройства
	Impair Defenses: Indicator Blocking T1562.006	Атакующие используют ВПО, которое патчит Event Tracing for Windows
	Hide Artifacts: Hidden Files and Directories T1564.001	Атакующие используют ВПО, которое осуществляет сокрытие данных

Тактика	Техника	Описание
Credential Access	**Steal Application Access Token** T1528	Атакующие выгружают содержимое служебных каталогов мессенджера Telegram для получения доступа к переписке пользователя
	Unsecured Credentials: Private Keys T1552.004	Атакующие выгружают корневые сертификаты со скомпрометированных систем
	Input Capture: Web Portal Capture T1056.003	Атакующие модифицируют код корпоративных порталов (Bitrix) и встраивают в него модули, которые сохраняют все вводимые пользователями аутентификационные данные в файл
Discovery	**System Service Discovery** T1007	Атакующие проводят разведку конфигурации отдельных рабочих станций и серверов, устройства инфраструктуры, а также активности пользователей. Атакующие точечно проверяют работоспособность установленных в процессе развития атаки инструментов и при необходимости перезапускают их или модифицируют. Для проведения разведки атакующие преимущественно используют встроенные утилиты и различные оснастки ОС
	Remote System Discovery T1018	
	System Owner/User Discovery T1033	
	Network Service Discovery T1046	
	System Network Connections Discovery T1049	
	Process Discovery T1057	

Тактика	Техника	Описание
Discovery	**System Information Discovery** T1082	Атакующие проводят разведку конфигурации отдельных рабочих станций и серверов, устройства инфраструктуры, а также активности пользователей.
	File and Directory Discovery T1083	Атакующие точечно проверяют работоспособность установленных в процессе развития атаки инструментов и при необходимости перезапускают их или модифицируют.
	Account Discovery T1087	Для проведения разведки атакующие преимущественно используют встроенные утилиты и различные оснастки ОС
	Network Share Discovery T1135	
	Software Discovery T1518	
	Log Enumeration T1654	Атакующие осуществляют поиск по журналам системных событий Windows для получения информации о конфигурации сетевых интерфейсов скомпрометированного устройства
Lateral Movement	**Remote Services: Remote Desktop Protocol** T1021.001	Атакующие используют протокол удаленного рабочего стола Windows для подключения к устройствам в скомпрометированной инфраструктуре
	Remote Services: SMB/ Windows Admin Shares T1021.002	Атакующие используют утилиты, позволяющие загружать файлы и удаленно выполнять команды на скомпрометированных устройствах при помощи протокола SMB
	Remote Services: Windows Remote Management T1021.006	Атакующие используют службу WinRM для горизонтального перемещения по сети

Тактика	Техника	Описание
Lateral Movement	**Taint Shared Content** T1080	Атакующие модифицируют и подменяют исполняемые файлы на корпоративном файловом хранилище с разрешенным в организации ПО
	Replication Through Removable Media T1091	Атакующие используют модуль USB Worm для горизонтального перемещения при помощи USB-носителей
	Lateral Tool Transfer T1570	Атакующие распространяют свои инструменты в локальной сети, используя скомпрометированные ранее рабочие станции и серверы
Collection	**Data from Local System** T1005	Атакующие выгружают пользовательские данные
	Data from Removable Media T1025	Атакующие могут осуществлять сбор данных со съемных носителей с использованием FlashFileGrabber
	Screen Capture T1113	Атакующие могут получать снимки экрана с использованием PowerTaskel
	Automated Collection T1119	Атакующие используют инструменты и скрипты для сбора интересующих файлов и данных со скомпрометированных систем
	Archive Collected Data: Archive via Utility T1560.001	Атакующие архивируют при помощи предустановленных пользователями утилит (7z, ZIP) собранные данные для их последующей выгрузки
	Input Capture: Web Portal Capture T1056.003	Атакующие модифицируют код корпоративных порталов и встраивают в него модули, которые сохраняют все вводимые пользователями аутентификационные данные в файл. Для получения содержимого этого файла атакующим необходимо ввести в форму авторизации заранее сконфигурированные значения

Тактика	Техника	Описание
Command and Control	**Data from Local System** T1005	Атакующие выгружают системные данные мессенджера Telegram для получения доступа к переписка пользователя
	Application Layer Protocol: Web Protocols T1071.001	Атакующие используют протоколы HTTP/ HTTPS для связи с C2
	Proxy T1090	Используемый атакующими инструмент DQuic может проксировать соединение на C2
	Ingress Tool Transfer T1105	Атакующие загружают необходимые для развития атаки файлы на скомпрометированные устройства с подконтрольных им серверов
	Data Encoding: Standard Encoding T1132.001	Атакующие кодируют передаваемые данные в Base64
	Protocol Tunneling T1572	Атакующие используют инструменты, позволяющие настраивать сетевые туннели для доступа к скомпрометированным устройствам
Exfiltration	**Exfiltration Over C2 Channel** T1041	Атакующие используют Sliver для эксфильтрации данных
	Exfiltration Over Web Service: Exfiltration to Cloud Storage T1567.002	Атакующие выгружают собранные в процессе развития атаки данные при помощи сервисов временного обмена данными (bashupload.com, gofile.io)

Обзор менее активных APT-группировок

IronHusky

IronHusky — китайскоязычная хакерская группировка, впервые обнаруженная в июле 2017 года. Цель группировки в основном государственные учреждения Монголии, также атакам были подвержены государственные учреждения России и Индии.

В апреле 2025 года специалисты зафиксировали атаки на государственные учреждения Монголии и России с применением обновленной версии трояна **MysterySnail**, а также его упрощенной версии — **MysteryMonoSnail**. **MysterySnail** поддерживает 40 команд, что позволяет ему управлять файловой системой (чтение, запись и удаление файлов, а также перечисление дисков и каталогов), выполнять команды через командную оболочку, создавать и завершать процессы, управлять службами, подключаться к сетевым ресурсам. **MysteryMonoSnail** представляет собой урезанную версию **MysterySnail**, поддерживает всего 13 основных команд для просмотра содержимого каталогов, записи данных в файлы, запуска процессов и командных оболочек, а также отличается тем, что для взаимодействия с C2 использует протокол WebSocket вместо HTTP.

NGC4141

NGC4141 — группировка, обнаруженная осенью 2025 года и нацеленная на российские государственные организации с целью кибершпионажа. В ходе атаки **NGC4141** использовала в качестве первоначального вектора уязвимости в кастомных веб-приложениях целевой организации. Кроме того, злоумышленники используют общедоступный сервис FOFA, инструмент для работы с API **Postman**, инструменты для автоматического сканирования, веб-шеллы WSO и Godzilla. По предварительным данным, злоумышленники действуют из Восточной Азии.

Первые следы атаки датируются декабрем 2024 года. Несколько дней злоумышленники активно сканировали сайт на наличие уязвимостей — нагрузка доходила до тысяч запросов в час. Спустя время они перешли к ручному анализу системы и нашли способ проникновения. Атакующие использовали недокументированные возможности API в публично доступных веб-приложениях, найденные в результате ручного сканирования, через которые внедрили на сервер веб-шеллы, позволяющие управлять системой через веб-интерфейс. Примечательно, что веб-приложение было кастомным. Для таких решений нет готовых эксплойтов в открытом доступе, поэтому взлом подобного ресурса требует высокой квалификации. Через созданные веб-шеллы атакующие выполняли множество команд по разведке системы, ее окружения, сбору и эксфильтрации данных. Также они проверяли доступность различных ресурсов государственного сектора, следовательно, их целью были и другие организации из этой сферы.

SkyCloak

В октябре 2025 года исследователи выявили кампанию, нацеленную на военно-

служащих России и Беларуси. Особенностью этих атак стала цепочка заражения, в которой злоумышленники устанавливали многоступенчатый бэкдор с использованием OpenSSH и анонимной инфраструктуры Tor с мостами obfs4. Это позволяло им общаться с серверами через onion-адрес.

Письма рассылаются под видом военных документов и содержат ZIP-архив, внутри которого скрыт LNK-файл и дополнительный архив. Открытие ярлыка запускает цепочку PowerShell-команд, инициирующих дальнейшую загрузку компонентов. Эти команды выявляют, не запущен ли файл в виртуальной среде. При успешном прохождении проверки скрипт открывает приманку и одновременно создает запланированную задачу для ежедневного запуска компонента OpenSSH для Windows, размещенного под видом файла `githubdesktop.exe`. Через него устанавливается ограниченный по ключам SSH-доступ, позволяющий операторам удаленно взаимодействовать с жертвой. Второй элемент — модифицированная сборка Tor, размещенная под именем `pinterest.exe`, также запускается по расписанию. Ее задача — создать скрытую службу, связывающуюся с onion-адресом злоумышленников через obfs4-трафик. Это позволяет проксировать доступ к сервисам RDP, SMB и SSH по сети Tor, обеспечивая при этом устойчивое соединение и обход стандартных средств защиты. По завершении установки бэкдор передает сведения о зараженной системе, включая сгенерированный для нее onion-хостнейм, посредством команды curl. После этого злоумышленники получают возможность полноценно управлять целевой машиной, пользуясь **зашифрованным** каналом связи.

Стоит отметить, что новость об этой атаке также была опубликована в Telegram-канале группы IT Army of Ukraine (рис. 19).

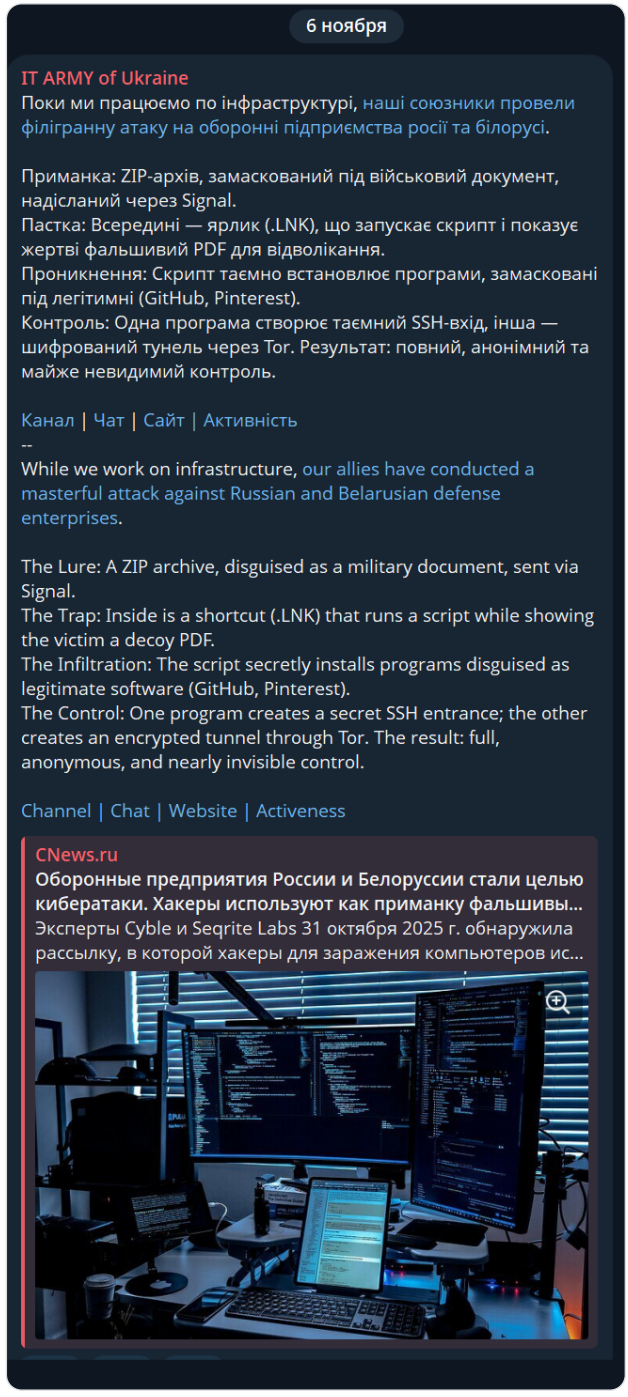


Рис. 19 — Скриншот поста в Telegram-канале группы IT Army of Ukraine

Mysterious Elephant

Mysterious Elephant — это APT-группа, обнаруженная в 2023 году, вероятно, действует из Индии. Основная цель атакующих — правительственные организации в Азиатско-Тихоокеанском регионе. Однако в 2025 году исследователи отмечали, что около **4%** атак на целевые страны приходится на Россию.

Для получения первоначального доступа к своим целям группа использует комбинацию из набора эксплойтов, фишинговых писем и вредоносных документов. Проникнув в систему, они задействуют ряд специально разработанных инструментов и утилит с открытым исходным кодом: PowerShell-скрипты, инструмент **BabShell**, предназначенный для создания реверс-шелла, кастомизированные загрузчики **MemLoader HidenDesk** и **MemLoader Edge**, бэкдор **VRat**, инструменты эксфильтрации **Uplo Exfiltrator**, **Stom Exfiltrator**, **ChromeStealer Exfiltrator**.

UNC5221

Предположительно, китайская прогосударственная группа, также известная по псевдонимам **QuietCrabs**, **UTA0178**, **UNC5221**, **Red Dev 61**. Впервые обнаружена в начале 2024 года, нацелена на множество стран.

В 2025 году специалисты в ходе расследования инцидентов в российских организациях выявили ВПО группы UNC5221. Атаки группировки характеризуются массовым сканированием интернета в поиске уязвимых серверов. В первом инциденте группа эксплуатировала CVE-2025-4427 и CVE-2025-4428 через день после официального заявления Ivanti. Во втором инциденте были обнаружены следы успешной эксплуатации CVE-2025-53770 в течение суток после публикации эксплойта, а неудачные попытки — в течение нескольких часов после первых публикаций неработающих эксплойтов.

Алгоритм действий группировки после получения доступа к серверу SharePoint следующий:

- закрепление на уязвимом сервере через загрузку ASPX-веб-шелла;
- получение информации о внешнем IP-адресе и проверка доступов на запись в файл;
- загрузка следующей стадии в виде KrustyLoader с внешнего сервера;
- загрузка и запуск через **KrustyLoader** импланта **Sliver**.

UNC5174

Исследователи сообщают, что группа **UNC5174**, действующая с 2023 года, в отчетном периоде атаковала среди множества других стран и российские организации. Атаки были начаты осенью 2024 года, а среди целей были ИТ, НИИ и государственные организации. Во время расследования одного из инцидентов специалисты установили, что в атаках группа использовала три инструмента: **SNOWLIGHT**, который выполнял роль загрузчика для **VShell RAT**, дополнительно злоумышленники применяли **GOREVERSE** — обратный шелл на Go, функционирующий через SSH.

Активность группы была обнаружена в рамках реагирования на инцидент у ИТ-подрядчика, в инфраструктуре которого также было выявлено присутствие еще одной восточноазиатской группы, отслеживаемой по имени NGC5081.

NGC5081

В конце мая 2025 года специалисты реагировали на инцидент в телекоммуникационной компании, реализованный через компрометацию ИТ-подрядчика. В сети подрядчика было обнаружено две группы: UNC5174 и группа, получившая имя **NGC5081**, которая использовала ранее неизвестный бэкдор на языке Rust **IDFKA** для Linux-систем. С помощью этого бэкдора атакующие в течение десяти месяцев (с осени 2024 года) сохраняли доступ к ИТ-инфраструктуре подрядчика, а также получили доступ к базам минимум двух компаний-клиентов, где хранилась информация об абонентах и метаинформация об их звонках. Атакующие не закрепляли бэкдор — это было возможно благодаря тому, что системы не перезагружались несколько лет. Помимо IDFKA, группа использовала бэкдор **Tinyshell**.

Space Pirates

В 2025 году специалисты зафиксировали фишинговую кампанию группы **Space Pirates**, направленную преимущественно на госсектор. Позднее удалось обнаружить аналогичные рассылки, распространяемые с лета 2024 года. Фишинговое письмо 2025 года отправлено с почты подрядчика, предположительно скомпрометированного ранее. В ходе атаки злоумышленники распространяли вредоносные архивы через сервис одноразовых ссылок, принадлежащий организации-жертве. Архив содержит вредоносный LNK-файл, который загружает документ-приманку и следующий компонент атаки в виде VBS-загрузчика. Загрузка файлов из цепочки атаки выполняется со скомпрометированного ресурса негосударственной образовательной организации. VBS-загрузчик запускает приманку и загружает загрузчик **TADS**, который выполняет большую проверку на факт запуска в виртуальной среде. Если проверка пройдена, то выполняет запрос, в результате загружается плагин Scythe. Он отвечает за закрепление финальной нагрузки через планировщик задач. Плагин загружается в бесфайловом режиме и существует только в памяти.

Киберпреступные группы

Группы, использующие программы-вымогатели

В 2025 году угроза со стороны шифровальщиков оставалась одной из основных. Регулярно мы получали информацию о новых крупных инцидентах, связанных с шифрованием данных. Основываясь на кластеризации, выполненной специалистами F6, можно отметить, что каждый кластер преследует собственные цели и тактики. Например, проукраинские группировки обычно атакуют крупные компании, нередко совмещая шифрование с эксфильтрацией данных. Их основная задача — получить крупный выкуп и привлечь повышенное внимание к своим действиям. В то же время восточные и другие группировки преимущественно ориентируются на малый и средний бизнес, ограничиваясь сравнительно небольшими выкупами за расшифровку данных. На протяжении 2025 года специалистам F6 удалось выявить **более 600 атак** с использованием программ-вымогателей в России.

В 2025 году значительно снизилась активность таких группировок, как **Shadow**, **MorLock** и **Head Mare**, атаковавших российские компании на протяжении всего предыдущего года, что, вероятно обусловлено консолидацией проукраинских группировок и другими внутренними процессами. Значительно изменилась и активность группировки **Werewolves**: на протяжении всего года мы наблюдали фишинговые рассылки, атрибутируемые злоумышленникам, однако финальные нагрузки оставались неизвестными. В 2025 году уже нет такого взрывного роста числа атак с использованием программ-вымогателей, который мы наблюдали в предыдущие два года. Отметим, что многие атаки шифровальщиков в России все еще по-прежнему связаны с геополитической обстановкой и, очевидно, имеют связи с проукраинскими группами.

Продолжили свою криминальную деятельность ранее активные группировки: **Mimic**, **Proton/Shinra**, **Sauron**, **BlackFL/BlackHunt**, **LokiLocker/BlackBit**, **Enmity/Mammon**, **DCHelp**, **Masque**, **HsHarada**, **OldGremlin**, **Room155** и др.

Как и в прошлые годы, политически мотивированные злоумышленники чаще всего не используют новые уникальные программы, обходясь готовыми решениями на основе утекших в публичный доступ билдеров и исходных кодов **LockBit 3.0 (Black)**, **Conti v2/v3** и **Babuk**. Восточные партнерские программы (RaaS, Ransomware-as-a-Service) активно разрабатывают свои программы-вымогатели, соревнуясь и конкурируя друг с другом для привлечения новых партнеров.

По-прежнему группировкам, атакующим Россию, не свойственно создание сайтов утечек (DLS-ресурсов): если злоумышленники хотят опубликовать данные об атаке, они делают это в Telegram-/Twitter-каналах. Выявлены факты публикации скомпрометированных данных в каналах известных хактивистских групп, что подтверждает связи между шифровальщиками и хактивистами. Эта тенденция связана со спецификой атакующих Россию киберпреступников, поскольку проукраинские группы так или иначе группировки двойного назначения, и их основная цель — нанесение ущерба российским предприятиям.

На смену ушедшим или снизившим свою активность в 2025 году пришли новые группировки, использующие для своих атак программы-вымогатели. Таким образом, список групп двойного назначения, активность которых была замечена специалистами F6 в 2025 году, следующий:

- **Bearlyfy/Labubu (TitanImposter),**
- **Shadow/THOR,**
- **3119/TR4CK.**

Финансово мотивированные группировки и партнерские программы:

- **OldGremin,**
- **DCHelp,**
- **Masque,**
- **Mimic,**
- **Pay2Key,**
- **PE32,**
- **Proton/Shinra,**
- **LokiLocker/BlackBit,**
- **C77L,**
- **Sauron,**
- **BlackFL/BlackHunt,**
- **Enmity/Mammon,**
- **HsHarada,**
- **Room155,**
- **Storm-2603/GOLD SALEM/ CL-CRI-1040.**

Статистика по атакам некоторых группировок в 2025 году:

- **Bearlyfy/Labubu (TitanImposter)** — более **50** атак на компании и организации;
- **Shadow/THOR** — не менее **15** атак на различные компании и организации;
- **Mimic** — более **100** атак на компании среднего и малого бизнеса;
- **Proton/Shinra** — более **50** атак на небольшие компании;
- **DCHelp** — около 15 атак, в том числе и несколько громких.

Более подробная информация о группировках и в целом о ситуации с программами-вымогателями в России будет приведена далее.

Теперь же рассмотрим громкие события и общую ситуацию в мире шифровальщиков за пределами России.

Одна из наиболее активных партнерских программ — **Akira**. В октябре 2025 года атакующие запросили у своей жертвы выкуп в размере **$10 млн**. Партнерская программа **Hunters International** сменила свою направленность, отказавшись от атак, связанных с шифрованием данных, а также предложив своим жертвам бесплатную расшифровку.

Также произошло несколько других интересных событий. В августе 2025 года Министерство юстиции США сообщило о конфискации более $2,8 млн в криптовалюте у предполагаемого оператора программы-вымогателя **Zeppelin**. Этот арест не стал единичным случаем.

Так, по сообщениям международных СМИ, в рамках спецоперации Phobos Aetor в феврале 2025 года в Таиланде были арестованы двое злоумышленников за участие более чем в тысяче атак с применением программ-вымогателей. По данным властей, нанесенный преступниками ущерб оценивается в $16 млн. В ведомстве уточнили, что именно они были операторами группировок **8Base** и **Affiliate 2803**, применявших в своих атаках **Phobos**.

Во второй половине мая Европол провел второй этап Operation Endgame — операции против инфраструктуры киберпреступников, в частности ботнетов. Заявлено, что была нейтрализована инфраструктура, связанная с такими вредоносными программами, как **Bumblebee**, **Lactrodectus**, **Qakbot**, **Hijackloader**, **DanaBot**, **Trickbot** и **Warmcookie**. На первом этапе было отключено 100 серверов, используемых злоумышленниками. В этот раз

правоохранительные органы из семи стран отключили 300 серверов, 650 доменов, а также конфисковали €3,5 млн в криптовалюте.

17 июля 2025 года специалистами правоохранительных органов Японии был опубликован декриптор для расшифровки файлов жертв, подвергшихся атаке Phobos. Однако эта утилита не поддерживает старые версии Windows и имеет ряд недостатков. Специалисты F6 выпустили собственную утилиту для дешифровки файлов, пострадавших в ходе атак программы-вымогателя Phobos. Российские компании и физические лица, которые ранее пострадали от Phobos, теперь могут бесплатно и безопасно восстановить зашифрованные данные. Инструмент можно скачать на GitHub F6 DFIR.

В начале сентября 2025 года представитель **LockBit** на форуме RAMP объявил о запуске партнерской программы версии 5.0. Стоимость доступа составила **$500** — это наименьшая сумма за все время существования партнерского сервиса LockBit. Также интересно, что представитель DragonForce предложил LockBit и Qilin объединить силы и создать некий союз, чтобы контролировать рынок RaaS.

Жертвами вымогателей чаще всего становились российские инжиниринговые компании и предприятия из сфер оптовой и розничной торговли.

Все группировки, атаковавшие Россию в 2025 году, можно условно поделить на три кластера:

1. **Проукраинские группировки** — в ходе исследования атак установлено, что группировки так или иначе связаны между собой, зачастую используют схожие техники и инструменты, а порой совершают совместные атаки, в которых принимают участие сразу несколько групп.
2. **Восточные группировки** — эти атакующие практически идентичны по тактикам, техникам и процедурам, а также используют похожие инструменты. В основном партнерская программа строится на используемых шифровальщиках. Большинство восточных партнерских программ имеют отношение к странам, население которых говорит на персидском языке. (Специалистами F6 также было обнаружено несколько атак на белорусские компании.)
3. **Другие** — в этой категории находятся группировки, которые не имеют между собой общих унифицирующих признаков, тем не менее можно выделить тактики, техники и процедуры, наиболее часто используемые всеми группировками.

Проукраинские группировки

Shadow/THOR	
Начало активности	Март 2023 г.
Цель	Кража конфиденциальной информации, вымогательство финансовых средств за расшифровку данных и непубликацию похищенной информации, продажа похищенной информации, диверсия
Жертвы	Крупные компании
Сумма выкупа	• 4,5–320 млн рублей (в BTC или XMR). • Средняя сумма выкупа — 90 млн рублей
Получение первоначального доступа	Эксплуатация уязвимостей в публично доступных приложениях, доверительные отношения, учетные данные, приобретенные на закрытых торговых площадках, внешние службы удаленного доступа (RDP, VPN), фишинг
Используемые инструменты	LockBit 3.0 (Black), Babuk, Godzilla Webshell, DarkGate, FaceFish, SystemBC, Cobint, Netscan, PingCastle, AnyDesk, Mimikatz, PowerSploit, Cobalt Strike, Sysinternals, PsExec, ProcDump, Ngrok, Meterpreter

Впервые обнаруженная в марте 2023 года, группировка **Shadow** уже более двух лет активно атакует российские компании. Важно отметить, что появление новой группировки **THOR** совпало с последней известной атакой Shadow. Аналогично Shadow, группа THOR имеет чат для коммуникации с жертвой в сети Tor. Есть некоторые основания считать THOR преемником Shadow.

Весной были атакованы сразу несколько российских организаций, среди них компания из сферы здравоохранения. У одной из компаний была запрошена сумма в размере $65 000, у другой — $449 000. В одном из случаев злоумышленники получили доступ в инфраструктуру жертвы из сервиса MightyCall через OpenVPN. Напомним, что злоумышленники не ограничиваются лишь требованием выкупа, так как были замечены случаи кражи криптовалюты из личных кошельков сотрудников атакованных компаний, а также похищение файлов типа session из Telegram-аккаунтов жертв. В середине июня 2025 года специалистами F6 была получена информация о еще нескольких атаках группировки THOR. В одном из случаев злоумышленники запросили выкуп в размере $500 000, в другом — $200 000.

Bearlyfy/Labubu	
Начало активности	Январь 2025 г.
Цель	Шифрование данных и требование выкупа / шифрование и удаление данных
Жертвы	В начале активности — компании малого и среднего бизнеса, затем крупные компании
Сумма выкупа	$2000 — 350 000
Получение первоначального доступа	Компрометация аутентификационных данных, предоставленных подрядчикам. Эксплуатация публичных приложений систем Bitrix и 1С для получения доступа к сети. Группировка также получает доступ к целым группам компаний, обладающих сетевой связанностью, при компрометации одной из них
Используемые инструменты	Babuk, LockBit 3.0 (Black), PolyVice, PhantomTaskShell, MeshAgent, PhantomCore.PollDL, PhantomRAT, Sliver, XenAllPasswordsPro, PowershellKerberos, asio5, cloudflared, localtonet, shinysocks, gost, suo5, neo-regeorg, SoftPerfect Network Scanner, ADRecon, Croc, PsExec

Группировка **Bearlyfy**, появившаяся в начале 2025 года, уже отметилась более чем **30** атаками на российские компании. Изначально группировка атаковала небольшие коммерческие организации, запрашивая несколько тысяч долларов в качестве выкупа, однако уже к концу лета аппетиты злоумышленников заметно выросли и они стали запрашивать десятки тысяч долларов. При этом в некоторых атаках Bearlyfy не запрашивали выкуп, а шифровали данные без возможности их восстановления.

Для своих атак злоумышленники используют программы-вымогатели **LockBit 3 Black** и **Babuk**, однако со своими отличительными особенностями, например записки с требованиями выкупа создаются вручную.

Исследуя атаки группировки, специалисты F6 обнаружили отдельные пересечения в инфраструктуре Bearlyfy и PhantomCore, например использование одних и тех же серверов и IP-адресов. При этом подходы к атакам у группировок существенно различаются: PhantomCore проводит сложные, многоэтапные кампании с фокусом на скрытое присутствие и кражу данных, в то время как Bearlyfy использует обычные инструменты для перемещения внутри сети и удаленного управления системами с прицельным фокусом на достижение немедленного эффекта.

В состав Bearlyfy входят участники различных хакерских группировок, работающие по разным методикам и TTPs, что отражается в разнообразии применяемых техник

и инструментов. Использование программы-вымогателя **PolyVice** в нескольких атаках может свидетельствовать об участии в Bearlyfy бывших членов группировок, таких как, например, **HelloKitty/FiveHands** и **Vice Society**, атаковавших ранее западные компании. Также в части атак отличались и записки с требованиями выкупа, например в некоторых из них злоумышленники называли себя **Labubu**.

Описание типовой атаки Bearlyfy/Labubu

Группировка Bearlyfy проводит атаки по политически мотивированным причинам. В зависимости от профиля атакуемой организации злоумышленники шифруют данные с последующим требованием выкупа, уничтожают их без возможности восстановления либо проводят эксфильтрацию для последующего вымогательства или использования в дальнейших операциях.

На ранних этапах активности злоумышленники демонстрировали низкий уровень технических навыков и активно экспериментировали с различным инструментарием, однако по мере накопления опыта начали отдавать все большее предпочтение легитимным утилитам и стандартным средствам администрирования. В этот период основная цель атак группировки — небольшие компании, соответственно, суммы выкупа были невысоки.

В большинстве случаев Bearlyfy получает доступ к инфраструктуре жертвы за счет компрометации аутентификационных данных, предоставленных подрядчикам, либо непосредственной компрометации инфраструктуры сторонних организаций, имеющих доверенные связи с целевой сетью. Также Bearlyfy получает доступ к целым группам компаний, обладающих сетевой связанностью, при компрометации одной из них. Кроме того, Bearlyfy эксплуатирует публичные приложения систем Bitrix и 1С для получения доступа к сети.

Для повышения привилегий и получения новых аутентификационных данных участники Bearlyfy эксплуатируют уязвимость Zerologon, проводят атаки типа DCSync, а также применяют специализированные инструменты, такие как **Keefarce Reborne**, **XenAllPasswordsPro** и **PowershellKerberos**. Злоумышленники выполняют поиск паролей в различных файлах, помимо прочего, с помощью самописных PowerShell-скриптов и извлекают учетные данные из систем резервного копирования (например, Veeam). Отдельный интерес представляют данные клиентов Telegram на рабочих станциях администраторов. Их компрометация позволяет атакующим похищать сессии и осуществлять дальнейшее наблюдение за жертвами во время атаки или после наступления деструктивной фазы.

Для закрепления в инфраструктуре участники Bearlyfy активно используют различные средства сетевого туннелирования и удаленного доступа: asio5, cloudflared, localtonet, shinysocks, gost, suo5, neo-regeorg, SSH-туннели, решения для удаленного администрирования, такие как **MeshCentral** и **RuDesktop**, а также самописный PowerShell-бэкдор. Со временем участники группировки последовательно перестали загружать в сеть сторонние утилиты и перешли к более активному использованию уже доступного на системах SSH и других штатных механизмов, что позволяет снизить заметность их присутствия и усложнить обнаружение.

Для обхода обнаружения злоумышленники отключают или модифицируют конфигурации средств защиты информации, создают новые учетные записи или изменяют права уже скомпрометированных. При этом злоумышленники не всегда уделяют достаточное внимание этому этапу атаки: при анализе подключений фиксируются реальные имена хостов атакующих, а антивирусные средства регулярно детектируют и блокируют загружаемый ими инструментарий.

Разведка сети и объектов Active Directory осуществляется с использованием утилит **SoftPerfect**, **Network**, **Scanner**, **ADRecon**, а также различных встроенных оснасток Windows. Для горизонтального перемещения по сети преимущественно применяются протоколы RDP и SSH, однако также используются инструменты постэксплуатационных фреймворков **Impacket** и **PsMapExec**, утилиты **PsExec/PaExec** и **Rubeus**. В качестве нетривиального способа перемещения внутри инфраструктуры Bearlyfy применяет внешние обработки для 1С, позволяющие выполнять произвольный код на сервере приложений.

Эксфильтрация данных в рамках атак Bearlyfy осуществляется как через заранее развернутые сетевые туннели, так и посредством различных облачных сервисов обмена данными. Вместе с тем для этих целей применяются специализированные утилиты, например croc, что позволяет гибко организовывать каналы вывода информации за пределы инфраструктуры жертвы.

Финальной стадией большинства атак Bearlyfy становится шифрование данных с помощью программ-вымогателей **LockBit 3.0 (Black)** / **PolyVice** и **Babuk**. В ряде случаев злоумышленники ограничиваются целенаправленной кражей представляющих интерес данных и оставленными бэкдорами для последующего возвращения в инфраструктуру либо передачи доступа другой криминальной группе. Массовый запуск программ-вымогателей в системах осуществляется различными способами: через групповые политики с задачами, задания для программ централизованного управления инфраструктурой, отдельные скрипты, утилиту **PsMapExec**, средствами PowerShell, а также вручную в рамках активных RDP-/SSH-сессий.

3119/TR4CK	
Начало активности	Август 2025 г.
Цель	Шифрование данных и требование выкупа / шифрование данных без возможности восстановления
Жертвы	Компании малого и среднего бизнеса
Сумма выкупа	Предположительно, несколько тысяч долларов
Используемые инструменты	LockBit 3.0 (Black), самописный шифровальщик для Linux/ESXi, BootIce, PsExec

Первые атаки группировки **3119** были обнаружены в августе 2025 года. Злоумышленники используют программу-вымогатель **LockBit 3.0 (Black)** для шифрования машин под управлением Windows. В начале октября была обнаружена другая вариация записки с требованиями выкупа, в ней злоумышленники называют себя **TR4CK**. В арсенале группировки также появился самописный шифровальщик для Linux/ESXi. С большой долей вероятности представители 3119 могут быть связаны с проукраинской группировкой **CyberAnarchySquad** (CAS), так как имя пользователя в социальной сети Twitter и в мессенджере Telegram у администратора CAS заканчивается на 3119. Также CAS использовали 3119 в качестве пароля при публикации базы данных и как расширение зашифрованных файлов при атаке на российские компании в 2024 году.

Детализированная таблица по техникам и процедурам, характерным для проукраинских группировок

Тактика	Техника	Описание
TA0001 Initial Access	**Exploit Public-Facing Application** T1190	Проукраинские группировки эксплуатируют уязвимости публично доступных сервисов, таких как Atlassian Confluence, Zimbra, MS Exchange, JetBrains TeamCity, Bitrix и 1C
	Valid Accounts: Domain Accounts T1078.002	Проукраинские группировки используют действительные учетные записи жертв, купленные на теневых рынках
	External Remote Service T1133	Для доступа к периметру используют публично доступные сервисы жертв, такие как VPN и RDP
	Trusted Relationship T1199	Проукраинские группировки используют действительные учетные записи жертв, добытые в результате атак на поставщиков ИТ-услуг и продуктов
	Phishing: Spearphishing Attachment T1566.001	Проукраинские группировки проводили фишинговые рассылки с вредоносными вложениями, которые загружали вредоносную программу DarkGate
TA0002 Execution	**Windows Management Instrumentation** T1047	Проукраинские группировки используют wmiexec (`wmiexec.exe`) из фреймворка Impacket для выполнения различных команд. Вместе с тем используются командлеты PowerShell, например Get-WMIObject для выполнения команд и WMI-запросов на локальных и удаленных системах
	User Execution: Malicious File T1204.002	Атакующие используют методы социальной инженерии, чтобы вынудить пользователя запустить вредоносный файл из вложения фишингового сообщения

Тактика	Техника	Описание
TA0002 Execution	**Native API** T1106	В используемых атакующими программах применяются функции Native API
	Scheduled Task/Job: T1053.002	Для удаленного запуска проукраинские группировки используют модуль atexec фреймворка CrackMapExec
	Scheduled Task /Job: Scheduled Task T1053.005	Для запуска программ и выполнения команд проукраинские группировки создают задания планировщика Windows
	Command and Scripting Interpreter: PowerShel T1059.001	Для выполнения различных действий проукраинские группировки используют командный интерпретатор Windows (`cmd.exe`) и PowerShell в системах под управлением Windows и оболочку Bash в системах под управлением Unix-подобных ОС
	Command and Scripting Interpreter: Windows Command Shell T1059.003	
	Command and Scripting Interpreter: Unix Shell T1059.004	
	System Services: Service Execution T1569.002	Проукраинские группировки используют утилиты PsExec из пакета Sysinternals и smbexec (`smbexec.exe`) из фреймворка Impacket для выполнения различных команд, сценариев и исполняемых файлов
TA0003 Persistence	**Scheduled Task/Job: Scheduled Task** T1053.005	Для сохранения доступа к внутреннему периметру жертв проукраинские группировки создают задания планировщика Windows для запуска утилиты Ngrok

Тактика	Техника	Описание
TA0003 Persistence	**Valid Accounts: Domain Accounts** T1078.002	Для сохранения доступа к внутреннему периметру жертв проукраинские группировки используют скомпрометированные легитимные доменные учетные записи
	External Remote Service T1133	Для сохранения доступа к внутреннему периметру жертв проукраинские группировки используют RDP, VPN и почтовые сервисы
	Create Account: Local Account T1136.001	Для сохранения доступа к внутреннему периметру жертв проукраинские группировки создают локальные и доменные учетные записи
	Create Account: Domain Account T1136.002	
	Create or Modify System Process: Windows Service T1543.003	Для сохранения доступа к внутреннему периметру жертв проукраинские группировки инсталлируют программу удаленного доступа AnyDesk в качестве службы, а также создают службы для закрепления Cobint
	Hijack Execution Flow: Dynamic Linker Hijacking T1574.006	В системах под управлением ОС Linux атакующие используют руткит Facefish, который загружается посредством LD_PRELOAD (`/etc/ld.so.preload`)
	Server Software Component: Web Shell T1505.003	Для сохранения доступа к внутреннему периметру жертв проукраинские группировки используют веб-шелл Godzilla, размещаемый на публично доступных веб-серверах
	Boot or Logon Autostart Execution: Registry Run Keys T1547.001	Для сохранения доступа к внутреннему периметру жертв проукраинские группировки используют ключи автозапуска реестра для запуска бэкдоров

Тактика	Техника	Описание
TA0004 Privilege Escalation	**Exploitation for Privilege Escalation** T1068	Проукраинские группировки эксплуатируют уязвимости ОС Windows CVE-2020-1472 (Zerologon), CVE-2021-40449, CVE-2022-21882, CVE-2022-21999, CVE-2023-21746 для повышения привилегий
	Scheduled Task/Job: Scheduled Task T1053.005	Для запуска загруженных инструментов и программ-вымогателей с привилегиями NT SYSTEM проукраинские группировки используют задания планировщика Windows
	Create or Modify System Process: Windows Service T1543.003	Для повышения привилегий и выполнения команд с привилегиями NT SYSTEM проукраинские группировки создают службы одноразового выполнения
	Valid Accounts: Domain Accounts T1078.002	Для повышения привилегий проукраинские группировки используют скомпрометированные легитимные доменные и локальные учетные записи с высоким уровнем привилегий
	Valid Accounts: Domain Accounts T1078.003	
TA0005 Defense Evasion	**Masquerading: Masquerade Task or Service** T1036.004	Проукраинские группировки маскируют имена заданий планировщика и служб Windows под продукты Intel, Microsoft и др.
	Masquerading: Match Legitimate Name or Location T1036.005	Проукраинские группировки маскируют имена файлов, скриптов, приложений под продукты таких компаний, как Intel, Microsoft, VMware и т. п. Также под официальную программу VMware злоумышленники маскируют разработанную ими программу `vcenter_run.exe`. Некоторые загружаемые инструменты проукраинские группировки размещают по путям, схожим с системными и прикладными программами различных вендоров. Наряду с программами имена доменов маскируются под ресурсы Microsoft, Kaspersky, Positive Technologies и др.

Тактика	Техника	Описание
TA0005 Defense Evasion	**Indicator Removal: Clear Windows Event Logs** T1070.001	Проукраинские группировки очищают журналы событий Windows
	Indicator Removal on Host: File Deletion T1070.004	Проукраинские группировки удаляют свои утилиты, скрипты, а также результаты их работы из каталогов `%PUBLIC%`, `%PUBLIC%\Temp`, `%PROGRAMDATA%`, `%USERPROFILE%\Desktop` и т. д.
	Valid Accounts: Domain Accounts T1078.002	Проукраинские группировки используют легитимные доменные учетные записи пользователей
	Domain Policy Modification: Group Policy Modification T1484.001	Проукраинские группировки используют PowerShell-скрипт gpo.ps1 для внесения изменений в групповые политики с целью нейтрализации средств защиты
	Modify Registry T1112	Созданная с помощью PowerShell-скрипта gpo.ps1 групповая политика модифицирует в системах домена параметры системного реестра, связанные с WinRM, Windows Defender, Windows Firewall и др.
	Use Alternate Authentication Material: Pass the Hash T1550.002	При отсутствии аутентификационных данных в явном виде и во избежание обнаружения проукраинские группировки используют скомпрометированные NTLM-хеши привилегированных пользователей для прохождения аутентификации в домене Windows
	Impair Defenses: Disable or Modify Tools T1562.001	Проукраинские группировки отключают встроенные средства защиты, а также антивирусные средства сторонних разработчиков, изменяют их настройки, в том числе и списки исключений

Тактика	Техника	Описание
TA0005 Defense Evasion	**Impair Defenses: Disable or Modify System Firewall** T1562.004	Атакующие отключают брандмауэр Windows
	Reflective Code Loading T1620	Для запуска на хосте бэкдора Cobint используется шелл-код из скрипта PowerShell и программа-установщик ReflectiveLoader. Также используется выполнение сборок .NET непосредственно в памяти
TA0006 Credential Access	**Credentials from Password Stores: Credentials from Web Browsers** T1555.002	Проукраинские группировки используют утилиты XenAllPasswordPro и ff_grab, позволяющие извлекать пароли пользователей из множества программ, таких как почтовые клиенты, браузеры, FTP-клиенты и др.
	Credentials from Password Stores: Windows Credential Manager T1555.004	Проукраинские группировки используют утилиты XenAllPasswordPro и Mimikatz для извлечения аутентификационных данных из диспетчера учетных данных Windows
	Credentials from Password Stores: Password Managers T1555.005	Атакующие экспортируют данные, хранимые в парольных менеджерах KeePass, Passwork и др.
	OS Credential Dumping: LSASS Memory T1003.001	Проукраинские группировки используют утилиту ProcDump для получения дампа процесса `lsass.exe` и извлекают данные из `lsass.exe` программой Mimikatz
	OS Credential Dumping: NTDS T1003.003	Проукраинские группировки используют утилиту Windows ntdsutil для создания копии базы данных NTDS.dit. Для извлечения NTLM-хешей паролей из БД Active Directory используется утилита Secretsdump

Тактика	Техника	Описание
TA0006 Credential Access	**OS Credential Dumping: DCSync** T1003.006	Проукраинские группировки проводят атаки DCSync при помощи Mimikatz
	Unsecured Credentials: Credentials in Files T1552.001	Проукраинские группировки ищут и извлекают аутентификационные данные из различных текстовых и конфигурационных файлов. Проукраинские группировки копируют токены авторизованных Telegram-сессий с систем жертвы. Проукраинские группировки используют скрипт Veeam-Get-Creds.ps1 для извлечения диспетчера учетных данных Veeam Backup and Replication
	Unsecured Credentials: Bash History T1552.001	Проукраинские группировки ищут и извлекают аутентификационные данные из истории выполненных команд оболочек Unix-подобных систем
TA0007 Discovery	**Network Service Discovery** T1046	Для разведки сетевой инфраструктуры жертвы атакующие используют сетевые сканеры Slitheris Network Discovery, PingCastle, fscan, NetScan
	Account Discovery: Local Account T1087.001	Для сбора и изучения сведений о локальных и доменных группах, а также об их принадлежности к тем или иным группам проукраинские группировки используют команды `whoami`, `net user`, `net group`, `net localgroup`, а также инструменты ADRecon, PowerView, adPEAS
	Account Discovery: Domain Account T1087.002	
	Permission Groups Discovery: Local Groups T1069.001	

Тактика	Техника	Описание
TA0007 Discovery	**Permission Groups Discovery: Domain Groups** T1069.002	Для сбора и изучения сведений о локальных и доменных группах, а также об их принадлежности к тем или иным группам проукраинские группировки используют команды `whoami`, `net user`, `net group`, `net localgroup`, а также инструменты ADRecon, PowerView, adPEAS
	Domain Trust Discovery T1482	Для сбора и изучения сведений о доверительных отношениях между доменами проукраинские группировки используют утилиту Windows nltest.exe, а также скрипт ADRecon
	Remote System Discovery T1018	Для получения информации об удаленных системах атакующие используют сетевые сканеры Slitheris Network Discovery, Advanced IP Scanner, fscan.
	Process Discovery T1057	Для сбора и изучения сведений о системах, инсталлированных программах и запущенных процессах атакующие используют скрипт PowerShell SA.ps1 и инструмент PowerView
	System Information Discovery T1082	
	Software Discovery T1518	
	System Owner/User Discovery T1033	Проукраинские группировки собирают и изучают сведения о владельцах систем, а также о вошедших в целевую систему пользователях.
	System Network Configuration Discovery: Internet Connection Discovery T1016.001	Проукраинские группировки собирают и изучают сведения о сетевых подключениях целевых систем, о наличии смежных подсетей, а также проверяют доступность целевых систем к сети Интернет

Тактика	Техника	Описание
TA0007 Discovery	**System Network Connections Discovery** T1049	Для сбора и изучения сведений о сетевых подключениях проукраинские группировки используют команду net use
	File and Directory Discovery T1083	Проукраинские группировки изучают содержимое каталогов локальных смонтированных сетевых дисков, а также различных каталогов удаленных систем, как правило, с помощью проводника Windows, а также команд оболочек bash и cmd
	Network Share Discovery T1135	
	Log Enumeration T1654	Проукраинские группировки используют PowerShell-скрипт Get-RDPLogs.ps1 (rdp.ps1, rdplogs.ps1) для сбора и изучения записей журналов событий с контроллеров доменов и с прочих серверов с целью поиска рабочих станций пользователей с наивысшими привилегиями
TA0008 Lateral Movement	**Remote Services: Remote Desktop Protocol** T1021.001	Атакующие используют RDP для продвижения по сети
	Remote Services: SMB/ Windows Admin Shares T1021.002	Для перемещений по SMB проукраинские группировки используют утилиты Sysinternals Psexec, Impacket SMBExec
	Remote Services: SSH T1021.004	Для перемещений с использованием SSH проукраинские группировки используют SSH-клиентов PuTTY и SSH
	Remote Services: Windows Remote Management T1021.006	Для перемещений по протоколу WinRM атакующие используют командлет Enter-PSSession и Invoke-Command

Тактика	Техника	Описание
TA0008 Lateral Movement	**Exploitation of Remote Services** T1210	Проукраинские группировки эксплуатируют уязвимости Zerologon (CVE-2020-1472) и EternalBlue (CVE-2017-0144) для перемещения в уязвимые системы
	Use Alternate Authentication Material: Pass the Hash T1550.002	Проукраинские группировки перемещаются в инфраструктуре с использованием скомпрометированных NTLM-хешей паролей легитимных пользователей
	Lateral Tool Transfer T1570	При перемещениях по узлам инфраструктуры проукраинские группировки копируют необходимый инструментарий в каталоги `%Public%`, `%Public%\Temp`, `%systemroot%\Logs`, `%ProgramData%` и реже `%userprofile%\Desktop`, `%userprofile%\Downloads`
TA0009 Collection	**Data from Local System** T1005	Проукраинские группировки ищут и собирают интересующие их данные с локальных и сетевых хранилищ, а также из баз данных
	Data from Network Shared Drive T1039	
	Data from Information Repositories T1213	Проукраинские группировки ищут и собирают интересующие их данные, хранимые в различных информационных системах, таких как Confluence, wiki и т. п.
	Archive Collected Data: Archive via Utility T1560.001	Для сжатия собранных конфиденциальных данных проукраинские группировки используют как встроенные архиваторы Windows, так и имеющиеся в системах сторонние
	Recovered Data	Проукраинские группировки могут восстанавливать удаленные данные и искать в них интересующую информацию. Для этого используются программы Recuva, GiliSoft Data Recovery и Wise Data Recovery

Тактика	Техника	Описание
TA0011 Command And Control	**Application Layer Protocol: Web Protocols** T1071.001	Применяемый атакующими фреймворк постэксплуатации Cobint использует для взаимодействия с C2 протоколы HTTP, HTTPS
	Data Encoding: Standard Encoding T1132.001	Фреймворк постэксплуатации Cobint использует кодирование Base64
	Data Encoding: Non-Standard Encoding T1132.002	ВПО DarkGate использует Base64 с нестандартной таблицей символов
	Encrypted Channel T1573	Проукраинские группировки используют для удаленного доступа к скомпрометированным системам Cobint, Facefish, AnyDesk, которые осуществляют асимметричное/симметричное шифрование канала связи с C2
	Ingress Tool Transfer T1105	После получения первоначального доступа проукраинские группировки загружают набор инструментов, необходимых для дальнейшего развития атаки. Атакующие копируют набор необходимых утилит и скриптов в каталоги `%Public%`, `%Public%\Temp`, `%Systemroot%` и `%Systemroot%\System32`
	Remote Access Software T1219	Для удаленного доступа к скомпрометированной инфраструктуре проукраинские группировки используют программу удаленного доступа (RAT) AnyDesk
	Protocol Tunneling T1572 **Proxy** T1090	Для доступа к скомпрометированной системе атакующие используют туннели, построенные с использованием Ngrok и revsocks

Тактика	Техника	Описание
TA0010 Exfiltration	**Exfiltration Over Web Service: Exfiltration to Cloud Storage** T1567.002	Атакующие загружают похищенные данные на облачные хранилища данных (Mega[.]io, gofile[.]io, dropmefiles[.]net и др.). В зависимости от объема данных злоумышленники осуществляют эксфильтрацию с помощью веб-браузеров либо программы Rclone
	Exfiltration Over C2 Channel T1041	Некоторые похищенные данные направлялись по каналам взаимодействия с управляющим сервером Cobint. Эксфильтрацию информации малого объема проукраинские группировки проводят через буфер обмена во время активных RDP-сессий
	Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Non-C2 Protocol T1048.002	Эксфильтрация больших объемов информации проводится проукраинскими группировками с помощью утилиты Rclone. Данные передаются по протоколу SFTP на подконтрольные атакующим ресурсы
TA0040 Impact	**Inhibit System Recovery** T1490	Атакующие осуществляли удаление теневых копий томов, отключали возможности восстановления систем Windows, а также удаляли резервные копии систем
	Account Access Removal T1531	Проукраинские группировки скриптами PowerShell меняют пароли учетных записей root на гипервизорах ESXi. В случаях обнаружения специалистами жертвы вредоносной активности на заключительном этапе проукраинские группировки могут поменять пароли всех учетных записей домена
	System Shutdown/Reboot T1529	Атакующие могут отключать системы администраторов скриптами PowerShell

Тактика	Техника	Описание
TA0040 Impact	**Data Destruction** T1485	Атакующие создают задачи на удаление бэкапов при помощи систем управления резервного копирования. В некоторых атаках для уничтожения данных использовалась программа-вайпер Endurance-Wiper
	Disk Wipe: Disk Content Wipe T1561.001	Проукраинские группировки используют утилиту BOOTICE для очистки содержимого дискового пространства методом принудительной перезаписи случайными данными хранилищ резервных копий
	Defacement: Internal Defacement T1491.001	В некоторых атаках злоумышленники меняют обои рабочего стола хостов и выводят текст с требованием выкупа на принтеры
	Data Encrypted for Impact T1486	Для шифрования данных в Windows-системах злоумышленники используют программу-вымогатель LockBit 3.0 (Black) / Poly Vice, для шифрования данных в Linux-системах — программу-вымогатель Babuk

Восточные группировки

Mimic Ransom	
Начало активности	Июнь 2022 г.
Цель	• Шифрование данных и требование выкупа. • Атакующие не похищают данные жертвы и не имеют сайта утечек (DLS)
Жертвы	Преимущественно компании малого бизнеса
Сумма выкупа	Средняя сумма выкупов злоумышленников, как правило, составляет до 100 тыс. руб. за один хост и до 300 тыс. руб. за сервер
Получение первоначального доступа	Скомпрометированные службы удаленного доступа, преимущественно публично доступный RDP (Remote Desktop Protocol)
Используемые инструменты	Mimic

Mimic — программа-вымогатель, появившаяся в июне 2022 года. По мнению специалистов F6, программа-вымогатель Mimic — одна из самых сложных современных программ-вымогателей. Mimic попадает на компьютер жертвы в виде самораспаковывающегося 7-Zip-архива (7-Zip SFX). Шифрование данных осуществляется с помощью алгоритма потокового шифрования ChaCha20. Для получения ключа ChaCha20 используется реализация протокола Диффи — Хеллмана на эллиптических кривых (ECDH) X25519. В отличие от других программ-вымогателей, Mimic не генерирует на хосте сессионные ключи, шифруя затем сессионный закрытый ключ с помощью открытого мастер-ключа, а использует в качестве сессионного ключа случайно выбранный из готового набора, содержащегося в коде шифровальщика. Для проведения массовых атак программа-вымогатель Mimic содержит большое количество сессионных ключей. С большой долей вероятности Mimic используют для атак несколько групп. Все атакованные Mimic цели по-прежнему либо физические лица, либо небольшие коммерческие организации. Злоумышленники также начали активно использовать мессенджеры TOX и Jabber для общения с жертвами.

Proton/Shinra	
Начало активности	Март 2023 г.
Цель	• Шифрование данных и требование выкупа. • Атакующие не похищают данные жертвы и не имеют сайта утечек (DLS)
Жертвы	Преимущественно компании малого бизнеса
Сумма выкупа	В среднем $4500–5000
Получение первоначального доступа	Скомпрометированные службы удаленного доступа, преимущественно публично доступный RDP (Remote Desktop Protocol)
Используемые инструменты	Proton, Mimikatz, Process Hacker, Sysinternals

Proton — написанный на C++ аналог шифровальщика LokiLocker/Blackbit. Аналогично LokiLocker/BlackBit, Proton в ранних версиях при запуске проверял наличие установленной раскладки клавиатуры fa-IR (персидская клавиатура). Все больше партнеров восточных группировок выбирают именно Proton взамен LokiLocker/Blackbit. Атаки с использованием данного шифровальщика наблюдались на протяжении всего 2025 года, преимущественно жертвами стали компании малого бизнеса. **Shinra**, ветвь развития Proton, обнаруженная в апреле 2024 года, также активна и используется параллельно различными партнерами.

Sauron	
Начало активности	Октябрь 2024 г.
Цель	• Шифрование данных и требование выкупа. • Атакующие не похищают данные жертвы и не имеют сайта утечек (DLS)
Жертвы	Компании среднего и малого бизнеса
Сумма выкупа	Как правило, несколько тысяч долларов
Получение первоначального доступа	Скомпрометированные службы удаленного доступа, преимущественно публично доступный RDP (Remote Desktop Protocol)
Используемые инструменты	Sauron

Sauron — программа-вымогатель, впервые обнаруженная в октябре 2024 года, разработанная на основе исходного кода **Conti 3** и имеющая схожие концептуальные черты с семейством Proxima. Новые версии Sauron, как и Proton/Shinra, стали шифровать имена файлов. Как только процесс шифрования завершается, Sauron меняет обои на рабочем столе и отправляет сообщение с требованием выкупа. В 2025 году также наблюдался небольшой спад активности.

C77L	
Начало активности	Март 2025 г.
Цель	• Шифрование данных и требование выкупа. • Атакующие не похищают данные жертвы и не имеют сайта утечек (DLS)
Жертвы	Преимущественно компании малого бизнеса
Сумма выкупа	Как правило, несколько тысяч долларов
Получение первоначального доступа	Скомпрометированные службы удаленного доступа, преимущественно публично доступный RDP (Remote Desktop Protocol)
Используемые инструменты	C77L

C77L — группировка, использующая для своих атак программу-вымогатель и активная как минимум с конца марта 2025 года. Как и в других восточных RaaS-сервисах, в контексте данной группировки используются разнообразные варианты программы-вымогателя. Российские компании атакуют преимущественно варианты **C77L** и **X77C**. Предположительно, группировка C77L появилась в результате разделения партнерской программы Proton. Для шифрования файлов позаимствована концепция Phobos по использованию сессионных ключей AES. Атакует мелкие коммерческие предприятия или физических лиц.

BlackFL/BlackHunt	
Начало активности	Ноябрь 2022 г.
Цель	• Шифрование данных и требование выкупа. • Атакующие не похищают данные жертвы и не имеют сайта утечек (DLS)
Жертвы	Компании среднего и малого бизнеса
Сумма выкупа	Как правило, несколько тысяч долларов
Получение первоначального доступа	Скомпрометированные службы удаленного доступа, преимущественно публично доступный RDP (Remote Desktop Protocol)
Используемые инструменты	BlackHunt, Risen, LockBit 3 Black, Babuk, Proxima, Surtr, Conti v3, Cobalt Strike

BlackFL/BlackHunt — восточная партнерская программа, активная как минимум с 2022 года. Изначально атакующие использовали для шифрования данных программы-вымогатели BlackHunt и Risen. С начала 2025 года атакующие стали именоваться BlackFL, арсенал группировки при этом значительно расширился: **LockBit 3.0 (Black)**, **Babuk**, **Proxima**, **Surtr**, модификация **Conti v3**. Цели группировки — предприятия малого и среднего бизнеса по всему миру. Атакующие активно используют фреймворк постэксплуатации **Cobalt Strike**. BlackFL/BlackHunt — одна из немногих восточных группировок, атакующих Linux-системы. В самом начале 2025 года BlackFL/BlackHunt атаковали российскую медицинскую организацию.

PE32	
Начало активности	Январь 2025 г.
Цель	• Шифрование данных и требование выкупа. • Атакующие не похищают данные жертвы и не имеют сайта утечек (DLS)
Жертвы	Компании среднего и малого бизнеса
Сумма выкупа	От $700 до $7000 за сервер и от $10 000 до более чем 2 BTC за компанию
Получение первоначального доступа	Скомпрометированные службы удаленного доступа, преимущественно публично доступный RDP (Remote Desktop Protocol)
Используемые инструменты	PE32Mimikatz, NirSoft, Advanced Port Scanner, SoftPerfect Network Scanner, PsExec, Process Hacker

PE32 — персидское семейство программ-вымогателей, написанное на Rust и активное как минимум с января 2025 года. В программе-вымогателе PE32, помимо использования Rust для разработки, реализована одна из самых сложных схем шифрования наподобие Mimic и Secles. PE32 — это первая известная программа-вымогатель, которая стала использовать для шифрования файлов стандарт постквантовой криптографии ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism).

В качестве вектора атаки партнеры PE32 в основном используют уязвимые публично доступные службы удаленного доступа, и прежде всего это RDP (Remote Desktop Protocol). Сумма выкупа составляет от **$700** до **$7000** за сервер и от **$10 000** до более чем **2BTC** за компанию (зависит от размера данных и самой компании).

LokiLocker/BlackBit	
Начало активности	Август 2021 г.
Цель	• Шифрование данных и требование выкупа. • Атакующие не похищают данные жертвы и не имеют сайта утечек (DLS)
Жертвы	Компании среднего и малого бизнеса
Сумма выкупа	• $10 000 — 100 000 • Конечная сумма выкупа зависит от количества приобретаемых жертвой декрипторов (декриптор расшифровывает данные на одном хосте)
Получение первоначального доступа	Скомпрометированные службы удаленного доступа, преимущественно публично доступный RDP (Remote Desktop Protocol)
Используемые инструменты	BlackBit, AccountCrack, Mimikatz, NirSoft, Advanced Port Scanner Process Hacker 2, Revo Uninstaller

LokiLocker/BlackBit — это группа шифровальщиков, которая была обнаружена в августе 2021 года. LokiLocker/BlackBit шифрует данные с помощью AES-256 в режиме GCM (счетчик с аутентификацией Галуа), а ключ затем шифруется с помощью открытого RSA ключа жертвы. Стоит отметить, что на протяжении всего 2025 года активность группировки была невысокой. Вполне вероятно, что это связано с появлением конкурента в виде Proton и его вариаций.

Enmity/Mammon	
Начало активности	Апрель 2023 г.
Цель	• Шифрование данных и требование выкупа. • Атакующие не похищают данные жертвы и не имеют сайта утечек (DLS)
Жертвы	Компании среднего и малого бизнеса
Сумма выкупа	От $3000 до $10 000 за расшифровку одного сервера и от $20 000 до 2 BTC за расшифровку всех компьютеров
Получение первоначального доступа	Скомпрометированные службы удаленного доступа, преимущественно публично доступный RDP (Remote Desktop Protocol)
Используемые инструменты	Enmity

Enmity — это программа-вымогатель, впервые обнаруженная в апреле 2023 года и активная на протяжении всего 2024 года. По имеющимся данным, злоумышленники запрашивают от **$3000** до **$10 000** за расшифровку одного сервера и от **$20 000** до **2 BTC** за расшифровку всех компьютеров внутри компании. Один из векторов первоначального доступа злоумышленников — подключение через RDP.

Стоит также отметить, что активность данной группировки заметно снизилась в 2025 году, но она продолжает свою деятельность и разрабатывает новые версии программ-вымогателей. Так, в августе 2025 года были обнаружены образцы новой версии — **MoonLight**.

HsHarada	
Начало активности	Декабрь 2022 г.
Цель	• Шифрование данных и требование выкупа. • Атакующие не похищают данные жертвы и не имеют сайта утечек (DLS)
Жертвы	Компании среднего и малого бизнеса
Сумма выкупа	В среднем $50 000
Получение первоначального доступа	Скомпрометированные службы удаленного доступа, преимущественно публично доступный RDP (Remote Desktop Protocol)
Используемые инструменты	HsHarada, Cobalt Strike, Godzilla Webshell, Meterpreter

HsHarada/Rapture — это семейство программ-вымогателей, впервые обнаруженное 31 декабря 2022 года, является дальнейшей ветвью развития программы-вымогателя **Ghost** (**Cring**). Свое название HsHarada получила по одному из адресов электронной почты, который используется злоумышленниками в записке с требованием выкупа. Преступники шифруют файлы жертвы, а затем требуют выкуп, который обычно выплачивается в криптовалюте Monero, ориентированной на конфиденциальность, что усложняет процесс отслеживания и атрибуции.

Все файлы, зашифрованные HsHarada, имеют случайное буквенно-цифровое расширение, добавляемое к концу имени файла с зашифрованными данными. Это же расширение добавляется и к названию записки о выкупе.

HsHarada в качестве первоначального вектора зачастую использует старые уязвимости серверов Exchange. Их атаки характеризуются высокой быстротечностью, время от получения первоначального доступа до старта процесса шифрования может составлять не более 2 часов.

На протяжении 2025 года HsHarada проявляла довольно низкую активность. В одной из атак на российскую компанию весной 2025 года злоумышленники получили первоначальный доступ через скомпрометированную учетную запись (подключившись через RDP) и в дальнейшем перемещались в системе жертвы через RDP. Запрошенный выкуп составил **$35 000**.

Описание типовой атаки восточных группировок

Получение первоначального доступа

В качестве начального вектора атак злоумышленниками преимущественно используются скомпрометированные службы удаленного доступа (T1133), и прежде всего это RDP.

Для получения доступа к терминальному серверу атакующие могут использовать подбор имени пользователя и пароля (T1110). Также корректные учетные данные (T1078) могут быть приобретены у других злоумышленников, например в андеграунде у брокеров начального доступа.

Подготовка к развитию атаки

Получив первоначальный доступ, атакующие копируют на скомпрометированный хост набор инструментов или его часть (T1105), а также стремятся закрепиться и получить доступ к привилегированным учетным данным, чтобы иметь возможность продвигаться по сети.

Для получения привилегированных учетных данных атакующие используют популярную легитимную утилиту **Mimikatz** (T1003). Некоторые партнеры использовали утилиты **NirSoft** для извлечения паролей.

Для получения списка пользователей в Active Directory (T1087) некоторые партнеры пользовались .NET-утилитой **LoginParser**.

Для подбора паролей к учетным данным (T1110) атакующие используют различные сборки .NET- утилиты **AccountRestore**.

Сбор информации об ИТ-инфраструктуре

Для разведки сети (T1018, T1046) атакующие используют следующие сетевые сканеры:

- **Advanced Port Scanner,**
- **SoftPerfect Network Scanner.**

Злоумышленники применяют различные версии консольной утилиты NS для сканирования общих ресурсов сети (Shares) (T1135) и подключения их как сетевых дисков, а также монтирования скрытых томов.

Для поиска файлов и папок атакующие использовали утилиту **Everything**. Это производилось прежде всего для поиска аутентификационных данных, сохраненных в текстовых файлах (T1552).

Продвижение по сети

Для продвижения по сети партнеры используют RDP (T1021.001) и учетные данные, которые были похищены или получены в результате успешного перебора паролей (brute force) (T1110).

Развертывание программы-вымогателя

Атакующие предварительно отключают антивирусное программное обеспечение до развертывания программы-вымогателя (T1562.001).

Для нейтрализации средств безопасности атакующие могут использовать следующие легитимные утилиты:

- **Process Hacker,**
- **KAV Removal Tool,**
- **ESET AV Remover,**
- **IObit Unlocker,**
- **Revo Uninstaller.**

Распространение программы-вымогателя по ИТ-инфраструктуре жертвы производилось атакующими преимущественно вручную (T1570).

Детализированная таблица по техникам и процедурам, характерным для восточных группировок

Тактика	Техника	Описание
TA0001 Initial Access	**External Remote Services** T1133	В качестве первоначального доступа атакующие преимущественно используют публично доступный RDP
	Valid Accounts T1078	Злоумышленники использовали для получения доступа скомпрометированные учетные данные
TA0002 Execution	**Command and Scripting Interpreter: Windows Command Shell** T1059.003	Атакующие используют Windows Command Shell для выполнения различных действий
TA0003 Persistence	**Valid Accounts** T1078	Полученные атакующими легитимные учетные записи используются для закрепления в скомпрометированной инфраструктуре
	Create Account T1136	Некоторые партнеры для закрепления в системе создавали привилегированные учетные записи
TA0004 Privilege Escalation	**Valid Accounts** T1078	Атакующими для повышения привилегий используются легитимные учетные данные с правами администратора. Существующие учетные данные администратора домена использовались злоумышленниками для продвижения по сети

Тактика	Техника	Описание
TA0005 Defense Evasion	**Impair Defenses: Disable or Modify Tools** T1562.001	Атакующие используют различные легитимные утилиты для нейтрализации средств безопасности: • Process Hacker (`PH.exe`); • KAV Removal Tool (`KAVREMVR.exe`); • ESET AV Remover (`avremover_nt32_enu.exe, avremover_nt64_enu.exe`); • IObit Unlocker (`unlocker-setup.exe`); • Revo Uninstaller (`RevoUninProSetup.exe`)
	Indicator Removal on Host: Clear Windows Event Logs T1070.001	Атакующие очищают журналы событий Windows (Event Logs) на скомпрометированном хосте
	Indicator Removal: File Deletion T1070.004	Атакующие удаляют после использования свои ранее загруженные на хост инструменты
TA0006 Credential Access	**OS Credential Dumping** T1003	Для получения привилегированных учетных данных атакующие используют популярную легитимную утилиту Mimikatz
	Unsecured Credentials T1552	Некоторые партнеры использовали для извлечения паролей утилиты NirSoft RouterPassView, PstPassword, VNCPassView. Также некоторые атакующие использовали утилиту Everything для поиска аутентификационных данных в текстовых файлах
	Credentials from Password Stores: Credentials from Web Browsers T1555.003	Некоторые партнеры использовали для извлечения паролей утилиты NirSoft OperaPassView, WebBrowserPassView
	Credentials from Password Stores: Windows Credential Manager T1555.003	Некоторые партнеры использовали для извлечения паролей утилиту NirSoft CredentialsFileView

Тактика	Техника	Описание
TA0006 Credential Access	**Brute Force** T1110	Злоумышленники используют подбор паролей для получения доступа
TA0007 Discovery	**Remote System Discovery** T1018	Для получения информации об удаленных системах атакующие используют сетевые сканеры Advanced Port Scanner, SoftPerfect Network Scanner
	Network Service Scanning T1046	Для сканирования открытых портов в сети атакующие используют сетевые сканеры Advanced Port Scanner, SoftPerfect Network Scanner
	Account Discovery T1087	Для получения списка пользователей в Active Directory некоторые партнеры пользовались утилитой LoginParser
	Network Share Discovery T1135	Атакующие используют различные версии консольной утилиты NS для сканирования общих ресурсов сети
	File and Directory Discovery T1083	Для получения информации о файлах и каталогах некоторые партнеры использовали утилиту Everything
TA0008 Lateral Movement	**Remote Services: Remote Desktop Protocol** T1021.001	Атакующие использовали RDP для дальнейшего продвижения по сети
	Lateral Tool Transfer T1570	При продвижении внутри сети жертвы и развертывании программы-вымогателя атакующие осуществляют копирование на хост необходимого набора инструментов
TA0011 Command and Control	**Ingress Tool Transfer** T1105	После получения первоначального доступа атакующие копируют на скомпрометированный хост набор необходимых инструментов

Тактика	Техника	Описание
TA0040 Impact	**Data Destruction** T1485	Атакующие с помощью программы-вымогателя после истечения 30-дневного срока выплаты выкупа могут уничтожить все данные на скомпрометированных хостах
	Data Encrypted for Impact T1486	Атакующие используют программы-вымогатели для шифрования файлов на скомпрометированных хостах с целью получения выкупа

Другие атакующие, использующие программы-вымогатели

Masque	
Начало активности	Январь 2024 г.
Цель	Шифрование данных и требование выкупа
Жертвы	Преимущественно компании малого и среднего бизнеса
Сумма выкупа	$50 000 — 100 000
Получение первоначального доступа	Уязвимости в публично доступных сервисах
Используемые инструменты	LockBit 3.0 (Black), Babuk, AnyDesk, Mimikatz, ProcDump, PsExec, SMBexec, Chisel, MystiqueLoader, XenAllPasswordPro, Localtonet

Masque — русскоязычная группировка, появившаяся в январе 2024 года и использующая для атак программу-вымогатель **LockBit 3.0 (Black)** и модификацию **Babuk**. Записка о требовании выкупа составлена только на русском языке. Это свидетельство того, что группировка нацелена на российские компании. В большинстве случаев начальный вектор атаки Masque — компрометация публично доступных сервисов, таких как VMware Horizon, через эксплуатацию уязвимости CVE-2021-44228 (Log4Shell) в библиотеке Log4j, несмотря на то что с момента ее обнаружения прошло значительное время. После успешной эксплуатации уязвимости атакующие используют скомпрометированный

сервер в качестве плацдарма для дальнейшего развития атаки. В самой записке о выкупе нет никаких деталей, кроме контактов злоумышленников в мессенджере qTox.

В 2025 году группировка продолжила стабильно атаковать российские компании. В некоторых атаках после отказа жертвы от выплаты выкупа злоумышленники создавали Telegram-канал, где активно публиковали данные о компании и ее сотрудниках. Также атакующие похищали Telegram-аккаунты некоторых сотрудников пострадавшей компании и меняли на них облачные пароли.

OldGremlin	
Начало активности	Март 2020 г.
Цель	Шифрование данных и требование выкупа
Жертвы	Преимущественно компании малого и среднего бизнеса
Сумма выкупа	В среднем несколько миллионов долларов
Получение первоначального доступа	Уязвимости в публично доступных сервисах
Используемые инструменты	TinyFluff, TinyCrypt, TinyIsolator, TinyLink, TinyNode, TinyHTA, TinyKiller, OldGremlin.JsDownloader

OldGremlin — русскоязычная хакерская группировка, впервые обнаруженная в марте 2020 года и атакующая исключительно российские компании. Всего за свой первый период активности (с марта 2020-го по сентябрь 2022 года) хакеры провели 16 вредоносных кампаний с целью получения выкупа за расшифровку данных. В 2021 году группа требовала у жертвы **250 млн руб.** за восстановление доступа к данным. В 2022 году ценник поднялся до **1 млрд руб.** В 2025 году группировка по-прежнему активна, известно как минимум о нескольких жертвах, которыми стали российские компании. Также специалистами F6 были обнаружены новые утилиты — версии **TinyKiller** и **TinyIsolator**.

Pay2Key	
Начало активности	Март 2025 г.
Цель	Шифрование данных и требование выкупа
Жертвы	Преимущественно компании малого и среднего бизнеса
Сумма выкупа	В среднем несколько тысяч долларов
Получение первоначального доступа	Фишинговые вложения и ссылки в письмах
Используемые инструменты	Pay2Key (Mimic)

Pay2Key — RaaS-сервис с одноименной программой-вымогателем, активный как минимум с февраля 2025 года. Программа-вымогатель **Pay2Key** — отдельная ветвь развития (форк) другого распространенного шифровальщика — **Mimic**. Первое сообщение с рекламой Pay2Key было создано пользователем Isreactive на форуме Gerki. Хотя на многих форумах и запрещено проводить атаки на страны СНГ, начиная с апреля 2025 года специалисты F6 фиксируют фишинговые рассылки на российских пользователей, содержащих **Pay2Key Ransomware**. Как правило, программа-вымогатель доставляется в архиве или пользователь скачивает ее самостоятельно по ссылке из письма. Запрашиваемые суммы выкупа обычно составляют несколько тысяч долларов. В августе-сентябре 2025 года было обнаружено, что злоумышленник **VasyGrek** в своих фишинговых рассылках начал использовать шифровальщик Pay2Key.

Room155	
Начало активности	Декабрь 2022 г.
Цель	Шифрование данных и требование выкупа
Жертвы	Преимущественно компании малого и среднего бизнеса
Сумма выкупа	В среднем несколько тысяч долларов
Получение первоначального доступа	Фишинговые вложения в письмах
Используемые инструменты	XWorm, Revenge-RAT, Darktrack, LockBit 3.0 (Black), AveMaria, DCRat, Stealerium, DCRat, VenomRAT, AnyDesk

Room155 — кибергруппа, действующая как минимум с декабря 2022 года. Злоумышленники рассылают фишинговые письма, в приложении к которым содержится архив с ВПО и документ-приманка. В известных случаях в письмах содержится либо **Revenge RAT**, либо **XWorm**. Шаблоны документов злоумышленники загружают с легитимных российских ресурсов, посвященных финансовой тематике. Согласно обнаруженным данным, злоумышленники шифруют устройства жертв с помощью шифровальщика **LockBit 3.0 (Black)**.

Группа проводила фишинговые рассылки с марта на протяжении всего года. В первой половине 2025 года использовали омоглифы в темах писем, а также двойные расширения у исполняемых файлов. Распространяли как Revenge RAT, так и XWorm. Во второй половине года перестали использовать омоглифы в темах и двойные расширения у файлов. Преимущественно доставляли XWorm. Предположительно, с августа стали указывать в контактах для связи Telegram-аккаунт, помимо почты.

Storm-2603/GOLD SALEM/CL-CRI-1040	
Начало активности	Март 2025 г.
Цель	• Шифрование данных и требование выкупа. • Группировка похищает данные жертвы и публикует их на сайте утечек (DLS) в случае отказа от уплаты выкупа
Жертвы	Компании в телекоммуникационной, финансовой, промышленной, ИТ и государственной отраслях
Сумма выкупа	В среднем от $450 000 до $1 000 000
Получение первоначального доступа	Группировка получает доступ через уязвимые серверы Microsoft SharePoint, используя цепочку эксплойтов ToolShell (CVE-2025-49704, CVE-2025-49706, CVE-2025-53770, CVE-2025-53771)
Используемые инструменты	LockBit 3.0 (Black), Warlock (X2anylock), Babuk, AK47 C2 Framework, Velociraptor, PsExec, Mimikatz, Masscan, SharpHostInfo, WinPcap, NetExec (nxc), Impacket, Visual Studio Code as tunneling tool, Cloudflare Tunnel, Radmin remote administration tool, Wstunnel, Gorilla WebSocket

Первые следы активности **Storm-2603** датируются мартом 2025 года. Группировка атакует организации в странах Северной и Южной Америки, Европы, также были замечены атаки на компании в России.

Известный первоначальный вектор получения доступа — эксплуатация цепочки уязвимостей в SharePoint-серверах (ToolShell), которая приводит к установке веб-шелла. Через этот доступ Storm-2603 выполняет первые команды для разведки и начинает закрепление в системе. Далее злоумышленники загружают и запускают дополнительные инструменты для дальнейшего продвижения в сети:

Mimikatz для кражи учетных данных из памяти **lsass**, **Impacket** и **PsExec** для удаленного выполнения команд и перемещения между хостами, а также **Masscan** и **SharpHostInfo** для сетевой разведки. Для удаленного администрирования устанавливались следующие утилиты: **Cloudflare Tunnel**, **Visual Studio Code** с возможностью туннелирования, **Radmin** и кастомный фреймворк **AK47** с возможностью коммуникации как через HTTP, так и через DNS. Атакующие также использовали уязвимую версию Velociraptor в качестве C2, а также для повышения привилегий и загрузки утилит для удаленного доступа. Для обхода средств защиты использовалась техника Bring Your Own Vulnerable Driver (BYOVD): группировка доставляла в систему легитимный, но уязвимый драйвер, и с помощью него из контекста ядра завершала процессы антивирусов.

Завершающий этап операций Storm-2603 — разворачивание шифровальщиков и вымогательство. Группировка использовала как минимум два семейства шифровальщиков: **Warlock** (также известный как **X2anylock/xlockxlock**) и **LockBit 3.0 (Black)**, а в отдельных случаях — **Babuk** для Linux и **VmWare ESXi**. Распространение вредоносного ПО может происходить через групповые политики (GPO), запуск специальных скриптов, а также через DLL sideloading — техники. После шифрования на системах остаются записки с идентификатором жертвы и контактами в виде адресов электронной почты и учетной записи в Tox, через которые операторы Storm-2603 ведут дальнейшие переговоры о выкупе.

В ходе реагирования на инцидент специалистам F6 удалось зафиксировать активность группировки Storm-2603. Через зараженный сервер Microsoft SharePoint злоумышленники загружали Velociraptor, чтобы в дальнейшем использовать его для связи с C2 и загрузки Visual Studio Code с опцией туннелирования. Дополнительно были загружены еще две утилиты для туннелирования трафика — Cloudflare Tunnel и **Wstunnel**. Злоумышленники проводили разведку через команды net, netstat и quser. Также было зафиксировано горизонтальное продвижение по сети через RDP и SMB с использованием утилиты **NetExec** и скомпрометированного NTLM-хеша пароля одного из пользователей.

Детализированная таблица по техникам и процедурам, характерным для других атакующих, использующих программы-вымогатели

Тактика	Техника	Описание
TA0001 Initial Access	**External Remote Services** T1133	В качестве первоначального доступа атакующие преимущественно используют публично доступный RDP
	Spearphishing Attachment T1566.001	
	Valid Accounts T1078	Злоумышленники использовали для получения доступа скомпрометированные учетные данные
TA0002 Execution	**Command and Scripting Interpreter: Windows Command Shell** T1059.003	Атакующие используют Windows Command Shell для выполнения различных действий
	System Services: Service Execution T1569.002	Злоумышленники могут воспользоваться диспетчером управления службами Windows (SCM) для выполнения вредоносных команд или полезных нагрузок. Также используются утилиты PsExec, SBMexec, SDelete
	Scheduled Task/Job: Scheduled Task T1053.005	Атакующие создают задание в планировщике
TA0003 Persistence	**Create Account** T1136	Некоторые злоумышленники для закрепления в системе создавали привилегированные учетные записи
TA0004 Privilege Escalation	**Valid Accounts** T1078	Атакующие для повышения привилегий используют легитимные учетные данные с правами администратора

Тактика	Техника	Описание
TA0005 Defense Evasion	**Impair Defenses: Disable or Modify System Firewall** T1562.004	Атакующие отключают либо добавляют новые правила для антивирусных решений на хостах
	Indicator Removal on Host: Clear Windows Event Logs T1070.001	Атакующие очищают журналы событий Windows (Event Logs) на скомпрометированном хосте
	Indicator Removal: File Deletion T1070.004	Атакующие удаляют после использования свои ранее загруженные на хост инструменты
TA0006 Credential Access	**OS Credential Dumping** T1003	Для получения привилегированных учетных данных атакующие используют популярную легитимную утилиту Mimikatz
	Unsecured Credentials T1552	Злоумышленники используют утилиту **XenAllPasswordsPro** для извлечения паролей из различных программ и приложений
	Brute Force T1110	Некоторые злоумышленники используют подбор паролей для получения доступа
TA0007 Discovery	**Remote System Discovery** T1018	Для получения информации об удаленных системах атакующие используют сетевые сканеры Advanced Port Scanner, SoftPerfect Network Scanner
	Network Service Scanning T1046	Для сканирования открытых портов в сети атакующие используют сетевые сканеры Advanced Port Scanner, SoftPerfect Network Scanner
	Lateral Tool Transfer T1083	Атакующие изучают пользовательские каталоги на разных хостах

Тактика	Техника	Описание
TA0008 Lateral Movement	**Remote Services: Remote Desktop Protocol** T1021.001	Атакующие используют RDP для перемещения внутри инфраструктуры
	Lateral Tool Transfer T1570	При продвижении внутри сети жертвы и развертывании программы-вымогателя атакующие осуществляют копирование на хост необходимого набора инструментов
TA0011 Command and Control	**Ingress Tool Transfer** T1105	После получения первоначального доступа атакующие копируют на скомпрометированный хост набор необходимых инструментов
TA0040 Impact	**Data Encrypted for Impact** T1486	Атакующие используют программы-вымогатели для шифрования файлов на скомпрометированных хостах с целью получения выкупа

Политически мотивированные киберпреступные группы

Несмотря на то что политически мотивированные группы (хактивисты) используют различные методы для реализации атак, всех их объединяет общая идея, тесно связанная с геополитической обстановкой. Группы нацелены на нанесение ущерба, остановку работы ресурсов, простои компаний и организаций. Причем для них характерна публичность: они заявляют в своих социальных сетях и каналах об успешном проведении атак. Тем самым политически мотивированные киберпреступники привлекают к себе больше внимания, а чем громче новости с их упоминанием, тем сильнее эффект устрашения.

Интересные особенности, которые мы заметили в отчетном периоде после публикаций громких новостей об атаках:

- Злоумышленники проводят вредоносные email-рассылки, маскируясь под группировку, совершившую громкую атаку ранее.
- Злоумышленники проводят информационные атаки. Так, например, в конце июля было несколько громких атак, на фоне которых стали появляться и другие сообщения о сбоях в различных организациях. В качестве доказательств были приложены снимки экрана сервиса мониторинга сбоев. Специалисты F6 не выявили сбоя в работе заявленных организаций. В ходе анализа удалось обнаружить однотипные комментарии, добуквенные пересечения и опечатки, а также аномальное количество постов на сервисе мониторинга сбоев. Кроме того, часть пользователей сообщала о «сбоях из-за хакерских атак» за несколько дней до появления новости о проблемах с доступностью сервисов организации, что свидетельствует о вероятных информационных атаках.

Всего четыре группы были замечены за проведением DDoS-атак в 2025 году: **IT Army of Ukraine**, **CyberSec's**, **Himars DDoS**, **Кіберкорпус**. IT Army of Ukraine, как и годом ранее, остается угрозой № 1 по числу DDoS-

атак. На ее фоне у других групп число атак было незначительным. Отметим, что в 2025 году большое внимание эта группировка по-прежнему уделяет атакам на телеком-провайдеров, но также были выявлены атаки и на другие индустрии, включая госсектор, финансы, транспорт, промышленность и ИТ.

В целом фокус политически мотивированных групп смещается на нанесение большего ущерба за счет использования программ-вымогателей. В 2025 году более десяти хактивистских группировок отметились хотя бы одной атакой с использованием программы-вымогателя. Так, например, группировка **4B1D**, появившаяся в феврале 2025 года, атаковала как минимум **9** российских компаний, зашифровав их данные без возможности восстановления. Группировка **BO Team**, в свою очередь, запросила выкуп у атакованной компании в размере **$50 000**, однако после выплаты не предоставила дешифратор.

Жертвами вымогателей чаще всего становились российские инжиниринговые компании и предприятия из сфер оптовой и розничной торговли. Примечательно, что чувствительные данные остаются одной из главных целей политически мотивированных группировок: атакующие сначала похищают информацию и лишь затем шифруют инфраструктуру жертвы.

Проукраинские группировки, нацеленные преимущественно на диверсии и отметившиеся использованием программ-вымогателей:

- **Yellow Drift,**
- **4B1D,**
- **C.A.S. (Cyber.Anarchy.Squad),**
- **RMRF (sudo rm -RF),**
- **DC8044,**
- **BO Team,**
- **Ukrainian Cyber Alliance (U.C.A.),**
- **Хакерський кіт,**
- **SilentCrow,**
- **Belarusian Cyber-Partisans (Киберпартизаны BY).**

Группировки, ориентированные на DDoS-атаки

IT Army of Ukraine

Деятельность **IT ARMY of Ukraine** всегда согласуется с геополитической ситуацией, и 2025 год не стал исключением. Был ряд событий, который «разворачивал» активность группировки в сторону определенных целей. Но телекоммуникационный сектор по-прежнему приоритетная цель группы. В 2025 году атакам со стороны IT ARMY of Ukraine было подвержено более 100 интернет-провайдеров, причем, помимо операторов в городах-миллионниках, цели были и в небольших городах в разных уголках страны. Такая нацеленность легко объяснима, ведь атака на провайдера парализует работу его клиентов и заметна большому количеству пользователей. В частности, были атакованы операторы в Москве и Московской области, Красноярском крае, Туле, Екатеринбурге, Челябинске, Самаре, Севастополе, Казани, Воронеже, Иркутске, Кизилюрте, Симферополе, Оренбурге и др.

Атаки на провайдеров злоумышленники выполняют волнами. В среднем провайдеры находятся в списках целей в течение нескольких дней. Зачастую злоумышленники атакуют в один период сразу несколько операторов в одном регионе, а иногда проводят повторные атаки на одни и те же организации спустя некоторое время.

В своем Telegram-канале группа нередко анонсирует целые кампании против определенной индустрии, призывая своих партнеров атаковать. В топ-5 индустрий, атако-

ванных группировкой в 2025 году, помимо телекоммуникаций, вошли финансы, ИТ и разработка ПО, промышленность и энергетика, госсектор, транспорт. Также замечены более редкие случаи атак и на другие индустрии: ретейл, строительство, СМИ и др.

Наиболее громкие атаки, о которых сообщают СМИ, злоумышленники сопровождают публикацией постов в своем Telegram-канале, добавляя скриншоты с сервиса мониторинга сбоев и из новостных публикаций. Например, в марте 2025 года группа проводила DDoS-атаки на провайдера Lovit. Согласно данным РКН, максимальная мощность этой DDoS-атаки достигала 219,06 Гбит/с и 22,39 млн пакетов в секунду. В результате возникли проблемы с доступом у пользователей в ряде ЖК в нескольких регионах, где Lovit был единственным провайдером. Злоумышленники писали у себя в канале об этой громкой атаке в марте, а в сентябре прокомментировали новость о том, что ФАС России возбудила дело против застройщика после сообщений о сбое у провайдера-монополиста.

В последнем квартале 2025 года группа провела так называемые ими стрес-тесты (сохранена орфография оригинального источника). Цели были замечены в сферах угольной промышленности и финансов. Атаки продолжались нетипично долго для таких целей, поскольку в большинстве случаев все индустрии, кроме телекома, группировка атакует одним днем, в то время как в данных «тестах» атаки проводились на протяжении нескольких дней. Так, например, компания «Портовый альянс», управляющая сетью морских грузовых терминалов, заявила, что злоумышленники в течение трех дней атаковали ее цифровые системы, осуществляя DDoS-атаку. Согласно их данным, атака сочетала амплификацию DNS, SYN, IP Fragmentation и UDP-флуд с пиковой интенсивностью до 16 Гбит/с с использованием ботнета более чем из 15 тысяч уникальных IP.

Himars DDoS

Himars DDoS была наименее активной в 2025 году, в числе ее целей были в основном интернет-провайдеры. Атакующие сообщали об атаках в своем Telegram-канале вплоть до марта 2025-го. С каждым годом группа все реже сообщает об атаках. Если судить по публикациям в канале, то в 2024 году было совершено 104 атаки на российские организации, а в 2025-м — всего 13 атак, информация о которых публиковалась в январе. Отметим, что периодически злоумышленники затихают на несколько месяцев и ничего не пишут в канале. Так и в данном случае: в марте Himars DDoS опубликовала информацию об атаке на сервис для пополнения Steam, после чего другой активности выявлено не было.

CyberSec's

В июне группировка **CyberSec's** объявила о начале использования DDoS-утилиты **Gorgon Stress** для проведения атак на Иран. В июле злоумышленники заявили об обновлении утилиты Gorgon Stress до версии 1.9.9.9.7 в своем Telegram-канале. На протяжении года группировка заявляла о DDoS-атаках на различные российские ресурсы. Большая часть атак была направлена на финансовую, транспортную и промышленную отрасли. Кроме того, группа публиковала различные базы данных.

Кіберкорпус

Кіберкорпус — канал проукраинских хактивистов, атакующих российские компании и активных как минимум с июля 2024 года. В июле группа заявила о масштабной операции против энергетической компании. В результате атакующими была получена информация, после чего на стороне жертвы данные и резервные копии были уничтожены. С августа по октябрь 2025 года группа

проводила DDoS-атаки на государственные ресурсы, финансовую отрасль, телеком-оператора и на транспортную организацию.

Группировки, ориентированные на саботаж и публикацию утечек

Silent Crow

Silent Crow — группа проукраинских хактивистов, которая впервые заявила о себе 7 января 2025 года, опубликовав в Telegram-канале информацию об атаке на федеральные органы власти России. Спустя два дня Telegram-канал группы заблокировали, в результате чего они переехали на новый канал, который был создан в феврале 2022-го и ранее назывался Cyber Legion. Таким образом, появилась связь между Silent Crow и группой Cyber Legions.

Silent Crow на протяжении всего года заявляла о сливе различных баз данных российских и белорусских организаций. Наибольшее внимание привлекли заявления об атаках на авиаотрасль. В частности, в июле они заявили о совместной с Belarusian Cyber-Partisans атаке на авиакомпанию, в результате которой якобы получили доступ к разного рода данным и уничтожили их. В сентябре в результате дефейса сайта другой авиакомпании появился логотип Silent Crow.

BO Team

BO Team — это проукраинская группировка, начавшая активную деятельность в январе 2024 года, использующая вайпер для уничтожения инфраструктур и данных жертв. В качестве первоначального вектора группа использует рассылки вредоносных архивов. После компрометации уничтожает резервные копии файлов и инфраструктуру компании, а также удаляет данные с хостов. В нескольких случаях злоумышленники использовали программу-вымогатель **Babuk**.

В 2025 году группа была активнее, чем в предыдущем году. В первый же день 2025 года в своем Telegram-канале группировка BO Team заявила о взломе и об уничтожении данных ряда ресурсов, имеющих отношение к судебной системе РФ. Часть атак группы была направлена на ИТ-организации. В марте атаке подвергся крупный производитель оборудования. Злоумышленники оставили записку с требованием выкупа, но после оплаты не предоставили дешифратор. Воспользовавшись этим инфоповодом, в мае неустановленные злоумышленники провели рассылку во множество организаций из разных отраслей. Цитата из письма: «Ваша IT-инфраструктура находится под нашим контролем! Мы внедрили вредоносный код нового поколения в ваши системы. В случае невыполнения наших требований вы подвергнитесь мощной кибератаке. Все ваши данные будут безвозвратно утрачены, а системы выведены из строя» (сохранена орфография оригинального источника). Для того чтобы вызвать больше доверия, злоумышленники предлагали присылать подтверждение оплаты на якобы взломанную почту одной из жертв BO Team.

Некоторые из атак, анонсируемых BO Team, сопровождались заявлениями сотрудников ГУР Минобороны Украины, в которых они брали на себя ответственность за атаку. Например, атака 12 июня 2025 года на российского телеком-оператора. Ущерб от инцидента по предварительной оценке составил почти **66 млн руб**. Злоумышленники заявили, что вывели из строя большую часть инфраструктуры компании. Позднее в официальном Telegram-канале атакованная компания сообщила, что фактов утечки персональных данных обнаружено не было, в ответ на это злоумышленники в своем Telegram-канале опублико-

вали базу данных, содержащую информацию о сотрудниках.

В 2025 году было выявлено несколько рассылок группы BO Team. Например, в мае группа проводила кампанию, приуроченную к транспортно-логистическому форуму: злоумышленники развернули фишинговые домены, через которые распространяли вредоносный архив с ВПО BrockenDoor. Во второй половине 2025 года группа провела несколько кампаний по рассылке вредоносных архивов под видом различных опросов, в частности связанных с корпоративным ДМС. Анализ показал, что атакующие используют несколько версий бэкдора **BrockenDoor**, а также в ряде случаев устанавливают бэкдор **ZeronetKit**.

CyberUnknown

CyberUnknown (Unknown92007291) — это злоумышленник, который начал действовать в сентябре 2024 года. Посредством использования веб-сканера **Nikto** он проводил сканирование ресурсов компаний из следующих сфер: государственной, военной, энергетической, промышленной, телекоммуникационной, информационной, образовательной и транспортной. Полученные данные злоумышленник публикует на сервисе MediaFire.

DC8044

DC8044 — группировка, действующая с января 2019 года. С 2022-го группа DC8044 участвует в кибератаках на российские цели.

1 января 2025 года группа опубликовала базы данных двух российских интернет-провайдеров. В августе совершила атаку на продуктовую сеть, получив доступ к различным базам и системам Confluence, ADAudit Plus, vSphere Client, Free BPX. После чего на протяжении недели злоумышленники продолжали публиковать похищенные данные и прилагали скриншоты из систем и внутренних переписок в специально созданном Telegram-канале.

В августе DC8044 в своем Telegram-канале сообщили об атаке на российское предприятие пищевой промышленности.

Осенью 2025 года опубликовали пост об атаке на российского провайдера, в котором сообщили, что вместо публикации базы данных в открытых источниках будут делиться семплом на несколько тысяч записей в личных сообщениях.

Yellow Drift

Группа заявила о себе в 2025 году: сообщала в своем Telegram-канале об атаках на несколько организаций, в результате которых была выведена из строя часть инфраструктуры жертв. В одном из постов группа сообщила об атаке на аудиторскую компанию и опубликовала часть полученных данных.

Ukrainian Cyber Alliance

Ukrainian Cyber Alliance (также известная как **RUH8**) — группа проукраинских хакеров, появившаяся в ноябре 2015 года. Злоумышленники продолжают проводить дефейс-атаки, публиковать скомпрометированные данные и информацию об успешных атаках, в ходе которых для уничтожения данных целевых организаций, предположительно, используется ВПО типа вайпер. В отчетном периоде группа также заявляла о совместных атаках с другими проукраинскими группировками, в частности с **BO Team**.

Belarusian Cyber-Partisans

Belarusian Cyber Partisans — это группа, созданная в 2020 году. С 2022 года, помимо белорусских организаций, атакует и российские. В 2025 году группировка несколько раз публиковала в своем Telegram-канале заявления об успешных атаках на российские организации, проведенных совместно с проукраинской группой **Silent Crow**. Для уничтожения данных использует вайпер, которому было присвоено имя **Pryanik**. Также среди используемого группой ВПО были выявлены следующие: **DNSCat2**, **SeekDNS**, **PartisanDNS**, **PartisanLoader**, **Vasilek**.

Hdr0

Hdr0 — это группировка, появившаяся в сентября 2022 года. В большинстве случаев совершает дефейс-атаки, которые в ряде случаев сопровождаются утечкой данных атакованной компании. 26 октября 2025 года Telegram заблокировал каналы злоумышленника. **Hdr0** сообщил об этом в своем аккаунте в Twitter и пообещал воссоздать канал в другом мессенджере.

4B1D

4B1D, предположительно, группа проукраинских хактивистов, появившаяся в начале 2025 года. Злоумышленники преимущественно шифруют данные жертв и уничтожают инфраструктуры с помощью специального ВПО типа вайпер. Киберпреступники могут быть связаны с группировкой **RUH8**, которая первой упомянула 4B1D у себя в Telegram-канале.

Другие финансово мотивированные группировки

Помимо групп-вымогателей и политически мотивированных групп, в отчетном периоде выявлена активность более 20 финансово мотивированных группировок. Наиболее примечательные из них Vasy Grek, Hive0117, CapFIX. Как и прогнозировали годом ранее, злоумышленники проводили атаки с использованиемм ВПО Buhtrap.

После публичного освещения вредоносной активности исследователями некоторые группировки меняют подход к атакам, начинают использовать новые инструменты. Например, злоумышленник Vasy Grek добавил в арсенал программу-вымогатель. Но также есть группы, которые годами используют один и тот же подход для проведения атак. К таким можно отнести, например, Hive0117.

Примечательной была кампания, в ходе которой злоумышленники рассылали ВПО Buhtrap через систему ЭДО. Это в некотором роде аналог атаки через доверительные отношения. Стоит отметить, что в 2025 году атаки через подрядчиков были замечены и у групп-вымогателей, и у прогосударственных групп. В отчетном году несколько групп отметились использованием майнеров в атаках на Россию.

Наиболее активные финансово мотивированные группы описаны далее.

Vasy Grek	
Псевдонимы	Fluffy Wolf
Начало активности	2016 г.
Целевые страны	Россия
Целевые индустрии	Промышленность, строительство, финансы, энергетика, транспорт, туризм, торговля, спорт, ИТ
Атакуемые платформы	Windows
Инструменты	PureCrypter, PureHVNC, PureLogs, Pay2Key, VenomRAT, PowerShell Stego downloader
Особенности	• Использование ВПО разработчика PureCoder (PureCrypter, PureHVNC, PureLogs). • Регистрация доменов и наполнение содержимого бухгалтерской и финансовой темами
Ресурсы	https://www.f6.ru/blog/vasygrek-and-mr-burns/ https://www.f6.ru/blog/vasygrek-new-attacks-2025/

В январе 2025 года группа **Vasy Grek** проводила рассылку писем преимущественно под видом актов сверки и другой бухгалтерской отчетности. В 2025 году злоумышленники перестали использовать **META Stealer** и продолжили использовать ВПО разработчика **PureCoder** — **PureCrypter**, **PureHVNC**, **PureLogs**. В мае 2025-го группа добавила **VenomRAT** в свой арсенал, а позднее еще и программу-вымогатель **Pay2Key**.

Vasy Grek рассылала несколько форматов писем:

- со ссылкой на вредоносный файл, хранящийся на GitHub;
- со ссылкой на вредоносный файл, хранящийся на домене VasyGrek;
- с вредоносным вложением.

В случаях писем со ссылками переход по ним осуществляется при клике на изображения с иконками файлов (пример на рис. 20).

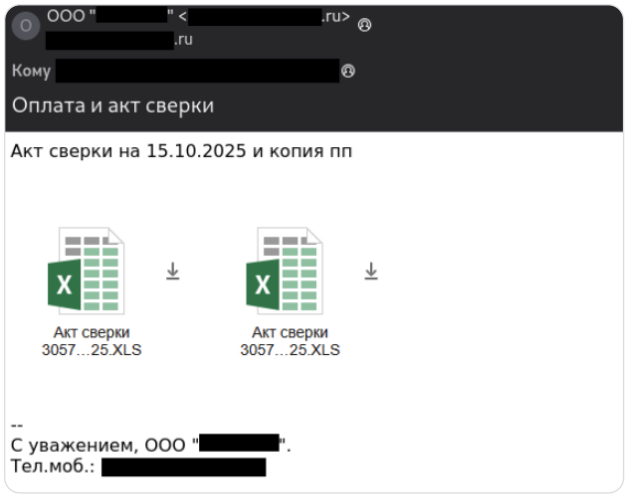


Рис. 20 — Пример письма группы Vasy Grek от 15.10.2025

В августе, помимо привычного для этой группы ВПО PureLogs и PureHVNC, на хосте жертвы был замечен запуск программы-вымогателя Pay2Key.

В ноябре злоумышленник обновил цепочку атак: в качестве вложения письма вместо архива с исполняемым файлом внутри стал применять архив с файлами BAT или VBS. Несмотря на использование разных начальных вредоносных скриптов (VBS и BAT), дальнейшая цепочка атаки у них идентична. Скрипт инициирует загрузку изображения, из которого позднее извлекается и дешифруется нагрузка. Нагрузка предназначена для загрузки новой полезной нагрузки в виде PureHVNC с удаленного ресурса, ее дешифровки и внедрения в процесс RegAsm.exe. В атаке использовался загрузчик, классифицируемый нами как PowerShell Stego downloader, который использовался разными атакующими.

Злоумышленник продолжал использовать зарегистрированные ранее домены, а также регистрировал новые, с которых в ходе атак загружалось ВПО. Для Vasy Grek характерны определенные паттерны при регистрации новых доменов. Это позволило нам создать правила для сетевой инфраструктуры злоумышленника и выявить регистрируемые домены еще до начала их использования в атаках. Например, часть такой пересекающейся инфраструктуры группы — на рис. 21.

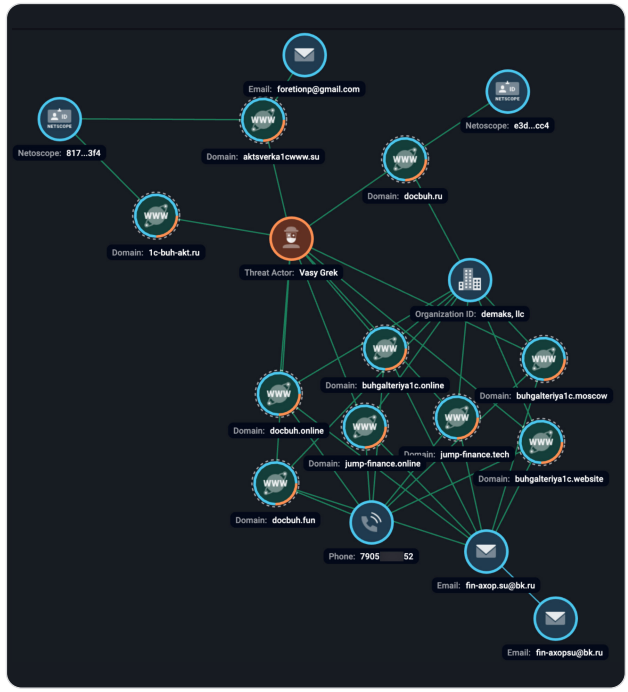


Рис. 21 — Пример графового анализа инфраструктуры группы Vasy Grek

На доменах злоумышленника размещались страницы, замаскированные под ресурсы с бухгалтерскими услугами.

Hive0117	
Псевдонимы	Watch Wolf
Начало активности	2021 г.
Целевые страны	Россия, Беларусь, Казахстан
Целевые индустрии	Разные
Атакуемые платформы	Windows
Инструменты	DarkWatchman RAT
Особенности	Устоявшееся поведение: повторное использование регистрационных данных для создания доменов, использование одних и тех же текстов писем, мимикрия под одних и тех же отправителей
Ресурсы	https://habr.com/ru/companies/F6/news/905930/ https://t.me/f6_cybersecurity/3881

2025 год группа **Hive0117** начала с фишинговых рассылок вредоносной программы **DarkWatchman** под видом заказа для оборонной промышленности. Злоумышленники часто прибегают к подходу, в соответствии с которым отправляют сначала чистое письмо, а когда потенциальная жертва вступает в переписку, ответным письмом направляют уже защищенное паролем вредоносное вложение.

В 2025 году группа отметилась несколькими волнами массовых рассылок, в ходе которых распространяла ВПО DarkWatchman. В апреле специалисты F6 обнаружили рассылку более **500** писем с почтового домена, зарегистрированного на те же регистрационные данные, которые группа использовала в 2023 году.

Стоит отметить, что Hive0117 периодически мимикрирует в своих рассылках под одни и те же организации. Например, с февраля по апрель 2025 года специалисты F6 детектировали рассылки, направленные от имени ФССП, к такой же маскировке группа прибегала в 2022 году. С марта 2025-го злоумышленники из Hive0117 проводили рассылки от имени логистического оператора PONY EXPRESS, схожие рассылки были выявлены в 2023 и 2024 годах. В июле была раскрыта рассылка от имени другого крупного логистического оператора. 24 сентября 2025 года, спустя почти два месяца с момента последней рассылки ВПО DarkWatchman, группа Hive0117 снова провела рассылку от имени ФССП в адрес российских организаций из разных отраслей.

Содержимое писем с одними и теми же темами злоумышленники практически не изменяют. Примеры рассылок от 03.12.2025 и 29.04.2025 представлены на рис. 22 и 23.

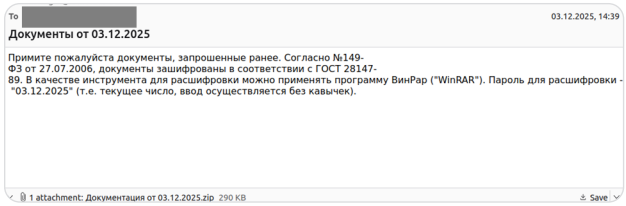


Рис. 22 — Пример письма группы Hive0117 от 03.12.2025

Рис. 23 — Пример письма группы Hive0117 от 29.04.2025

Атаки с использованием ВПО Buhtrap	
Целевые страны	Россия, Беларусь
Целевые индустрии	Финансы, строительство и др.
Атакуемые платформы	Windows
Инструменты	Buhtrap
Ресурсы	https://habr.com/ru/companies/F6/news/975730/

Buhtrap — это ВПО и одноименная финансово мотивированная киберпреступная группа. В 2016 году исходные коды Buhtrap были опубликованы в открытом доступе, что привело к его использованию другими атакующими.

В августе 2025 года был обнаружен нестандартный способ распространения ВПО Buhtrap. Злоумышленники рассылали вредоносные архивы по контрагентам от лица взломанных пользователей через систему ЭДО. Выявленная кампания проводилась в несколько волн минимум до октября 2025-го. Распространяемый архив включает исполняемый файл-загрузчик, который распаковывает содержащийся в себе дроппер второй стадии и запускает его в памяти. Дроппер проверяет, не выполняется ли он в песочнице. Если проверка пройдена, сбрасывает следующую стадию — файл-загрузчик. Последний уже отвечает за распаковку и запуск в памяти финальной нагрузки в виде **Buhtrap RAT**. При взаимодействии ВПО с C2 собранные данные записываются в `.dat`-файл и периодически отправляются на сервер в зашифрованном виде. В ответ будут получены фрагменты PNG-изображений, в конце которых добавляются зашифрованные данные, которые могут содержать исполняемые модули.

В последние два месяца 2025 года специалисты F6 наблюдали типичный для злоумышленников способ распространения Buhtrap RAT, используемый и в предыдущие годы, — через поддельные бухгалтерские сайты. На эти сайты жертва попадает через поисковую выдачу. Пример представлен на рис. 24.

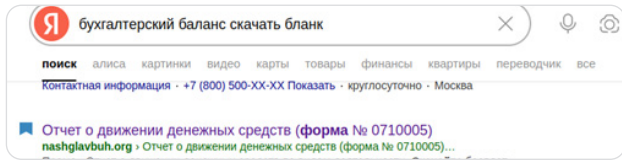


Рис. 24 — Запрос в поисковой выдаче и сайт-приманка, с которого распространялось ВПО Buhtrap

На странице содержится вредоносный JS-скрипт, который перехватывает клик на файл. Если посетитель определяется как потенциальная жертва, то после клика на файл будет открыта новая вкладка в браузере со ссылкой на ZIP-архив. Дальнейшая цепочка атаки повторяет описанную выше. Фрагмент JS-скрипта, отвечающий за загрузку вредоносного архива, представлен на рис. 25.

Рис. 25 — Расшифрованный фрагмент JS-скрипта, отвечающий за загрузку вредоносного архива

StrongBaba	
Псевдонимы	Scaly Wolf, Albino Ghouls
Начало активности	Июль 2023 г.
Целевые страны	Россия
Целевые индустрии	Промышленность, финансы, энергетика, НИИ, торговля
Атакуемые платформы	Windows
Инструменты	Chubaka Downloader, Chubaka Backdoor, StrongBaba Uploader, StrongBaba VNC Trojan, StrongBaba.RustAgent, Chisel, Meterpreter, HandleKatz
Особенности	Фишинговые письма не содержат никакого текста в теле, только вложения и тему

StrongBaba — преступная группа, активная как минимум с лета 2023 года. В ходе первой кампании злоумышленники рассылали ВПО **WhiteSnake**. С середины 2024 года группа стала использовать ВПО, написанное на C++ и получившее название **Chubaka Downloader** и **Chubaka Backdoor**. Загрузчик собирает данные о жертве, передает их на C2 и загружает нагрузку. На протяжении года группа добавляла небольшие изменения в свое основное ВПО, а также экспериментировала с новыми инструментами.

Интересная особенность группы: злоумышленники не добавляют в тело писем какой-либо текст. Пример одного из писем представлен на рис. 26.

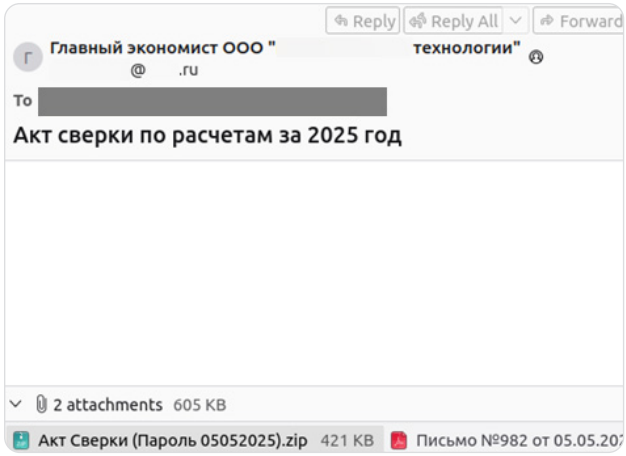


Рис. 26 — Пример письма группы StrongBaba

В сентябре 2025 года специалисты F6 Threat Intelligence выявили фишинговую рассылку нового ВПО. Атрибуцию к группе StrongBaba удалось сделать благодаря ряду общих признаков, среди которых:

- письма имеют финансовую направленность;
- отправлены с адресов @mail.ru;
- вложения — защищенные паролем архивы;
- мимикрия отправителя под ту же ИТ-организацию, что и в майской рассылке группы;
- PDF-приманка полностью идентична используемой в майской рассылке группы.

В архивах содержится ВПО, которому было присвоено имя **StrongBaba.RustAgent**. На момент исследования ВПО находилось в стадии разработки. Оно собирает информацию о зараженном устройстве, позволяет загружать и выгружать файлы с устройства жертвы, а также создает SSH-туннель.

CapFIX	
Псевдонимы	Insolent Hyena
Начало активности	Май 2025 г.
Целевые страны	Россия
Целевые индустрии	Финансы, торговля, госучреждения
Атакуемые платформы	Windows
Инструменты	OpcJacker, CapDoor, NeXDownloader
Ресурсы	https://habr.com/ru/companies/F6/articles/966072/

С середины 2025 года специалисты F6 фиксируют активность группы, которой было присвоено имя **CapFIX**. Согласно нашей телеметрии, рассылки группы были направлены преимущественно на финансовую и торговую индустрии. В связи с этим на момент исследования аналитики F6 считают группировку финансово мотивированной.

Злоумышленники рассылают хорошо подготовленные письма, используют спуфинг отправителя. Письма рассылались под видом инструкций по действиям при минной угрозе и требования предоставить отчетность по противодействию информационным атакам (рис. 27).

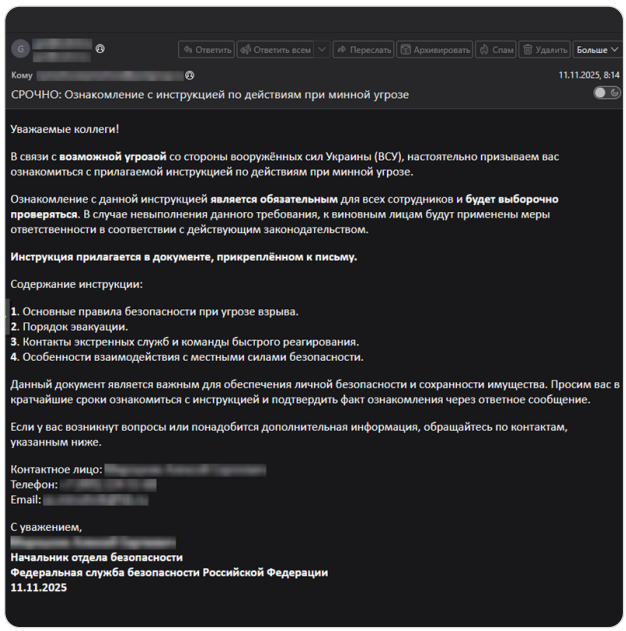


Рис. 27 — Пример письма группы CapFIX от 11.11.2025

Вложение представляет собой PDF-файл, который выглядит таким образом, что побуждает жертву нажать на кнопку для отображения содержимого документа. В первых атаках злоумышленники использовали легенду, согласно которой пользователю требуется подтвердить, что он не робот, через прохождение капчи. В более поздних атаках требовалось скачать программный комплекс «КриптоПро» или программу «КонсультантПлюс» для корректного отображения документа. Пример содержимого PDF-файла представлен на рис. 28.

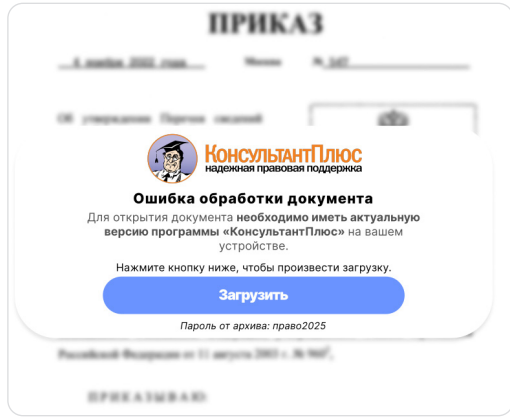


Рис. 28 — Пример содержимого PDF-файла, распространяемого группой CapFIX

В осенних атаках ссылка из PDF-файла вела на защищенный паролем вредоносный архив. Архив содержит MSI-файл, который распаковывает CAB-файл и устанавливает приложение **VB Decompiler Lite**. Из распакованного содержимого CAB-архива запускает легитимный исполняемый файл, который используется для загрузки бэкдора **CapDoor** с помощью техники DLL side-loading.

Narketing163	
Псевдонимы	Ravage Wolf
Начало активности	Июль 2023 г.
Целевые страны	Россия, Казахстан, Франция
Целевые индустрии	Транспорт, финансы, торговля, ИТ, НИИ, промышленность, энергетика, строительство
Атакуемые платформы	Windows
Инструменты	SnakeKeylogger, NOVA, MoDiRAT, CVE-2017-11882
Ресурсы	https://www.f6.ru/blog/narketing163/

Злоумышленник был назван **Narketing163** по одному из наиболее часто используемых им электронных адресов, который встречался во множестве писем в качестве обратного электронного адреса. В целях Narketing163 было выявлено **26** стран, включая страны СНГ.

В 2025 году злоумышленник рассылал письма на разных языках: русском, азербайджанском, турецком, английском. Тематика текстов связана с договорами, предложениями услуг и товаров, со сроками поставки, с обработкой заказов и их оплатой. В первом квартале 2025 года злоумышленник рассылал письма с вредоносным архивом во вложении, содержащим ВПО **SnakeKeylogger**.

С середины года у Narketing163 изменились цепочки атак. Ранее он прикреплял к письмам архивы, внутри которых располагался исполняемый файл с ВПО. Но теперь ВПО доставляется с использованием обфусцированных VBS-скриптов следующими способами:

- обфусцированный VBS-скрипт содержался внутри архива из вложения к письму;
- к письму прилагался PDF-документ, в котором была ссылка на скачивание архива с обфусцированным VBS-сценарием внутри;
- к письму прилагался DOCX-файл, в результате запуска которого на устройство загружался RTF-документ, эксплуатирующий уязвимость CVE-2017-11882, посредством чего осуществлялась загрузка и запуск обфусцированного VBS-сценария.

Последний способ доставки имеет сходство с атаками, проводимыми TA558. В анализируемых атаках Narketing163 не только применял схожий способ доставки, но и использовал именование файлов в виде «змеиного регистра» с длиной более 100 символов, аналогичное используемому группой TA558. Помимо цепочки атаки, изменилась и финальная нагрузка: вместо **SnakeKeylogger** стал рассылаться стилер **NOVA**. Если в системе жертвы был установлен французский язык и устройство жертвы находится во Франции, то оно заражается еще одной нагрузкой **MoDiRAT**.

xplogs22	
Начало активности	Ноябрь 2024 г.
Целевые страны	Россия, Беларусь, Казахстан
Целевые индустрии	Разные
Атакуемые платформы	Windows
Инструменты	SnakeKeylogger, FormBookFormgrabber, XWorm

В процессе мониторинга угроз в январе 2025 года была обнаружена рассылка писем с вложением и темой «Договор». Злоумышленники распространяли таким образом ВПО **SnakeKeylogger**. Группе было присвоено имя **xplogs22**, поскольку в конфигурациях ВПО для эксфильтрации данных жертв использовалась одноименная почта. Были выявлены и связанные более ранние атаки, в ходе которых распространялся **FormBookFormgrabber**.

Письма были обнаружены на русском, арабском, казахском, английском языках, что говорит о вероятной нацеленности атакующего на разные страны. Группировка xplogs22 использовала для рассылок как скомпрометированные электронные адреса, так и подменяла адрес отправителя с помощью спуфинга. С июля группа стала использовать в атаках **XWorm**.

CurrencyZipPay	
Начало активности	Август 2024 г.
Целевые страны	Россия, Армения
Целевые индустрии	Транспорт, ИТ, торговля, финансы, туризм, промышленность, строительство, энергетика
Атакуемые платформы	Windows
Инструменты	PureLogs, PureCrypter, Remcos
Особенности	Названия тем и архивов-вложений к письму полностью совпадают

CurrencyZipPay — хакеры, действующие с конца лета 2024 года. Злоумышленники рассылают письма, содержащие вредоносный архив с ВПО. В августе 2024-го они распространяли ВПО **Meta Stealer**, с осени того же года — **PureLogs**, а с середины 2025-го добавили в свой арсенал **Remcos**.

В конце февраля 2025 года специалисты F6 выявили рассылки ВПО PureLogs. Злоумышленники распространяли письма с архивами, содержащими .COM-файлы-лоадеры PureCrypter. Загрузчик **PureCrypter** внедряет код PureLogs в процесс InstallUtil.exe. После запуска PureLogs обращается к C2 и ожидает в ответ нагрузку-стилер.

Характерная черта группы: названия тем и вложенных архивов полностью совпадают. Письма были замечены на русском, армянском, румынском языках. В качестве тем злоумышленник использует «оплаты», «платежи», «договоры», «акты сверок». Пример типового письма группы на рис. 29.

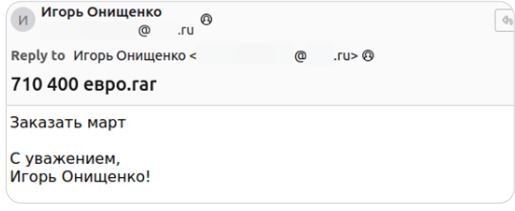


Рис. 29 — Пример письма группы Vasy Grek от 15.10.2025

NyashTeam	
Начало активности	2022 г.
Целевые страны	Россия, Беларусь, Казахстан, Китай
Атакуемые платформы	Windows
Инструменты	DCRat, WebRat
Ресурсы	https://www.f6.ru/blog/nyashteam/

Группировка **NyashTeam** с 2022 года предоставляет услуги MaaS, которые включают в себя продажу ВПО и предоставление хостинг-услуг для его размещения. Ориентируется прежде всего на русскоязычную аудиторию, но ее инструментами пользуются и другие злоумышленники из разных стран мира.

В рамках модели MaaS NyashTeam распространяет два семейства ВПО:

- **DCRat** — бэкдор, известный с 2018 года, поддерживающий возможности кражи данных, записи клавиатурного ввода, доступа к веб-камере, скачивания файлов, эксфильтрации паролей и выполнения произвольных команд.
- **WebRat** — ВПО, специализирующееся на краже учетных данных браузеров; поддерживает удаленное выполнение команд и позволяет доставлять дополнительное ВПО.

Злоумышленники продают ВПО через Telegram-боты. В большинстве случаев клиенты группировки распространяли ВПО через платформы YouTube и GitHub.

В 2025 году специалисты F6 детектировали регистрируемую группой NyashTeam инфраструктуру, а также и ее применение в атаках других злоумышленников, в частности Confman и Businessman.

В декабре 2025 года специалистами F6 выявлен образец ВПО, который оставляет на машине жертвы записку с требованием формата, как на рис. 30. Примечательно, что схожие имена Telegram-ботов использовала группировка NyashTeam ранее, и, предположительно, она могла переключиться на распространение программы-вымогателя после публичного освещения ее деятельности и блокировки большей части инфраструктуры.

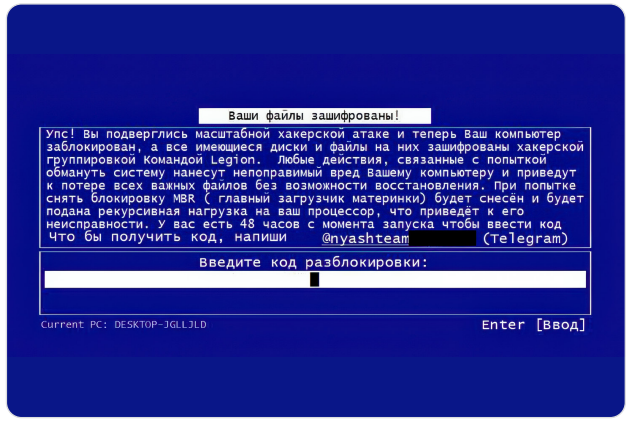


Рис. 30 — Содержимое записки с требованием злоумышленников

ComicForm	
Псевдонимы	Comix Wolf
Начало активности	Апрель 2025 г.
Целевые страны	Россия, Беларусь, Казахстан
Целевые индустрии	Финансы, промышленность, туризм, торговля, НИИ
Атакуемые платформы	Windows
Инструменты	SnakeKeylogger, NOVA, MoDiRAT, CVE-2017-11882
Ресурсы	https://www.f6.ru/blog/comicform/

С весны 2025 года специалисты F6 Threat Intelligence отслеживали массовую рассылку фишинговых писем с вложением, открытие которого приводит к установке **FormBook**.

В ходе атаки злоумышленники использовали исполняемый файл, который содержит ссылки на анимированные изображения с супергероями в формате GIF. Примечательно, что изображения не использовались для атаки, а являлись лишь частью кода вредоносной программы. Из-за героев из комиксов и нагрузки в виде FormBook специалисты F6 присвоили злоумышленнику имя ComicForm. Группа **ComicForm** использовала в рассылках в заголовке replay-to (обратный адрес) электронную почту rivet_kz@, зарегистрированную в бесплатном российском почтовом сервисе. Указанный заголовок встречался в письмах, написанных на русском или английском языках, отправленных с адресов электронной почты, зарегистрированных в доменах верхнего уровня .ru, .by и .kz.

Эти особенности позволили специалистам F6 выявить более позднюю кампанию группы в адрес российских промышленных организаций. В ходе атак злоумышленник рассылал фишинговые письма о необходимости подтвердить учетную запись. Введенные жертвой учетные данные отправляются в домен атакующих.

Phantom Papa	
Начало активности	Апрель 2025 г.
Целевые страны	Россия, Беларусь и др.
Целевые индустрии	Финансы, госучреждения, НИИ, здравоохранение, торговля, ИТ, промышленность, спорт, транспорт
Атакуемые платформы	Windows
Инструменты	Phantom Stealer
Ресурсы	https://www.f6.ru/blog/phantom-stealer/

В июне 2025 года специалисты F6 обнаружили новую вредоносную активность, которую назвали **Phantom Papa**. Злоумышленники рассылали письма с вложениями на русском и английском языках, часть из которых была фривольного содержания, а другая часть связана с платежами и финансовыми документами. В результате выполнения цепочки атаки устанавливался **Phantom Stealer**. Этот стилер продается на сайте, созданном злоумышленниками в феврале 2025-го. Некоторые из писем были написаны с ошибками в структуре. Это свидетельство того, что они были переведены на русский язык с использованием переводчика, а злоумышленник, вероятно, не русскоязычный.

Phantom Stealer основан на коде ВПО **Stealerium**. Он имеет возможность сбора паролей, банковской и криптовалютной информации, содержимого браузеров и мессенджеров. Для эксфильтрации данных может использовать Telegram, Discord или SMTP. Telegram-бот, который использовался злоумышленником, активен минимум с апреля 2025-го, по его имени и был назван атакующий (Phantom Papa).

mbryan80	
Начало активности	Январь 2025 г.
Целевые страны	Россия, Казахстан, Малайзия, Перу, Босния и Герцеговина, ОАЭ, Бразилия, Эквадор, Египет, Испания, Мексика, Португалия, Пакистан, Польша, Катар, Парагвай, Румыния, Словения, Танзания, Уругвай, Вьетнам
Целевые индустрии	Здравоохранение, финансы, НИИ, промышленность
Атакуемые платформы	Windows
Инструменты	NOVA

Весной 2025 года специалисты F6 выявили вредоносные рассылки, в ходе которых злоумышленники распространяли форк ВПО SnakeKeylogger — **NOVA**.

Атакующий пытался мимикрировать под казахстанские организации: домен отправителя был в зоне .kz, тема, содержимое и вложение к письму — на казахском языке. В текстах писем содержится якобы платежная информация от банка. Для эксфильтрации скомпрометированных данных жертв злоумышленник использует Telegram-бот. Помимо России, среди целей было выявлено еще множество стран из разных регионов мира.

DwmRemInjectors	
Начало активности	Апрель 2025 г.
Целевые страны	Россия
Целевые индустрии	Финансы, НИИ, энергетика, промышленность, туризм, торговля, телекоммуникации, строительство, здравоохранение, спорт
Атакуемые платформы	Windows
Инструменты	Remcos, XWorm

DwmRemInjectors — группировка, получившая название за счет имени используемого в первых атаках BAT-файла (`dwm.bat`) и ВПО (**Remcos RAT**). Рассылки группы носят массовый характер, но при этом для нее характерна отправка большого количества писем на различные адреса, принадлежащие одной компании.

За 2025 год было выявлено несколько волн рассылок, в которых злоумышленники использовали разные цепочки атак. Со временем некоторые из звеньев изменялись. В феврале и марте в качестве финальной нагрузки устанавливался Remcos RAT. В более поздних атаках группа, помимо Remcos, начала применять **XWorm**. Стоит отметить, что в конфигурации XWorm была указана ссылка на Pastebin, откуда RAT забирает актуальный адрес управляющего сервера. Такой подход позволяет атакующим оперативно обновить C2 при необходимости.

Группа часто прибегает к спуфингу отправителя. Еще одна отличительная черта атакующих — формат рассылаемых писем: в выявленных рассылках в имя отправителя они добавляют почту, а в подпись вставляют картинку с логотипом и контакты компании, под которую маскируют отправителя. В ряде писем подпись с логотипом была вставлена цельной картинкой, предположительно вырезанной из реального письма от организации, под которую мимикрируют злоумышленники. Пример одного писем группы — на рис. 31.

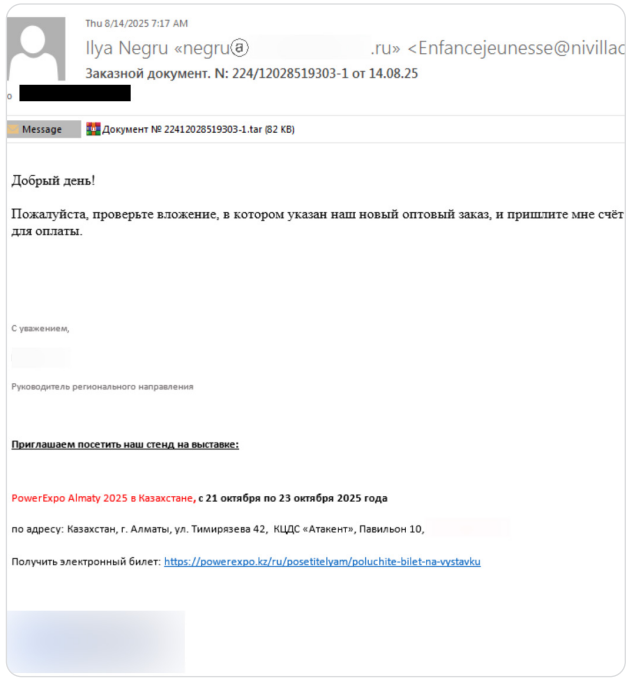


Рис. 31 — Пример письма группы DwmRemInjectors от 14.08.2025

Tax Miners	
Начало активности	Май 2024 г.
Целевые страны	Россия
Целевые индустрии	Торговля, финансы
Атакуемые платформы	Windows
Инструменты	XMRig
Особенности	Использование сервиса «Облако Mail» для распространения ВПО

Tax Miners — группировка, занимающаяся распространением майнера **XMRig** с 2024 года. Название было дано на основе имени C2-домена.

В начале года система F6 MXDR заблокировала письмо в адрес компании из сферы торговли. Письмо содержало ссылку на облачное хранилище, которая вела на вредоносный архив, защищенный паролем. Анализ показал, что злоумышленники подготовили следующую цепочку атаки: письмо со ссылкой → защищенный паролем 7z → SFX-архив → EXE-дроппер и приманка → XMRig. Примечательно, что во всех атаках группы ссылка из письма вела на «Облако Mail», а сами письма рассылались с почтовых адресов, созданных на популярных почтовых веб-сервисах.

Позднее цепочка претерпевала незначительные изменения. В частности, вместо приманки жертве для маскировки показывали окно с ошибкой запуска, был добавлен еще один промежуточный дроппер. Но финальная нагрузка осталась прежней — **XMRig**.

Kinsing	
Псевдонимы	H2Miner, Resourceful Wolf, Money Libra
Начало активности	2019 г.
Целевые страны	Россия и др.
Целевые индустрии	Финансы, телекоммуникации, транспорт, развлечения и др.
Атакуемые платформы	Windows, Linux
Инструменты	Kinsing, XMRig, различные CVE
Ресурсы	https://www.f6.ru/blog/kinsing/

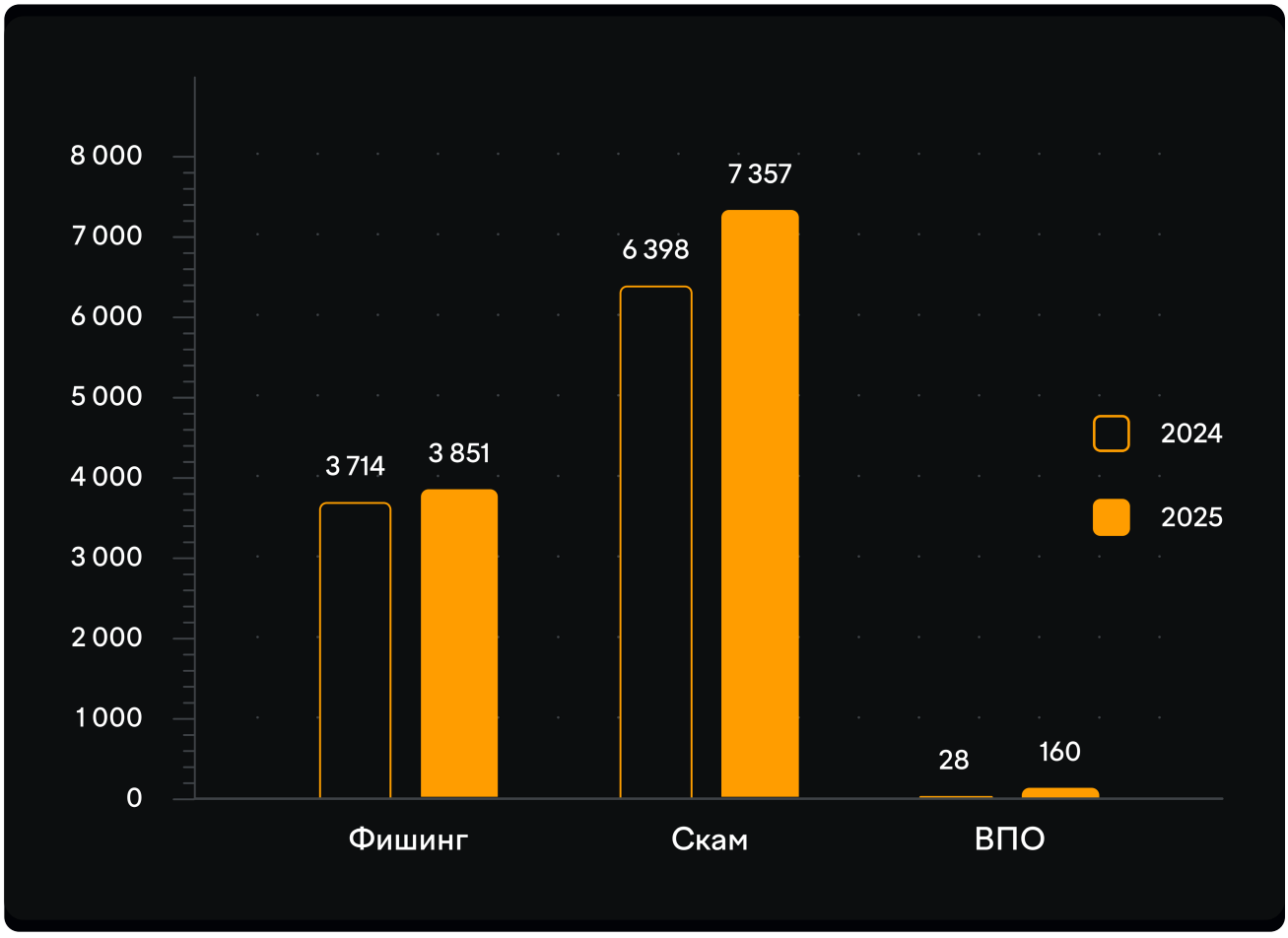
Kinsing — киберпреступная группа, действующая с 2019 года и специализирующаяся на криптоджекинге, в первую очередь майнинге Monero, а также на создании и расширении ботнетов. Главная мотивация — финансовая выгода, достигаемая за счет использования ресурсов зараженных систем для майнинга криптовалюты. В 2025 году специалисты F6 выявили атаки группы Kinsing, нацеленные на российские организации.

Атаки Kinsing проходят в несколько этапов с задействованием определенной инфраструктуры. На первом этапе группировка использует начальные серверы, посредством которых проводится массовое сканирование в поисках уязвимых систем. При обнаружении уязвимости происходит эксплуатация для получения удаленного доступа. На втором этапе используются серверы загрузки, с которых на компрометированные хосты доставляются основные компоненты ВПО: скрипты для отключения защитных механизмов, удаления конкурирующих вредоносных процессов, эксплуатации уязвимостей, а также загрузки и запуска дополнительных файлов, Kinsing, майнер **XMRig** и др. Зараженные узлы формируют ботнет Kinsing, управляемый через C2-серверы.

Скам и фишинг

В 2025 году эксперты F6 фиксировали рост числа ресурсов, которые использовались мошенниками во всех типах атак, включая фишинг, скам и распространение вредоносных приложений. Особенно резко увеличилось количество ресурсов, связанных с распространением вредоносного ПО, которые маскировались под реальные бренды. Таких ресурсов выявлено и заблокировано почти в 6 раз больше, чем в 2024 году. Бурный рост обусловлен активностью скам-групп, нацеленных на заражение Android-устройств.

Количество заблокированных ресурсов (в среднем на один бренд) в 2024 и 2025 годах



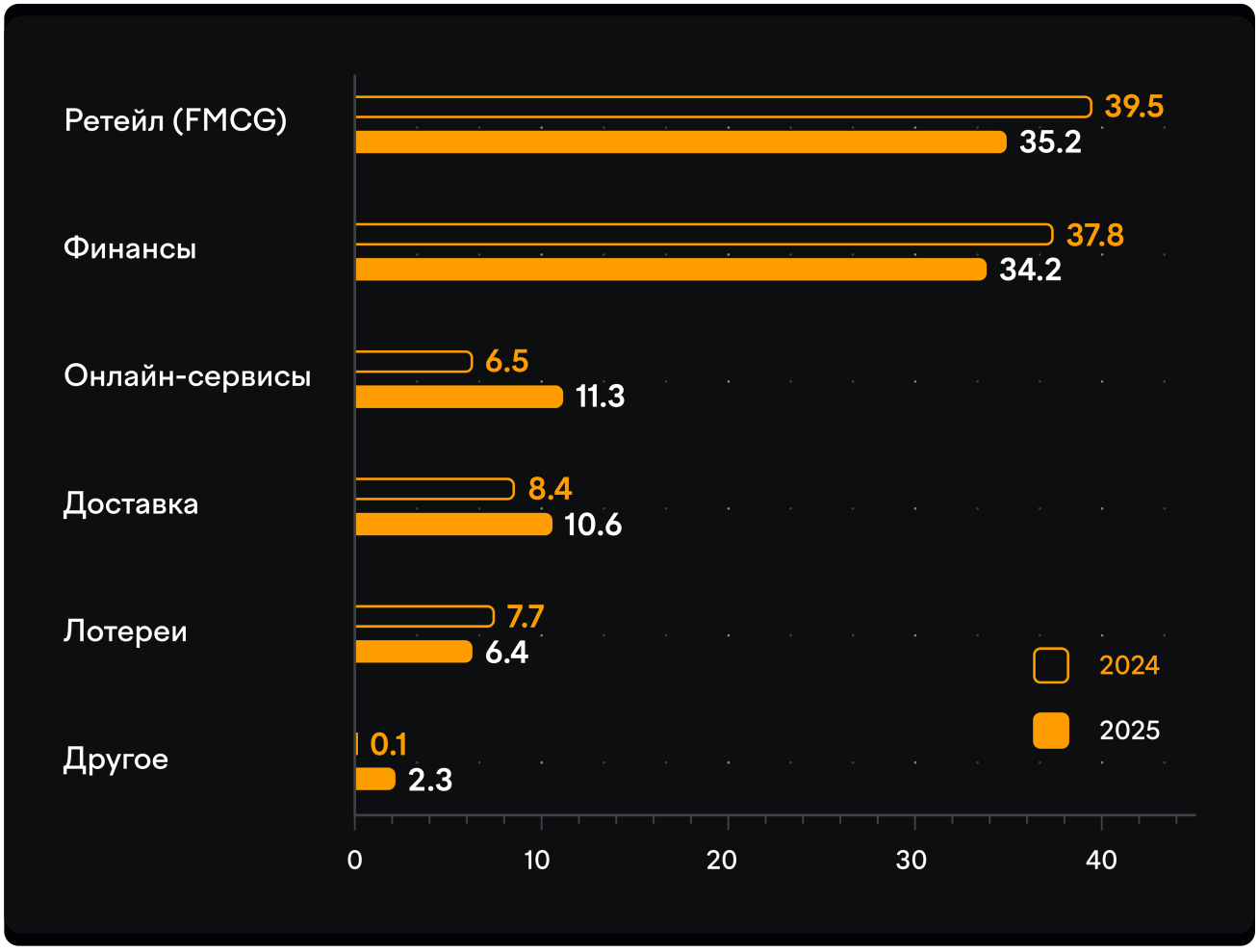
Распределение фишинга и скама по отраслям и индустриям

Ретейл (FMCG)

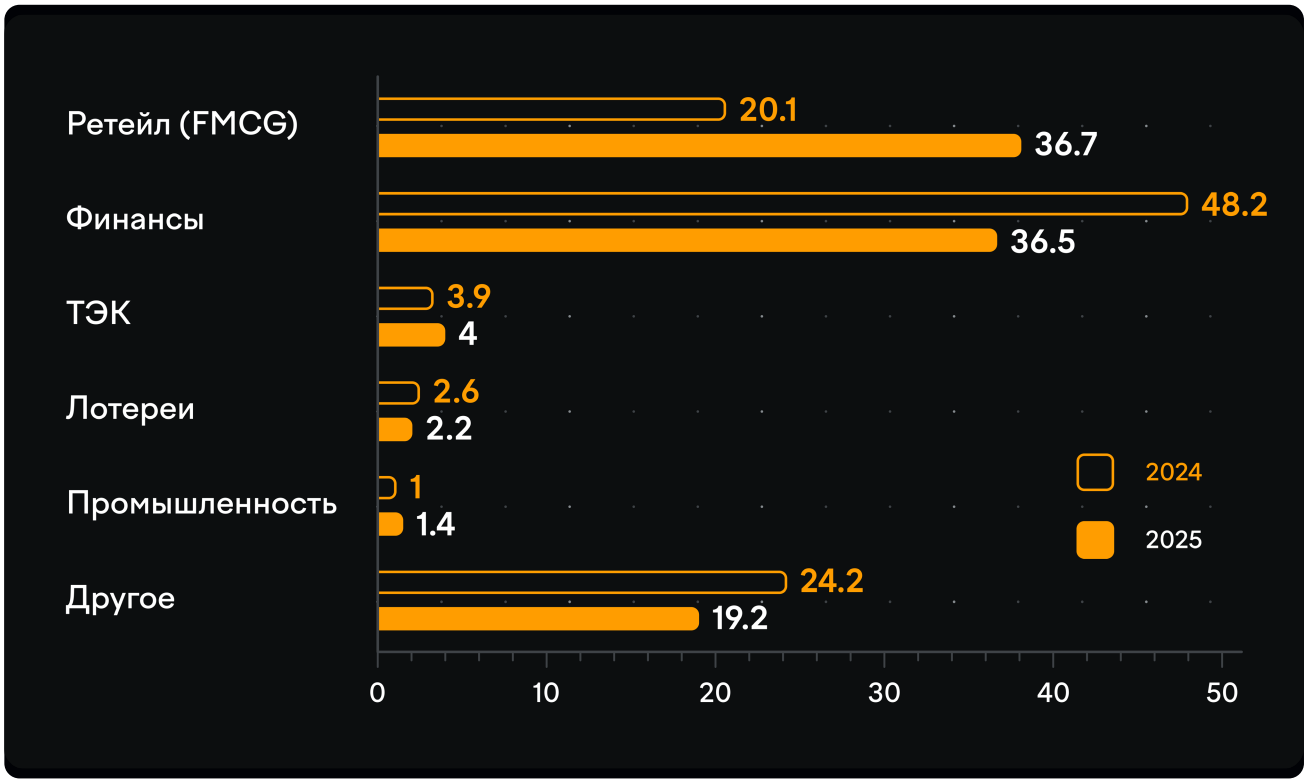
Электронная коммерция, по оценкам экспертов F6, в 2025 году оставалась одной из главных целей как фишинговых, так и мошеннических атак.

Бренды из этой индустрии эксплуатируются в схеме «Мамонт» для создания фишинговых сайтов, а в мошеннических партнерских программах — для создания мошеннических сайтов, преимущественно с розыгрышами. Создание фишинговых ссылок стало максимально автоматизированным процессом — это одна из причин, по которой специалисты F6 фиксируют увеличение числа создаваемых злоумышленниками ресурсов. Также под видом мобильных приложений различных брендов киберпреступники распространяют ВПО.

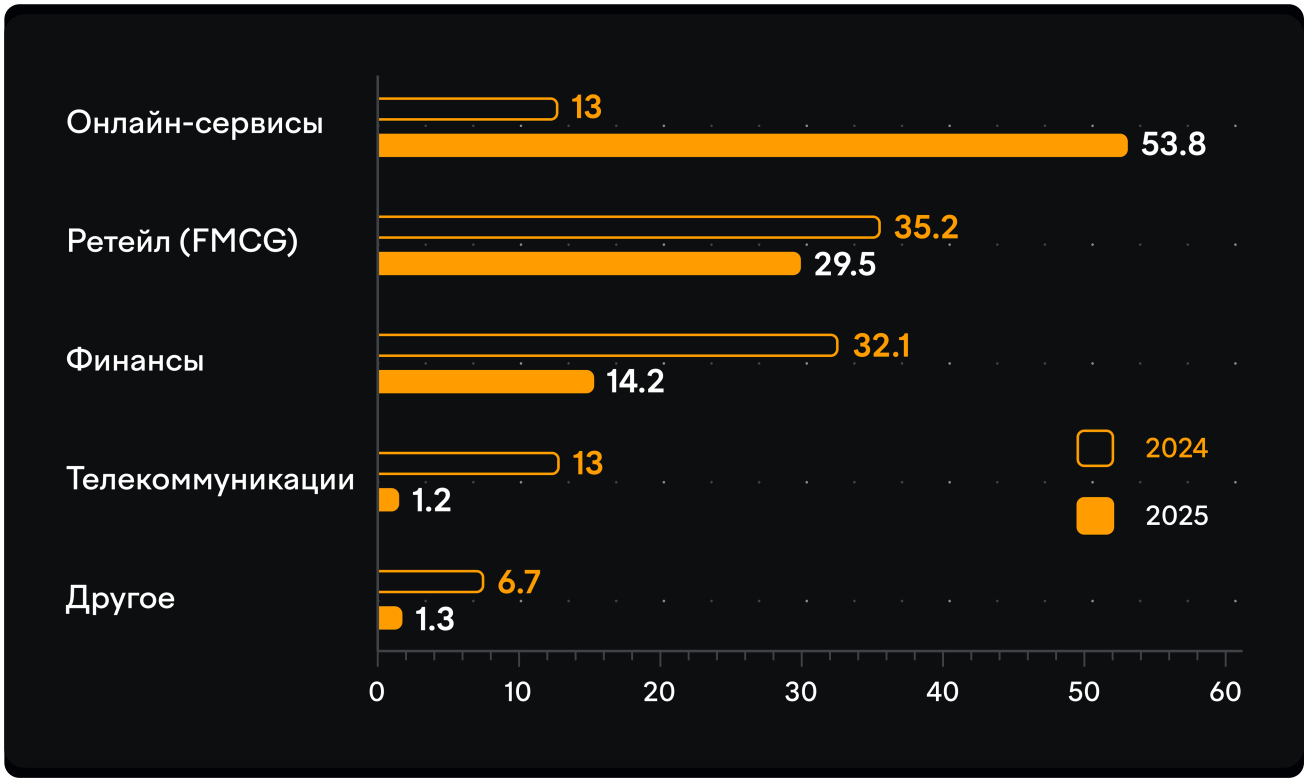
Распределение фишинга по индустриям (в %)



Распределение скама по индустриям (в %)



Распределение ВПО по индустриям (в %)



Финансы

Банковский сектор на втором месте среди отраслей, под которые киберпреступники чаще всего маскируются в атаках на пользователей. Злоумышленники проводят фишинговые атаки для получения данных банковских карт и данных для входа в личный кабинет банка клиентов. В скам-атаках злоумышленники регулярно используют финансовые бренды в схемах инвестиционного мошенничества, поддельных опросах и розыгрышах.

Онлайн-сервисы

Онлайн-сервисы на третьем месте по количеству фишинговых атак. Мошенники используют их как прикрытие для кражи данных банковских карт, мимикрируя под официальные сайты, похищают данные для входа в онлайн-сервисы с последующим привлечением пользователей сервиса в мошеннические схемы. Онлайн-сервисы занимают первое место по частоте использования в схемах распространения ВПО для мобильных устройств.

Доставка

Бренды сервисов доставки активно используются в схеме «Мамонт» с оплатой несуществующих товаров. Злоумышленники генерируют ссылки на фишинговые сайты определенных логистических компаний.

Лотереи

Лотереи уже долгое время используются мошенниками в качестве приманки в различных схемах. Однако в 2025 году мы фиксируем снижение активности злоумышленников на фоне активной борьбы компаний — организаторов лотерей с цифровыми угрозами.

ТЭК и промышленность

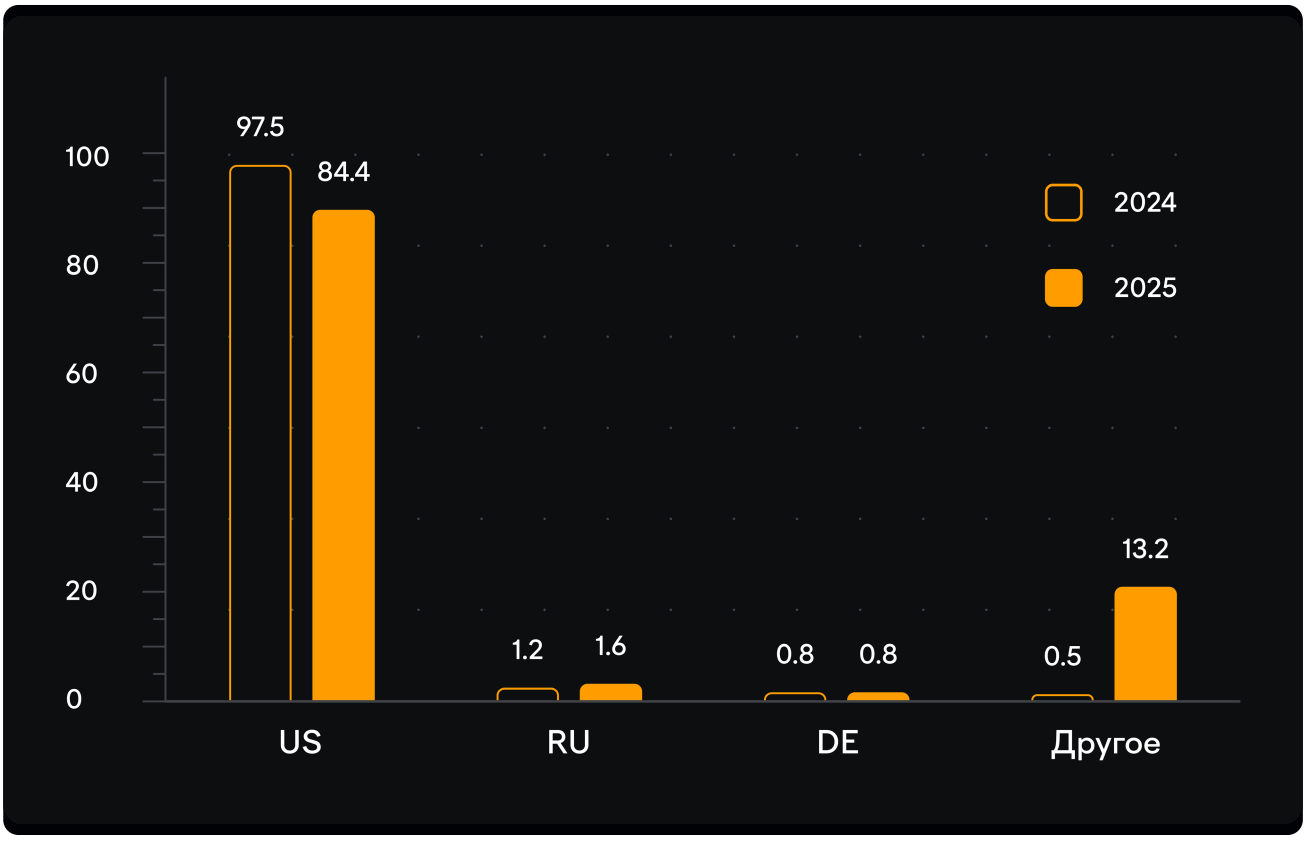
Бренды из этих отраслей часто используются как прикрытие в схемах инвестиционного мошенничества. Также мошенники копируют официальные ресурсы для атак на клиентов компаний.

Распределение фишинга и скама по хостам и доменным зонам

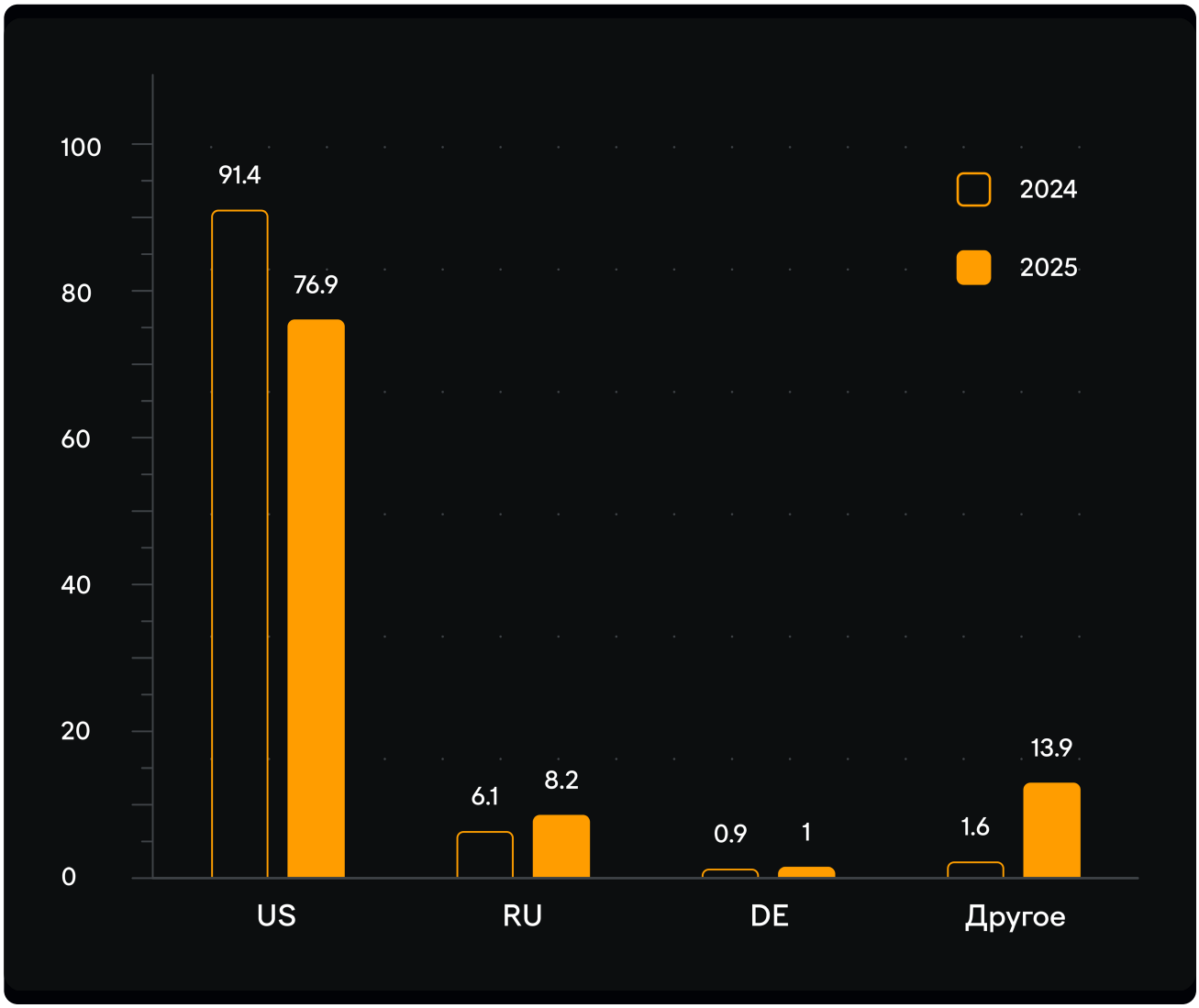
В 2025 году, как и в предыдущие годы, американские хостинг-провайдеры лидировали по размещению фишингового и мошеннического контента, нацеленного против российских пользователей.

Злоумышленники используют систему DNS компании Cloudflare, которая кеширует содержимое сайта для улучшения работы пользователей. Система защищает IP-адрес сайта от прямого воздействия, что затрудняет взаимодействие с хостинг-провайдером для устранения нарушений. Это влияет на срок жизни фишинговых и мошеннических ресурсов. Хотя Cloudflare может раскрыть хостинг-провайдера по запросу, некоторые провайдеры отказываются признавать нарушения, когда видят IP-адреса Cloudflare, а не свои собственные.

Распределение по хостинг-провайдерам фишинговых ресурсов (в %)

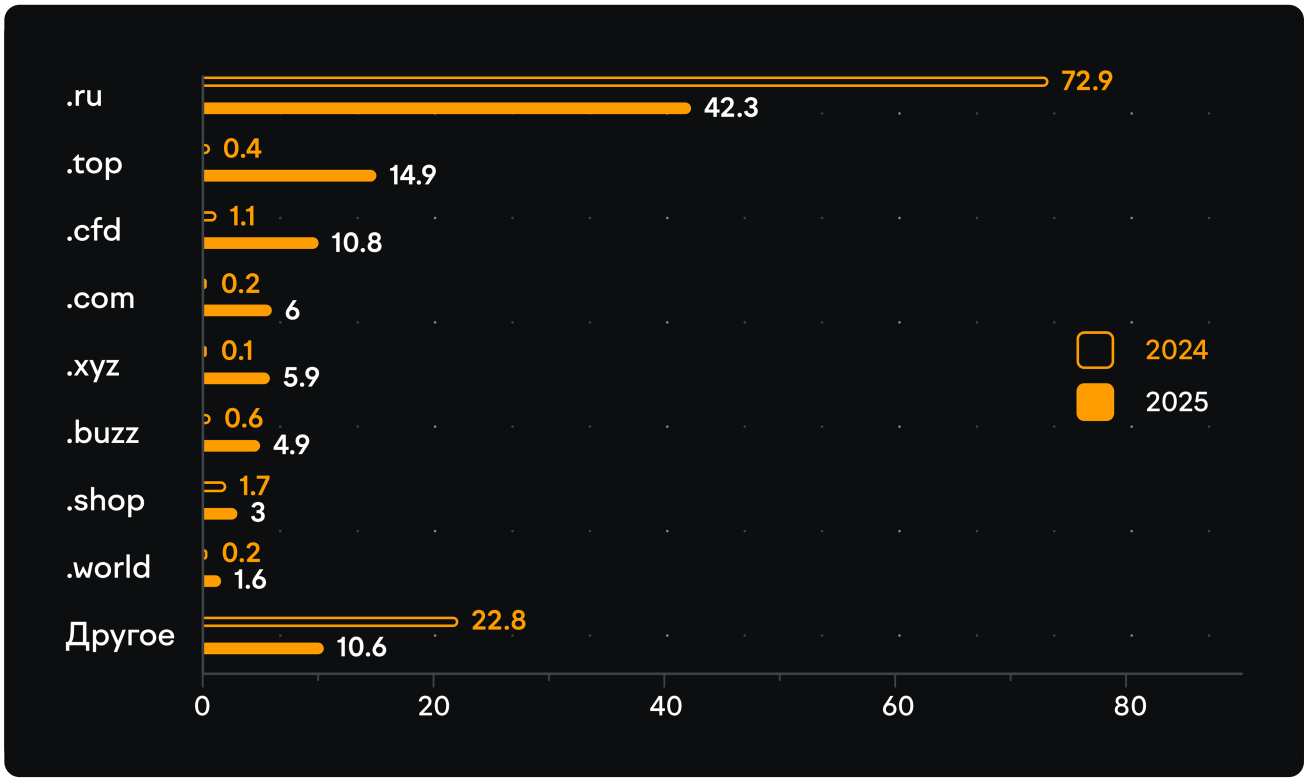


Распределение по хостинг-провайдерам мошеннических ресурсов (в %)

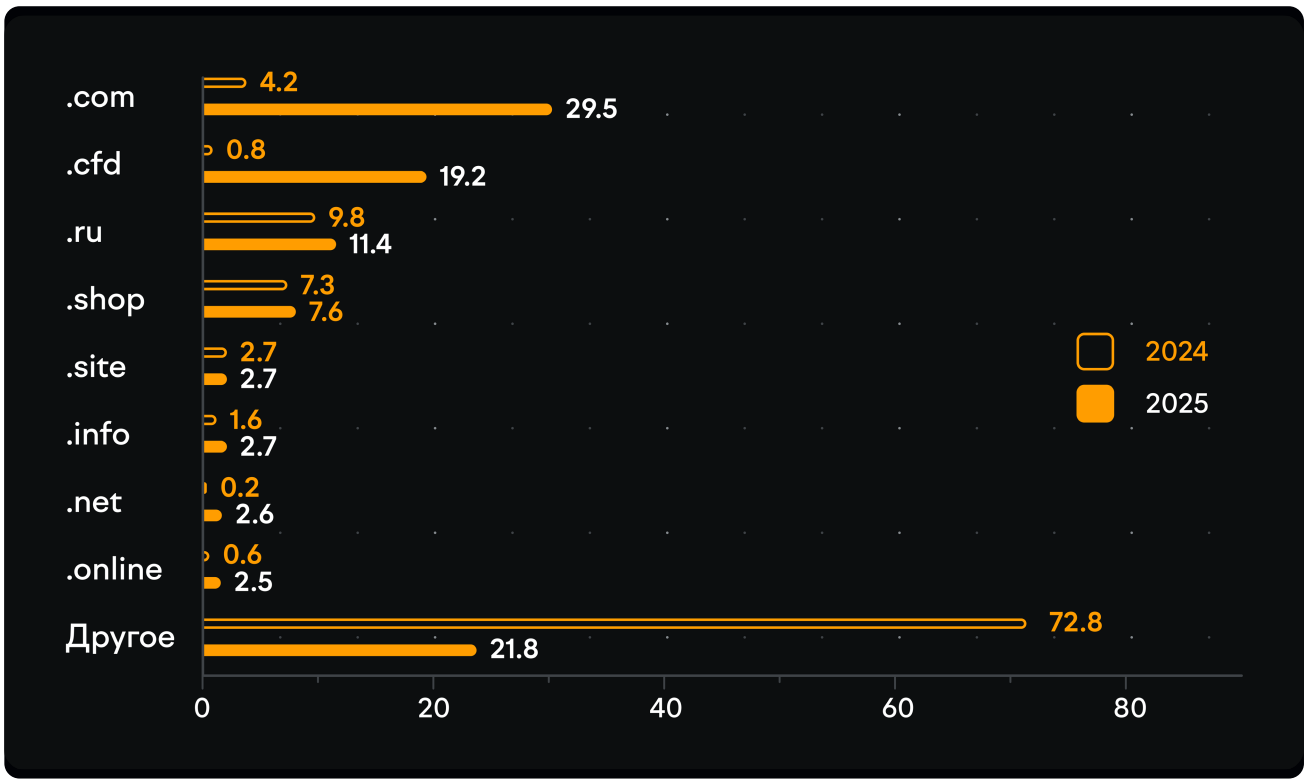


Выбор доменных зон киберпреступниками меняется из года в год. Заметно сократилось количество регистраций фишинговых ресурсов в зоне .ru. Это связано с эффективной работой регуляторов и CERT по оперативной блокировке фишинговых доменов. В результате злоумышленники все чаще выбирают другие доменные зоны и иностранных регистраторов, несмотря на более высокую стоимость регистрации.

Распределение регистрируемых фишинговых доменов по зонам (в %)



Распределение регистрируемых мошеннических доменов по зонам (в %)



Обзор самых популярных мошеннических схем в России

Специалисты DRP F6 на протяжении всего 2025 года фиксировали появление новых мошеннических схем. В основном это были фишинговые схемы с угоном Telegram-аккаунтов, инвестиционного мошенничества и партнерских программ со множеством вариантов привлечения потенциальных жертв через эксплуатацию брендов, новых инфоповодов и сценариев.

Что касается схем с распространением вредоносных приложений для операционной системы Android, то большинство из них носят гибридный характер. Чтобы увеличить охват потенциальных жертв за счет владельцев устройств с операционной системой iOS, киберпреступники используют фишинговые сайты, с помощью которых похищают данные банковских карт либо учетной записи iCloud.

Ниже мы приводим некоторые из новых схем мошенничества, которые аналитики F6 обнаружили в 2025 году. Большинство из них активно используются и сейчас, от других злоумышленники отказались в пользу более эффективных сценариев обмана.

Январь 2025 года

Схема: вредоносные приложения

Описание схемы:

Под видом владельцев ПВЗ злоумышленники размещали фейковые вакансии на популярных рекрутинговых онлайн-сервисах. Пользователю предлагали пройти дистанционное собеседование, в ходе которого интересовались, какая модель смартфона у него (преступников интересовали только пользователи Android). Затем жертву просили заполнить анкету и направляли ссылку для загрузки мобильного приложения, которое якобы необходимо для работы. На самом деле это приложение — Android-троян, который позволял похищать деньги со счетов пользователя.

Февраль 2025 года

Схема: «Мамонт»

Описание схемы:

Классическая схема связана с предоплатой покупки и доставки несуществующих товаров. Злоумышленники размещают лоты-приманки на сервисах бесплатных объявлений. После того как переговоры о покупке-продаже с официального ресурса переносятся в мессенджер, мошенники присылают ссылку на фишинговый сайт, где жертве предлагают ввести свои банковские данные, оплатить покупку по QR-коду или перевести

нужную сумму самостоятельно по реквизитам. После оплаты, если жертва не догадалась об обмане, мошенники сразу или через некоторое время могут предложить возврат, например, под предлогом сбоя на почте или повреждения товара. Деньги не вернут, а лишь повторно спишут стоимость товара.

В 2025 году участники этой схемы начали активно атаковать пользователей фриланс-сервисов. В портфель фишинговых шаблонов было добавлено три бренда в сфере фриланса. Также схема пополнилась шаблонами брендов из банковской сферы и телекоммуникаций.

В схеме «Мамонт» по-прежнему эксплуатировались бренды из следующих индустрий: доставка, перевозка животных, сервисы поиска автопопутчиков, маркетплейсы, онлайн-ретейл, аренда недвижимости, сервисы услуг, продажа авиабилетов, бронирование отелей, банковские переводы.

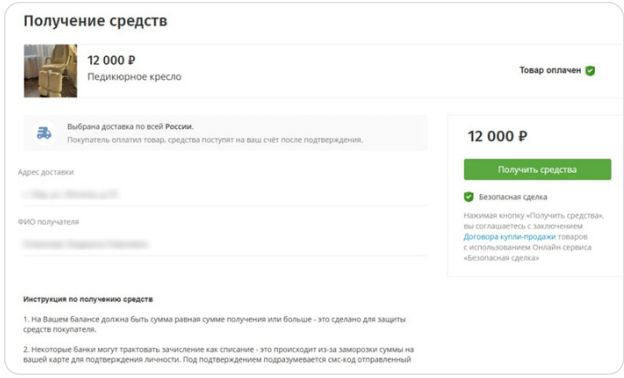


Рис. 32 — Скриншот фейкового ресурса, используемого в схеме «Мамонт»

Март 2025 года

Схема: фишинг в Telegram

Описание схемы:

Помимо кражи самих аккаунтов от мессенджера, злоумышленников интересуют цифровая валюта Telegram Stars (звезды) и коллекционные виртуальные подарки, включая NFT. Они могут выводиться автоматически на подставные учетные записи, а затем, как правило, продаются. Для создания фишинговых ресурсов злоумышленники использовали веб-панели или Telegram-боты, в которых создавали фишинговые страницы различной тематики. Злоумышленники применяли уловки: денежные призы, предупреждение от службы безопасности, годовую премиум-подписку в подарок, голосования, доступ в приватный канал и др.

Март 2025 года

Схема: фишинг в Telegram + вредоносные приложения

Описание схемы:

Мошенники создавали на популярных платформах объявления о вакансиях с высокими зарплатами. Предлагали разные должности: от курьера до топ-менеджера. Соискателям присылали ссылку для заполнения резюме. Для отправки резюме нужно было авторизоваться в Telegram. Пользователь вводил номер телефона и отправлял код подтверждения, после чего злоумышленники получали доступ к его аккаунту.

После взлома мошенники отправляли жертве сообщение от имени партии «Единая Россия» с предложением за 5000 руб. пройти опрос. Чтобы «пройти опрос», предлагалось скачать приложение с Android-трояном. С его помощью мошенники получали доступ к смартфону пользователя, перехватывали СМС и списывали деньги со счета.

Март 2025 года

Схема: вредоносные приложения

Описание схемы:

Сценарий онлайн-мошенничества со знакомствами, в котором приманкой служит бесплатное посещение салона красоты.

Скамеры изображали успешных мужчин 30–35 лет в сервисах для знакомств. Злоумышленник сообщал, что владеет сетью салонов красоты и хочет подарить девушке бесплатное посещение с услугами премиум-класса. Получив согласие жертвы, скамер отправлял ссылку на сайт фейкового салона для бронирования, а также «персональный промокод». Девушка заполняла форму, указывала промокод, имя и номер телефона.

Пользовательницам Android для подтверждения записи предлагали скачать под видом фирменного приложения Android-троян. Обладательницам iPhone нужно было подтвердить запись через Apple ID. Когда девушка вводила код двухфакторной аутентификации, контроль над устройством перехватывали злоумышленники.

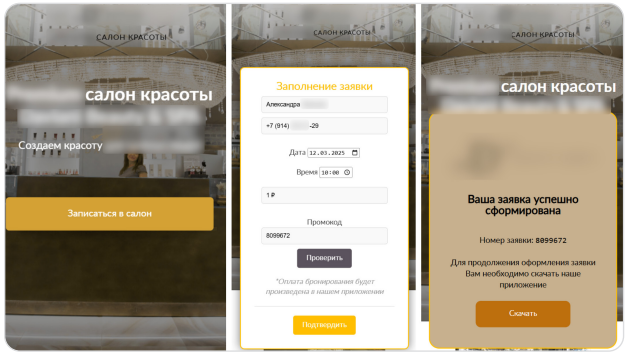


Рис. 33 — Скриншоты сайта фейкового салона красоты

Апрель 2025 года

Схема: вредоносные приложения

Описание схемы:

В преддверии сезона отпусков мошенники размещали в соцсетях короткие видео с выгодными предложениями. Например: «Апартаменты в Сочи. 5 минут до моря. От 3000 ₽ в сутки».

В переписке мошенники сообщали, что предоплата не требуется: потенциальной жертве предлагали «безопасное бронирование» через известный сервис. В этой схеме преступники использовали фейковые ресурсы трех популярных российских сервисов для бронирования отелей и квартир.

При переходе по ссылке пользователи устройств на iOS видели страницу фейкового сервиса с фотографиями квартиры, ценой и кнопкой «Забронировать». После выбора дат заселения отображалась сумма аренды. После нажатия кнопки «Оплатить» появлялась страница с формой для ввода данных банковской карты, а затем — кода из СМС.

Пользователи устройств на Android при переходе по ссылке от мошенников вначале видели такие же страницы фейкового ресурса с фотографиями квартир, ценой, номером объекта и выбором дат для бронирования. Но после нажатия кнопки «Оплатить» их перенаправляли на фейковый Google Play с предложением установить под видом фирменного приложения сервиса Android-троян.

Апрель 2025 года

Схема: вредоносные приложения

Описание схемы:

Схема использовалась против пользователей Android-устройств. Им предлагали скачать игровые моды и приложения. Для продвижения злоумышленники создавали Telegram-каналы, посвященные Roblox, Minecraft, Brawl Stars, Subway Surfers, Standoff 2 и др. Пройдя по ссылке, пользователь попадал в бот, где его просили подписаться на несколько Telegram-каналов, а затем скачать APK-файл. На самом деле это было ВПО, в том числе Android-трояны.

Апрель 2025 года

Схема: инвестиционное мошенничество

Описание схемы:

В преддверии Дня Победы была запущена реклама инвестиционного мошенничества с использованием бренда государственного фонда «Защитники Отечества». Пользователям предлагали заработать до 30 млн руб. якобы в рамках социального проекта, инвестируя в акции российских компаний. Для убедительности злоумышленники размещали фейковые комментарии от людей, которые «якобы» получили крупные выплаты.

Май 2025 года

Схема: фишинг в Telegram

Описание схемы:

Мошенники зарабатывали на популярности игрушечных монстров Лабубу. Аналитики F6 обнаружили Telegram-боты, в которых Лабубу выступал в качестве приманки. Под предлогом «Лабубу в подарок за отзыв» злоумышленники предлагали поделиться своим контактом, а затем ввести полученный код якобы для регистрации. Ввод кода предоставлял мошенникам доступ к учетной записи жертвы.

Июнь 2025 года

Схема: вредоносные приложения

Описание схемы:

Сценарий мошенничества, нацеленный на ИТ-специалистов, находящихся в поиске работы или допзаработка. Злоумышленники от лица крупных компаний якобы нанимали тестировщиков. Мошенники просили заполнить анкету: указать Ф. И. О., телефон, дату рождения и номер карты (якобы для зарплаты). После этого тестировщику присылали файл с первым заданием, который на самом деле оказывался Android-трояном. Чтобы убедить жертву установить вредоносную программу, мошенники сообщали, что задача — тестировать приложение как обычный пользователь, в том числе проходить регистрацию и проверять функции.

Рис. 34 — Пример мошенничества с фейковыми подработками

Июль 2025 года

Схема: партнерские программы

Описание схемы:

Злоумышленники предлагали оформить виртуальную кредитную карту с лимитом в 100 тыс. руб. под 99% годовых (или 0,27% от суммы займа в день). Ограничений по возрасту, кредитной истории и другим критериям нет. Под предлогом оформления карты скамеры просили заплатить комиссию в 3050 руб.

Август 2025 года

Схема: скам-схема

Описание схемы:

Киберпреступники под брендом «Здоровая Россия» создали сеть из 143 фейковых ресурсов. Пользователям предлагали оставить свой телефон, чтобы получить консультации врачей по широкому спектру заболеваний. Однако под предлогом врачебных рекомендаций пользователям навязывали дистанционную продажу сомнительных препаратов. Как правило, злоумышленники утверждали, что предлагаемые препараты не продаются в аптеках, а распространяются только дистанционно.

Сентябрь 2025 года

Схема: вредоносные мобильные приложения

Описание схемы:

Злоумышленники в специальных Telegram-ботах генерировали ссылки на фейковые сайты, с которых происходило скачивание вредоносных APK-файлов для Android-устройств.

Поиск жертв осуществлялся разными способами, чаще всего через чаты в Telegram или в других мессенджерах. Злоумышленники выставляли свое объявление/предложение, а после обращения потенциальной жертвы вынуждали ее перейти по вредоносной ссылке под различными предлогами.

1. Отслеживание заказа из фейкового маркетплейса

Злоумышленники создавали объявления с товарами по заниженной цене на маркетплейсах либо в фейковых магазинах. Под видом продавца/менеджера связывались с жертвой через Telegram или WhatsApp. В процессе разговора жертва сообщала личные данные, такие как ФИО. получателя, адрес доставки заказа и номер телефона. Для отслеживания заказа менеджер просил скачать вредоносное приложение.

2. Трудоустройство

Злоумышленники создавали фейковые объявления о найме на удаленную работу с привлекательными условиями и доходом. При общении в мессенджере после сбора персональных данных (СНИЛС, номер карты, контактный телефон и дата рождения) мошенники просили установить вредоносное приложение.

Сентябрь 2025 года

Схема: инвестиционное мошенничество

Описание схемы:

Злоумышленники создавали сайты — двойники благотворительных фондов, на которых под предлогом финансовой поддержки бойцов и их родных предлагали получать по 500 тыс. руб. ежемесячно за счет участия в фейковой инвестиционной программе. Для обмана мошенники размещали видеодипфейки с отзывами от имени участников СВО: на реальные кадры с бойцами накладывали чужие голоса.

Сентябрь 2025 года

Схема: FakeTeam

Описание схемы:

Усовершенствованная схема FakeBoss. Теперь атака проводится не одним лжеруководителем, а целой командой лжеколлег.

Злоумышленники создают групповой Telegram-чат, в который жертву добавляет посторонний аккаунт под нейтральным псевдонимом, например «Отдел кадров» и др. В чате несколько участников — «босс» и «коллеги» жертвы. В чате «босс» просит воспользоваться Telegram-ботом для подтверждения данных госсервиса и сообщить полученный шестизначный код. При переходе в бот у пользователя запрашивают контакты и присылают требуемый код. После чего преступники начинают следующий этап атаки — убеждают жертву, что ее личный кабинет госсервиса взломан и теперь надо перевести деньги на «безопасный счет», досрочно погасить кредит и задекларировать сбережения.

Октябрь 2025 года

Схема: скам-схема

Описание схемы:

Киберпреступники создали фейковый интернет-магазин под несуществующим брендом «Зооаптека PRO», где якобы можно было приобрести популярные импортные ветеринарные препараты для животных: «Бравекто», «Симпарику», «Апоквел», NexGard и др.

Мошенники привлекали покупателей через сайт фальшивой ветеринарной аптеки и сеть из более чем 20 Telegram-каналов и трех Telegram-ботов. «Заказ» можно было оформить только через личный аккаунт «менеджера», который предлагал внести 100%-ю предоплату переводом на карту или по номеру телефона.

После получения квитанции об оплате «менеджер» переводил пользователя на «логиста», который отвечал не всем пользователям, а лишь тем, кто настойчиво требовал информацию о заказе.

Если жертва требовала возврата средств, мошенники начинали новый этап атаки, который приводил к повторному списанию суммы за несуществующий товар.

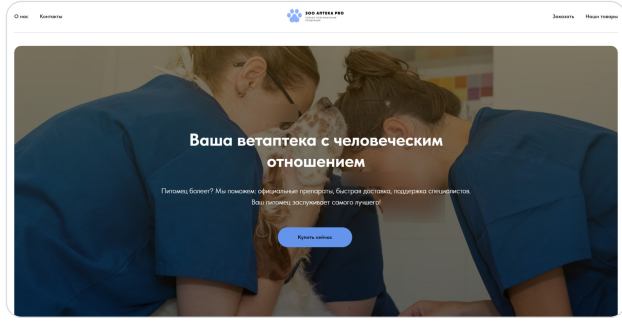


Рис. 35 — Скриншот сайта интернет-магазина несуществующего бренда

Октябрь 2025 года

Схема: FakeDate

Описание схемы:

Ранее в этой схеме мошенники создавали страницы несуществующих театров, кинозалов и антикафе. Теперь же они начали использовать сайты — двойники популярных сервисов.

Выбор активностей для свидания расширился: мошенники стали «продавать» билеты на выставку, квест, в музей, оперу и филармонию, в планетарий и на пейнтбол. Развязка схемы осталась прежней. После оплаты билетов «девушка» или переставала выходить на связь, или сообщала, что вынуждена отменить встречу. При попытке возврата средств со счета пользователя снова списывалась сумма за билеты.

Ноябрь 2025 года

Схема: партнерские программы

Описание схемы:

Сценарий мошенничества с продажей деликатесов через интернет. Скамеры создали сеть из 30+ Telegram-каналов, через которые предлагали купить икру и морепродукты с Дальнего Востока и Севера России.

Пользователей приглашали в фейковые магазины через домовые и районные чаты, размещали рекламу в Telegram, а также создавали клоны официальных поставщиков.

Когда пользователь писал автору сообщения, ему присылали приглашение в чат с «ценами и наличием». Оформить заказ можно было только через личное сообщение «менеджеру», который просил указать Ф. И. О., адрес, телефон и состав заказа. Перевести деньги требовали по номеру телефона или карты мошенника.

В подтверждение оплаты злоумышленник просил прислать банковскую квитанцию. После оплаты «менеджер» переставал выходить на связь или блокировал пользователя.

Декабрь 2025 года

Схема: вредоносные программы

Описание схемы:

Android-троян маскировали под расширенные и «18+»-версии приложений YouTube и TikTok.

Злоумышленники создали сеть вредоносных сайтов, маскирующихся под бренды зарубежных видеохостингов, на которых рекламировали вредоносные приложения, обещая пользователям «бесплатно» просмотр видео даже с плохим интернетом и без рекламы, доступ к заблокированному контенту, скачивание в 4K для просмотра офлайн и фоновый режим для прослушивания контента. Чтобы получить эти расширенные возможности, пользователь должен был скачать APK-файл — замаскированный под полезное приложение Android-троян.

Обзор самых популярных мошеннических схем в Республике Беларусь

В 2025 году эксперты F6 провели анализ ландшафта угроз в Республике Беларусь. В число самых популярных схем интернет-мошенничества, которые злоумышленники используют против пользователей в Беларуси, вошли вошли инвестскам, розыгрыши от имени банков, угон и блокировка iPhone.

Инвестскам

Приемы привлечения потенциальных жертв в России и Беларуси схожи: в качестве приманки для трафика на мошеннические ресурсы чаще всего использовали известные бренды или образы публичных личностей. Одна из самых распространенных ловушек — фейковые новости со ссылкой на несуществующие заявления главы государства, обещания дивидендов от продажи природных ресурсов.

Розыгрыши от имени банков

«Дарим нашим клиентам X рублей на карту» — такую рекламу-приманку с одинаковой вероятностью могли увидеть пользователи как в России, так и в Беларуси. Под этим предлогом пользователям предлагали пройти опрос или принять участие в розыгрыше, а для получения денег — авторизоваться в личном кабинете своего банка. После ввода учетных данных на фишинговой странице злоумышленники получали полный доступ к банковскому счету пользователя.

Угон аккаунтов Telegram и WhatsApp

Киберпреступники вели охоту на пользователей иностранных мессенджеров в России и Беларуси по одним и тем же сценариям. Одна из самых популярных приманок для угона аккаунтов — фейковое голосование. Аналитики F6 прогнозируют, что в ближайшее время масштаб фишинговых атак на пользователей Telegram в Беларуси может значительно усилиться. Причина в изменениях, которые происходят в сфере угона Telegram-аккаунтов.

Угон банковских аккаунтов через Telegram-боты

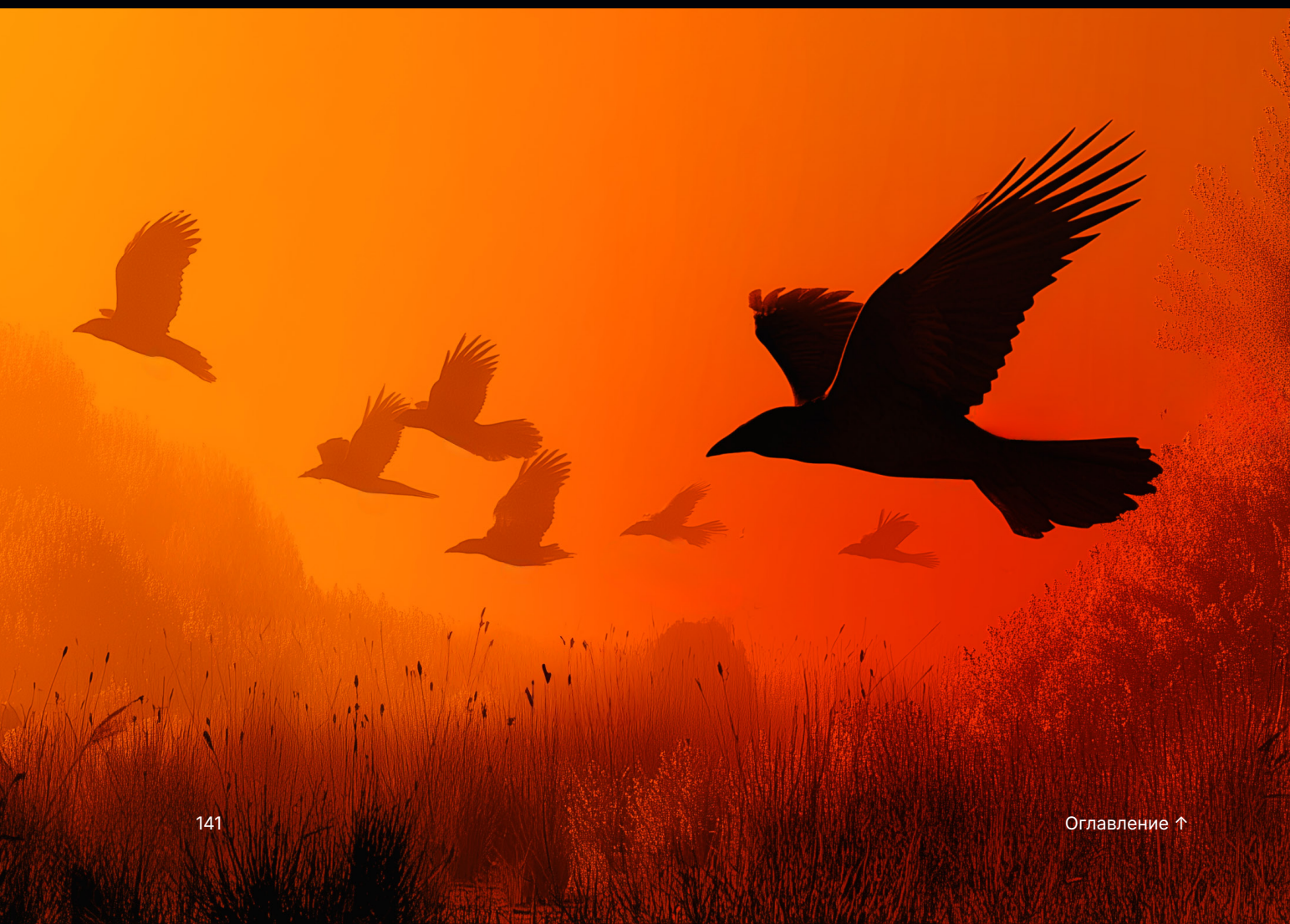
Среди мошеннических схем, по которым атаковали пользователей в Беларуси, аналитики F6 обнаружили и уникальные, те, которые в России не встречались или не получили широкого распространения, такие как фишинг (угон) банковских аккаунтов через Telegram-боты.

Блокировка iPhone через авторизацию в iCloud злоумышленника

Три самых популярных у злоумышленников сценария:

- знакомства, продажа игровых аккаунтов с привязкой через iCloud;
- фейковые вакансии;
- фейковые компенсации от государства.

Атаки на Android-устройства



Большая часть угроз для пользователей Android-устройств 2024 года осталась актуальной и в 2025-м. Основным способом распространения вредоносных программ для Android являются сообщения, которые побуждают пользователей скачать зараженные APK-файлы под видом популярных приложений, фото- и видеоархивов. По данным F6, на ВПО **Mamont** приходится **47%** заражений Android-устройств в России. По итогам 2025 года этот троян вышел на первое место, опередив ВПО на основе **NFCGate** по количеству скомпрометированных устройств и ущербу для пользователей.

Как показывает практика, многие киберугрозы, которые появляются за рубежом, со временем становятся актуальны и для российских пользователей. Так, первые версии ВПО на основе NFCGate изначально были обнаружены в других странах, а потом уже стали использоваться и в России. Специалисты F6 ожидают дальнейшего развития такого типа ВПО, в частности, прогнозируют модификацию **RatOn** для использования против клиентов российских банков.

Самый необычный способ распространения в 2025 году был замечен у ВПО **Triada**. Троян поставлялся в новых Android-устройствах, которые оказались заражены еще перед продажей. Вероятно, один из этапов цепочки поставок был скомпрометирован, а онлайн-магазины могли быть не осведомлены, что распространяют поддельные устройства, зараженные трояном Triada.

Mamont

Вредоносное Android-приложение Mamont в 2025 году стало одной из главных угроз для клиентов российских банков.

За два года с момента обнаружения возможности Mamont изменились, а киберпреступники автоматизировали процессы реализации атаки. Позже мошенники упростили схему распространения ВПО и в 2025 году заражали устройство жертвы с использованием прямой фишинговой рассылки вредоносного файла без публикации в магазинах приложений.

Атака чаще нацелена на открытые группы в мессенджерах, например на домовые чаты. Также для распространения фишинговых ссылок и вредоносных файлов через мессенджеры и СМС мошенники используют скомпрометированные устройства. Троян распространяется под видом папок фото и видео, списков погибших, раненых и пленных участников СВО, антивирусов и др.

Сразу после установки вредоносное ПО запрашивает разрешение на установку в качестве основного приложения для обмена СМС по умолчанию. Это разрешение требуется вредоносной программе для дальнейшей работы с СМС на устройстве жертвы. После установки Mamont отправляет сообщение злоумышленникам об успешном запуске и подключении устройства.

В результате модернизации вредоносной программы злоумышленники увеличили перечень атакуемых приложений пользователя, усовершенствовали функциональность обработки перехваченных СМС и управления устройствами жертв, поставив атаки на пользователей Android-устройств на поток.

ВПО на основе NFCGate и обратная версия

С августа 2024 года специалисты F6 Fraud Protection фиксируют использование вредоносных версий легитимного Android-приложения **NFCGate** в атаках на клиентов ведущих российских банков. В 2025 году киберпреступники продолжили совершенствовать

и расширять функциональность ВПО, в котором применяются технологии NFC.

По итогам 2025 года общий ущерб от использования всех вредоносных версий NFCGate против российских пользователей превысил **1,6 млрд руб**. В конце января 2025 года киберпреступники начали применять версию приложения, способную перехватывать СМС и push-уведомления с устройств жертв. В феврале злоумышленники стали активно проводить атаки с использованием связки **CraxsRAT** и NFCGate, которая позволяла устанавливать вредоносный софт для дистанционного перехвата и передачи NFC-данных банковских карт без единого звонка.

Весной 2025 года специалисты F6 Fraud Protection зафиксировали появление принципиально новой версии NFCGate, которая применяется в так называемой обратной схеме. В отличие от первых вредоносных модификаций приложения, которые в режиме реального времени передавали NFC-данные карты жертвы на устройство злоумышленника и позволяли ему снять деньги со счета пользователя через банкомат, изменился вектор передачи информации. В обратной версии NFCGate приложение использовало возможность ретрансляции NFC-трафика для передачи на устройство пользователя данных карты дропа. Когда в результате атаки мошенников пользователь подходил к банкомату, чтобы зачислить деньги на свой счет, он прикладывал смартфон к NFC-модулю банкомата, но вместо своей карты авторизовывался картой дропа, которому и отправлялась вся сумма.

В мае специалисты F6 зафиксировали в России первые попытки атак с использованием ВПО **SuperCard** — новой версии NFCGate для глобального киберкриминала. Это ВПО позволяло злоумышленникам похищать данные банковских карт путем перехвата NFC-трафика для последующего хищения денег с банковских счетов пользователей. В России использование таких модификаций злоумышленниками носило ограниченный характер, в то время как крупные кампании по их распространению были зафиксированы в Бразилии.

В сентябре 2025 года исследователи обнаружили в Чехии ВПО **RatOn**, которое включало в себя не только функциональность перехвата NFC-трафика банковских карт, но и широкий набор иных возможностей. Они позволяли злоумышленникам совершать кражу денег с банковского счета, не привлекая внимания пользователя, а также скомпрометировать данные на устройстве. Образец RatOn, проанализированный специалистами F6, был предназначен для атак на пользователей в Чехии, однако функциональность приложения поддерживала возможность работы с приложениями на русском языке. Так как предыдущие вредоносные версии NFCGate, обнаруженные первоначально в других странах, использовались в атаках на российских пользователей, специалисты F6 ожидают дальнейшую модификацию RatOn для использования против клиентов российских банков.

CraxsRAT

Специалисты F6 продолжают отслеживать активность, связанную с распространением ВПО **CraxsRAT**.

В марте 2025 года были выявлены факты одновременного использования ВПО CraxsRAT и легитимного ПО NFCGate в атаках на российских пользователей. Мошенникам больше не нужно звонить пользователям и убеждать жертву установить приложение, как это было в более ранних атаках. Злоумышленники предпочитали использовать троян CraxsRAT для доставки NFCGate на устройства пользователей. На это указывает увеличение доли устройств, на которых одновременно использовались CraxsRAT и NFCGate. Кроме того, специалисты F6 обнаружили на андеграундных форумах объявления об аренде вредо-

носного ПО, объединяющего возможности этих приложений.

Атаки brabus156

Летом 2025 года специалисты F6 обнаружили активность по распространению СМС-стилера для Android, маскирующегося преимущественно под различные банковские приложения и сервисы для оплат. Среди целевых стран — Россия, Беларусь, Узбекистан, Казахстан. Злоумышленникам, стоящим за распространением этого ВПО, мы присвоили имя brabus156 по используемой ими почте для регистрации инфраструктуры.

При установке такого вредоносного приложения на устройство сначала отображается WebView-ссылка, где размещена форма для заполнения данных — поля для ввода номера телефона и пароля от личного кабинета. На следующем шаге приложение запрашивает ряд прав, проверяет IP-адрес жертвы и отправляет информацию о зараженной системе в Telegram. Успешная установка приложения позволяет злоумышленникам любое полученное сообщение отправлять в Telegram. Эксфильтрация СМС-сообщений реализована через Telegram-бота, первая активность которого датируется ноябрем 2022 года. Скомпрометированный логин и пароль от приложений и доступ к СМС позволяют злоумышленникам выводить деньги с карт и счетов жертвы.

BONVI TEAM

Впервые Android-троян DeliveryRAT мы упоминали в предыдущем годовом отчете F6. Сервис BONVI TEAM распространял троян **DeliveryRAT** по модели MaaS минимум с августа 2024 года. На протяжении 2025 года специалисты F6 фиксировали регистрацию новой вредоносной инфраструктуры злоумышленников и успешно блокировали ее.

Кроме того, в апреле 2025 года специалисты F6 Threat Intelligence раскрыли обновленную версию трояна DeliveryRAT, которая использовалась злоумышленниками во второй половине года. В обновленную версию были добавлены следующие функциональные возможности:

- запуск по команде различных видов активностей для пользователя, в контексте которых присутствуют ввод информации о банковской карте, выбор фотографии, сканирование QR-кода и т. д.;
- выполнение DDoS-атак путем отправки одновременных запросов к переданной командой URL-ссылке;
- эксфильтрация списка контактов;
- рассылка СМС всем контактам;
- возможность обмениваться сообщениями с жертвой под видом поддержки (в разработке / отключено билдером).

Triada

В марте 2025 года исследователи обнаружили новые версии трояна **Triada** в Android-устройствах, которые оказались заражены еще перед продажей. В известных случаях заражения прошивка устройств имела отпечаток сборки, отличающийся от отпечатков официально опубликованных прошивок. Подделки под смартфоны известных брендов распространялись через онлайн-магазины. Вероятнее всего, один из этапов цепочки поставок был скомпрометирован, и онлайн-магазины могли не подозревать, что распространяют поддельные устройства, зараженные Triada. Специалисты обнаружили более 4500 зараженных устройств по всему миру, из которых почти 3500 — в России. Согласно данным исследователей, с середины 2024 года до момента обнаружения на подконтрольные злоумышленникам криптокошельки было выведено более $264 000 в различных криптовалютах.

Копия трояна Triada попадает в каждое приложение при его запуске на зараженном устройстве. В основе ВПО лежит модульная архитектура, поэтому атакующие получают полный контроль над системой жертвы, включая возможность адаптировать функциональность под конкретные приложения. В ходе анализа модулей встречались комментарии на китайском языке, из чего специалисты делают вывод, что разработчики являются носителями китайского.

Изученные полезные нагрузки в текущей версии Triada, в зависимости от приложения, в котором они работают, меняют адреса криптокошельков при попытке перевода криптовалюты, подменяют ссылки в браузерах, отправляют произвольные СМС и перехватывают ответы на них, а также похищают учетные данные от мессенджеров и социальных сетей.

Lazarus Stealer

В августе 2025 года исследователями обнаружена вредоносная кампания, связанная с распространением ВПО **Lazarus Stealer** для Android.

ВПО замаскировано под приложение GiftFlipSoft и нацелено на пользователей российских банковских приложений. При запуске вредоносная программа предлагает пользователю установить его как приложение для отправки СМС по умолчанию. Сразу после этого отображается всплывающее уведомление, в котором пользователю предлагается предоставить дополнительные разрешения, якобы необходимые для корректной работы приложения. Эти разрешения дают ВПО возможность перехватывать и отправлять входящие СМС, отслеживать работу программ в реальном времени, чтобы находить целевые банковские приложения. ВПО может создавать поддельные интерфейсы для официальных приложений, чтобы получить доступ к конфиденциальным данным.

Если Lazarus Stealer обнаруживает на устройстве жертвы приложение целевого банка, оно использует разрешение Draw Over Other Apps, чтобы отобразить на экране поддельную страницу банка. Наложенная картинка содержит поддельное предупреждающее сообщение, например: «Внимание! Замечена подозрительная активность. Для подтверждения учетной записи введите номер карты», чтобы обманом заставить пользователя предоставить конфиденциальную банковскую информацию или ввести реквизиты учетной записи. ВПО незаметно собирает номера карт, PIN-коды и другие личные данные.

С2 ВПО представлен в виде панели с доступом по реквизитам рис. 36.

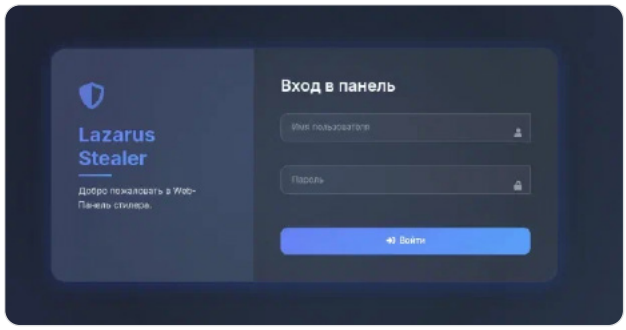


Рис. 36 — Административная панель Lazarus Stealer

В ходе анализа ВПО специалисты F6 обнаружили семь целевых мобильных приложений, пять из которых являются банковскими, одно относится к сфере предоставления государственных услуг и одно — к сфере торговли.

Кроме того, в ходе исследования образца ВПО Lazarus Stealer обнаружена информация об абонентском номере и ID пользователя мессенджера Telegram, которые, согласно логике программы, также получают информацию, похищенную с использованием ВПО. Данные пользователи связаны с Telegram-каналом, через который распространяется ВПО Lazarus Stealer.

LunaSpy

Исследователи обнаружили Android-ВПО **LunaSpy**, распространяющееся под видом антивируса через личные сообщения в мессенджерах. Потенциальной жертве может прийти сообщение с предложением установить ПО как от незнакомца, так и от взломанного аккаунта пользователя из контактов.

Первые версии LunaSpy появились в январе 2025 года, но на протяжении всего года специалисты F6 детектировали новую регистрируемую злоумышленником инфраструктуру и образцы ВПО. Эксперты полагают, что ВПО предназначено для использования в точечных атаках. Основной его целью стали представители российского бизнеса.

При первом запуске ВПО запрашивает доступ ко множеству системных разрешений. Далее вредоносная программа запускает несколько собственных сервисов и ежеминутно проверяет их активность, при необходимости запуская вновь. Через них LunaSpy подключается к C2-серверу и получает одну из следующих команд:

- отправка на сервер входящих и исходящих СМС;
- отправка на сервер списка контактов;
- отправка на сервер списка телефонных вызовов;
- отправка на сервер геолокации;
- активация или остановка потоковой трансляции звука с микрофона устройства;
- активация или остановка потоковой трансляции видео с камеры устройства;
- активация или остановка трансляции с экрана устройства;
- отправка на сервер изображений, хранящихся на карте памяти;
- отправка на сервер изображений с карты памяти по заданному диапазону имен;
- отправка на сервер заданного изображения с карты памяти;
- активация или остановка самозащиты;
- выполнение полученной shell-команды;
- отправка на сервер информации о сети и об интерфейсах устройства.

LunaSpy использует Accessibility Service для реализации функциональности кейлоггера и перехвата содержимого из мессенджеров и браузеров. В ВПО предусмотрена возможность работы с большим

числом управляющих серверов, информация о которых расположена в его конфигурации. Кроме того, в нем существует возможность переключения между хостинг-провайдерами.

Retka Android Trojan

В 2025 году исследователи обнаружили рассылку через Telegram Android-трояна, получившего имя **Retka**. Злоумышленники провоцируют жертву к немедленному запуску мимикрирующего под фото или видео APK-файла. Атакующие работают быстро: после заражения устройства жертвы уже через 13 минут они рассылали ВПО всем контактам в Telegram. Специалисты упоминают связь между двумя троянами **Retka** и **PhotoSmsTrojan**. Однако в результате дополнительного анализа специалисты F6 не выявили признаков, свидетельствующих о том, что данные ВПО были написаны одним и тем же разработчиком или на основе одного исходного кода. Что же касается трояна **PhotoSmsTrojan**, специалисты F6 продолжали наблюдать распространение этого Android-трояна по стандартной прошлогодней схеме — под видом фото и видео.

Retka — Android-ВПО, которое активно минимум с начала 2025 года. Список функциональных возможностей:

- эксфильтрация интересующих операторов ВПО имен установленных приложений на устройство;
- эксфильтрация информации о производителе и версии устройства, а также версии Android;
- одноразовая эксфильтрация содержимого буфера обмена;
- эксфильтрация 14 880 последних СМС с устройства;
- эксфильтрация получаемых на устройство СМС;
- отправка произвольных СМС (потенциально может использоваться для USSD-команд);
- отображение пользователю произвольной WebView-страницы.

WEB-RAT

WEB-RAT Android Trojan — это ВПО, активное минимум с февраля 2025 года. Оно распространяется под видом фото или видео. Троян поддерживает следующие возможности:

- эксфильтрация СМС, получаемых устройством;
- эксфильтрация истории СМС;
- эксфильтрация push-уведомлений, полученных устройством;
- эксфильтрация информации о звонках;
- эксфильтрация информации об устройстве;
- отправка СМС и звонков;
- ретрансляция звонков.

Для управления ВПО злоумышленники используют C2 с панелью управления. Вход в панель сопровождается анимацией с надписью WEB-RAT, вероятно указывающей на внутреннее название трояна (рис. 37).

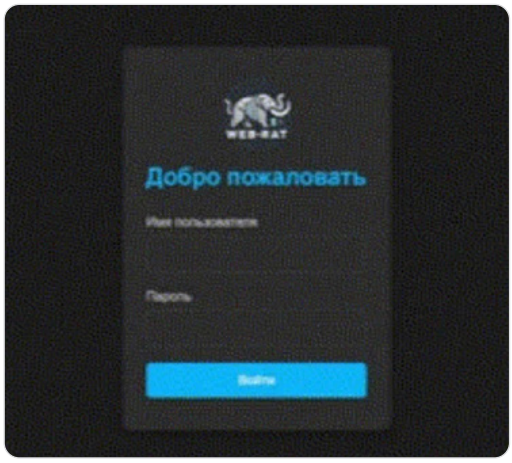


Рис. 37 — Скриншот страницы входа в панель управления C2 WEB-RAT

На одном из управляющих серверов специалисты обнаружили автоматический билдер вредоносных APK. Злоумышленник может указать название, информацию о своем нике и ID, управляющий сервер и WebView-ссылку, которую отобразит приложение при запуске.

FunnyBranchTrojan

С июня 2025 года злоумышленники распространяли Android-ВПО через фейковые Telegram-каналы (рис. 38). Вредоносная программа распространялась под видом приложения для поиска пропавших без вести участников СВО и т. д., причем сопровождалось сообщением с видеоинструкцией по установке приложения.

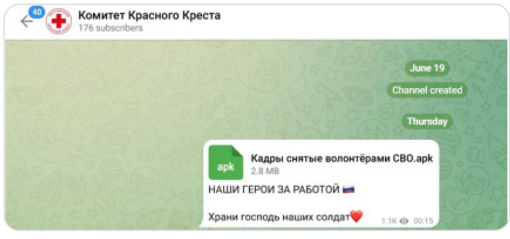


Рис. 38 — Скриншот фейкового Telegram-канала, используемого для распространения FunnyBranchTrojan

Специалисты F6 Threat Intelligence провели анализ распространяемого ВПО и присвоили ему имя **FunnyBranchTrojan**. ВПО написано на языке Kotlin и нацелено на эксфильтрацию СМС-сообщений. В ходе исследования было обнаружено три версии ВПО. Первая появилась весной 2025 года и выполняла эксфильтрацию данных с устройств через Telegram-бот, во второй и третьей версии эксфильтрация выполнялась на C2-сервер по протоколу HTTP.

BT_MOB

BT_MOB — Android-троян, раскрытый в начале 2025 года, продавался в Telegram-канале по схеме MaaS.

Осенью злоумышленники распространяли ВПО через фейковые домены, замаскированные под антирадар-сервис, транспортные компании и приложение для поиска пропавших на СВО.

Троян предоставляет злоумышленникам доступ к данным устройства (логам, журналам, буферу обмена, приложениям и файлам), имеет возможность ведения скрытой аудио- и видеозаписи, трансляции экрана устройства. ВПО поддерживает возможности кейлоггера и кражи учетных данных. BT_MOB использует WebSocket для выполнения команд в режиме реального времени и кражи данных.

Gorilla Android RAT

Gorilla Android RAT — многофункциональный банковский троян, написанный на Kotlin. Первые сообщения о продаже трояна появились в киберпреступных сообществах в конце февраля 2025 года. Из особенностей авторы отмечали СМС-менеджмент, управление устройствами, определение банковских

приложений, интеграцию с Telegram. Также у трояна был собственный Telegram-канал, в котором публиковались новости, и отдельный демонстрационный канал с информацией о функциональности с примерами работы приложения.

Подключение к C2-серверу выполняется по протоколу WebSocket. К серверу доступно также подключение по протоколу HTTP, так как на нем находится веб-панель Gorilla Panel для работы с зараженными устройствами.

В марте 2025 года троян распространялся через Telegram. В августе 2025 года управляющие серверы трояна и Telegram-канал уже были неактивны. Исследователи полагают, что автор ВПО был задержан.

ClayRAT

ClayRAT — Android-троян, обнаруженный в 2025 году. Поддерживает возможность получения и отправки СМС, имеет доступ к журналу вызовов и уведомлениям, собирает информацию об устройстве жертвы, способен делать фронтальные фотографии и совершать звонки с устройства жертвы.

С июля 2025 года исследователи фиксируют распространение Android-трояна ClayRAT. Кампания была нацелена как минимум на Россию и Беларусь. Злоумышленники распространяют ВПО через Telegram и фишинговые сайты, маскируя его под популярные приложения, например WhatsApp, Google Photos, TikTok и YouTube. ClayRAT также может распространяться через СМС: вредоносные ссылки рассылаются всем контактам в телефонной книге зараженного устройства.

В нескольких известных случаях злоумышленники регистрировали домены, которые очень точно имитировали страницы легитимных сервисов. С этих сайтов-двойников посетители перенаправлялись на каналы Telegram, где размещался вредоносный APK-файл или ссылка на его загрузку. Для повышения успешности установки вредоносное ПО часто сопровождалось простыми пошаговыми инструкциями, побуждающими пользователей обходить встроенные предупреждения безопасности Android. Операторы заполняли эти Telegram-каналы контентом: фейковыми положительными комментариями, завышенным количеством загрузок и фальшивыми отзывами пользователей, призванными снизить подозрения.

Чтобы обойти средства защиты, появившиеся в новых версиях Android, некоторые образцы ClayRAT действуют как дропперы. Видимое приложение представляет собой легковесный установщик, отображающий поддельный экран обновления магазина Android-приложений, в то время как зашифрованная полезная нагрузка скрыта в ресурсах приложения. Этот метод установки увеличивает вероятность того, что посещение веб-страницы приведет к установке ВПО.

Утечки данных

В 2025 году аналитики Threat Intelligence компании F6 зафиксировали на андеграундных форумах и в тематических Telegram-каналах появление 250 новых случаев публичных утечек баз данных компаний из России и СНГ. Для сравнения: в 2024-м выявлено 455 случаев утечек.

Суммарно утечки баз данных 2025 года содержали **более 767 млн строк** с данными российских пользователей. Как и ранее, большинство похищенных баз данных преступники выкладывали в публичный доступ бесплатно для нанесения наибольшего ущерба компаниям и их клиентам.

Статистика по утечкам

В данном разделе представлена статистика по количеству опубликованных баз данных в 2025 году. Стоит указать, что большинство из них были намеренно выложены в открытый доступ для привлечения как можно большего внимания со стороны киберпреступников. Однако часть утечек, аналогично 2024 году, все так же не появлялась в публичном пространстве, а распространялась или продавалась приватно.

Сравнение количества утекших строк с данными пользователей в 2023–2025 годах

Год	Количество утекших строк
2023	**296 000 000**
2024	**457 577 054**
2025	**767 590 322**

Наибольший интерес у киберпреступников вызывают случаи публикации в открытом доступе электронных почтовых адресов, телефонных номеров и паролей пользователей. Злоумышленники по-прежнему крайне заинтересованы в публикациях, содержащих чувствительную информацию, которую они впоследствии могут использовать в мошеннических схемах и для совершения каскадных атак на крупные компании. Из общего количества утекших данных **315 302 053** записи содержали электронные адреса, причем только **88 600 596** из них были уникальными. Также зафиксировано, что **156 105 438** записей содержали пароли пользователей, среди которых только **142 044 282** являлись уникальными. Записей с телефонными номерами насчитывается **794 975 692**, из которых уникальных всего **149 207 493**.

Количество утекших баз данных компаний из России и СНГ в 2023–2025 годах

Год	Количество утекших баз данных
2023	**246**
2024	**455**
2025	**250**

Как и годом ранее, в 2025 году злоумышленники чаще всего публиковали в открытом доступе данные, связанные с коммерцией: данные крупных российских маркетплейсов, интернет-магазинов и т. д. Государственный сектор занял второе место по количеству опубликованных баз данных. Веб-сайты компаний, предоставляющих профессиональные услуги, заняли третье место. Также в зону повышенного внимания попали сферы информационных технологий и здравоохранения.

Публикация утечек баз данных по отраслям в 2023–2025 годах

Отрасль	2023	2024	2025
Коммерческая сфера	**51**	**216**	**89**
Государственный сектор	**—**	**—**	**17**
Профессиональные услуги	**—**	**—**	**14**
Сфера информационных технологий	**—**	**—**	**13**
Здравоохранение	**14**	**37**	**12**

Тренды, связанные с утечками данных

Злоумышленники продолжают активно публиковать базы данных в Telegram

В 2025 году специалистами F6 Threat Intelligence было зафиксировано практически в **4** раза больше публикаций баз данных российских компаний в Telegram, чем на тематических форумах. Напомним, что в 2024 году **62,27%** всех публикаций приходилось на Telegram.

Одна из причин заключается в том, что в Telegram любой пользователь может создать тематический канал, тогда как на теневых форумах присутствует строгий регламент для ведения деятельности. Доступность данного мессенджера и закрытие ряда известных теневых площадок, где раньше публиковали базы данных, подтолкнули часть злоумышленников перейти в Telegram.

Еще одним фактором, способствующим переходу, является отсутствие явных ограничений на публикацию контента: злоумышленники по-прежнему публикуют как старые утечки, так и свежевыгруженные базы. При этом нередко теневые продавцы в Telegram продолжают намеренно вводить пользователей в заблуждение в попытке заработать на публично доступных данных, не рискуя своей репутацией в комьюнити. Тем не менее теневые форумы вряд ли исчезнут полностью: многие киберпреступники до сих пор предпочитают проводить сделки традиционным способом, пользуясь услугой гарант-сервисов и работая только с проверенными продавцами. Вместе с тем нельзя игнорировать тот факт, что для некоторых злоумышленников Telegram стал основной площадкой для распространения скомпрометированных данных.

Сравнительная статистика по количеству публикаций в Telegram и на форумах в 2024 и 2025 годах

Место публикации	2024	2025
Telegram	**326**	**205**
Форумы	**129**	**45**
Общее количество	**455**	**250**

Стало больше Telegram-каналов, публикующих приватные базы данных

В 2024 году активно появлялись новые Telegram-каналы, где злоумышленники выкладывали в публичный доступ приватные базы данных, приобретенные у других представителей киберпреступного сообщества.

В 2025 году этот способ распространения получил дальнейшее развитие. В отдельный тренд можно выделить создание и ведение подобных тематических каналов, которые занимаются распространением баз данных ограниченному кругу лиц. Актуальность баз данных может варьироваться: в открытом доступе могут оказаться как относительно свежие данные, так и базы, скомпрометированные за несколько лет до того, как стали общедоступными. В 2025 году было замечено **9** баз данных, которые впервые стали публичными, но были скомпрометированы в предыдущие годы.

Количество баз данных, скомпрометированных ранее, но опубликованных в открытом доступе в 2025 году

Год	Количество
2024	**2**
2023	**4**
2022	**2**
2018	**1**

Стало больше публикаций баз данных госсектора

В 2025 году увеличилось количество утечек информации из государственных сервисов. Если в 2024 году их было **11**, то за 2025 год злоумышленники опубликовали **17** новых утечек. По объему данных утечки госсервисов составили более **62%** от всех опубликованных записей. Стоит отметить, что некоторые сервисы подверглись утечкам в предыдущие годы.

Среди опубликованных записей были представлены такие данные, как ФИО, номера телефонов, адреса электронной почты, хешированные пароли, физические адреса, даты рождения, паспортные данные, налоговая информация, образование и места работы.

Утечки баз данных в России

В 2025 году аналитики Threat Intelligence компании F6 зафиксировали на андеграундных форумах и в тематических Telegram-каналах **230** новых случаев публичных утечек данных компаний из России.

В списке топ-5 самых объемных (по количеству строк) утечек 2025 года находятся 4 госсервиса: на них в сумме приходится около **600 млн строк**.

Мегаутечка, состоящая из 457 баз данных

Наши специалисты проанализировали данные, опубликованные в мегаутечке, состоящей из **457** различных баз данных. Среди них только **24** действительно являются ранее неизвестными утечками, в то время как остальные представляют собой либо уже известные утечки, либо компиляции данных из открытых источников. Суммарно в этих 24 утечках содержится порядка **500 тыс.** записей, которые касались следующих отраслей:

Отрасль	Количество
Розничная торговля	**11**
Муниципальные сайты и блоги	**6**
Интернет-услуги	**4**
Другие категории	**3**

Злоумышленники, публикующие данные на теневых ресурсах

TEST

Злоумышленник под псевдонимом TEST (@testing_BD) занимается продажей баз данных в Telegram с 23 декабря 2024 года. Скриншот профиля злоумышленника в мессенджере представлен на рис. 39.

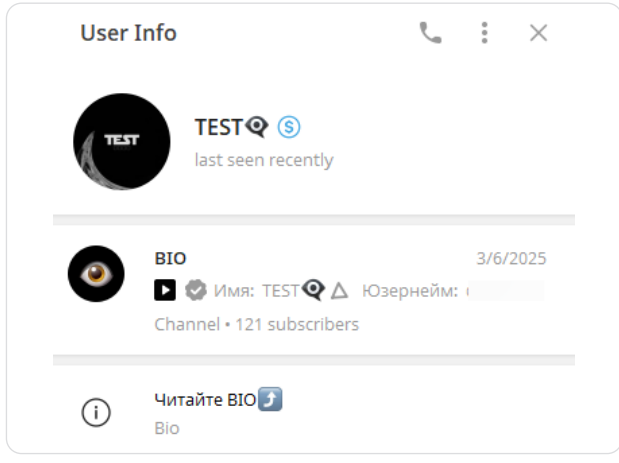


Рис. 39 — Скриншот профиля злоумышленника TEST в Telegram

Излюбленная тактика киберпреступника — публикация данных, выгруженных, предположительно, из CRM-систем. Пользователь является администратором и, вероятно, создателем Telegram-форума Umbrella Forum.

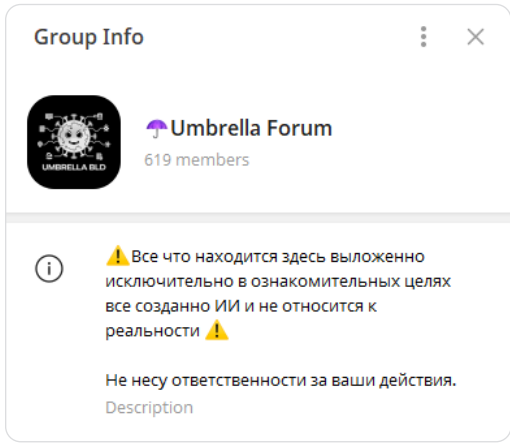


Рис. 40 — Скриншот канала злоумышленника TEST в Telegram

В 2025 году специалистами F6 Threat Intelligence было зафиксировано **67** случаев публикаций баз данных российских компаний злоумышленником TEST. Как было отмечено выше, во всех случаях данные были, предположительно, выгружены из CRM-систем пострадавших.

22 августа 2025 года канал злоумышленника TEST, где периодически публиковались базы данных, был заблокирован администрацией Telegram. Вскоре после этого киберпреступник создал новый канал на замену заблокированному, но активность в нем кратно снизилась, а публикации практически прекратились, чтобы избежать повторной блокировки за нарушение правил платформы Telegram.

Распределение по отраслям утечек, опубликованных злоумышленником TEST, за период анализа выглядит следующим образом:

Отрасль	Количество баз данных	Количество строк
Ретейл и интернет-магазины	**19**	**1 850 000**
Профессиональные услуги	**10**	**117 000**
Производство	**8**	**21 000**
Информационные технологии	**6**	**92 000**
Другие отрасли	**24**	**413 000**
Всего	**67**	**2 493 000**

CyberSec's

CyberSec's — хактивистская группа, которая специализируется на кибердиверсиях и саботаже против российских компаний. Среди их методов — DDoS-атаки, компрометация инфраструктуры, публикация скомпрометированных данных, атаки через подрядчиков. С конца 2024 года злоумышленники начали также совершать атаки с использованием программ-вымогателей. Скриншот с описанием канала представлен на рис. 41.

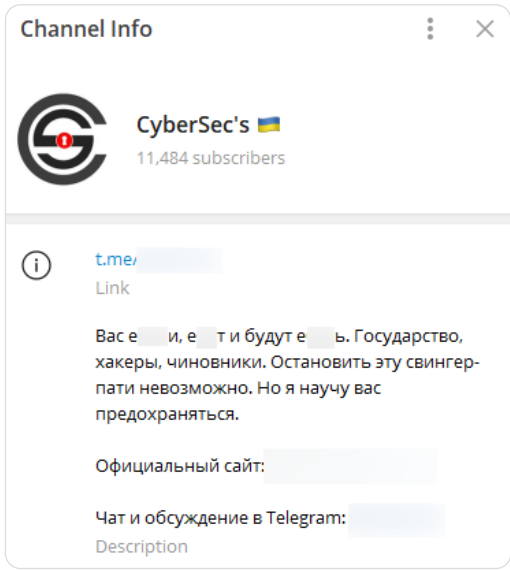


Рис. 41 — Скриншот канала злоумышленника CyberSec's в Telegram

В 2025 году специалистами F6 Threat Intelligence было зафиксировано **15** случаев публикаций баз данных российских компаний злоумышленником CyberSec's из отраслей ретейла, государственных услуг и телекома, содержащих в общей сложности **1,44 млн строк**.

Отрасль	Количество баз данных	Количество строк
Ретейл и интернет-магазины	**8**	**386 000**
Государственный сектор	**3**	**69 000**
Другие отрасли	**4**	**985 000**
Всего	**15**	**1 440 000**

Hdr0

Hdr0 — это хактивистская группировка, появившаяся в декабре 2022 года. Основная активность группы ведется в одноименном Telegram-канале (по состоянию на сентябрь 2025 года группа все еще оставалась активной).

Стоит указать, что 26 октября 2025 года, а затем еще и 1 декабря 2025 года администрация мессенджера заблокировала Telegram-каналы Hdr0. Группировка сообщила об этом в своем аккаунте в X (Twitter) и пообещала воссоздать канал в другом мессенджере, однако на конец 2025 года каких-либо новых ресурсов так и не было создано.

В 2025 году специалистами F6 Threat Intelligence было зафиксировано **14** случаев публикаций баз данных российских компаний злоумышленниками Hdr0 из отраслей ретейла, государственных услуг и образования, содержащих в общей сложности **1,04 млн строк**.

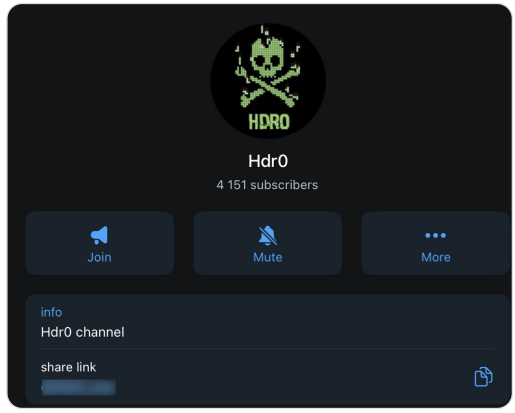


Рис. 42 — Скриншот канала группировки Hdr0 в Telegram

Отрасль	Количество баз данных	Количество строк
Образование	**4**	**14 000**
Ретейл и интернет-магазины	**3**	**816 000**
Государственный сектор	**3**	**120 000**
Другие отрасли	**4**	**90 000**
Всего	**14**	**1 040 000**

Sophia

Sophia — это злоумышленник, публикующий базы данных на андеграундных форумах. Скриншот профиля, зарегистрированного 5 сентября 2024 года на одной известной площадке, представлен на рис. 43.

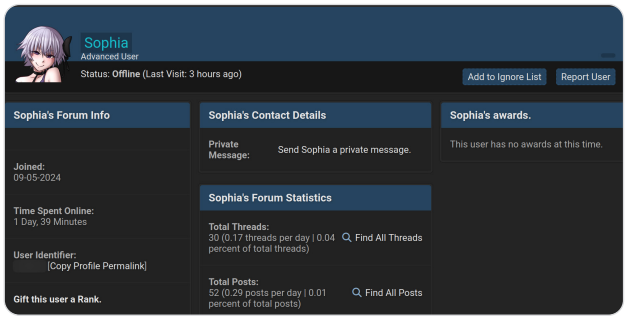


Рис. 43 — Скриншот профиля злоумышленника Sophia на андеграундном форуме

В 2025 году специалистами F6 Threat Intelligence было зафиксировано **11** случаев публикаций баз данных российских компаний злоумышленником Sophia из отраслей ретейла и информационных технологий, содержащих в общей сложности **77 тыс. строк**.

Злоумышленник также продает базы данных и делится их образцами на форумах.

STORM Data Base

STORM Data Base — это закрытый канал в Telegram, который публикует информацию о слитых базах данных из других каналов и от других злоумышленников. В нем активно публиковались утечки на протяжении 2025 года. Администратором этого Telegram-канала является злоумышленник под псевдонимом WorkBitchRu.

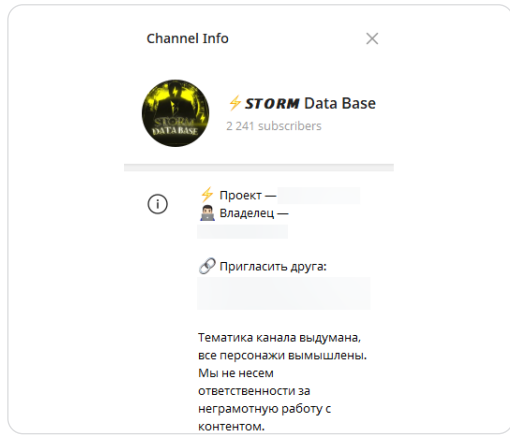


Рис. 44 — Скриншот канала STORM Data Base в Telegram

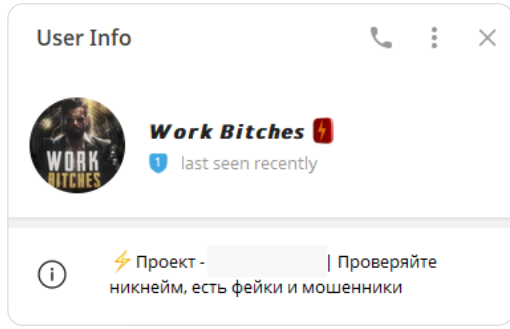


Рис. 45 — Скриншот профиля злоумышленника WorkBitchRu в Telegram

В 2025 году специалисты F6 Threat Intelligence зафиксировали **7** случаев публикаций баз данных российских компаний в канале STORM Data Base из отраслей ретейла, государственных услуг и здравоохранения, содержащих в общей сложности **400 млн строк**.

Береза

«Береза» — это Telegram-канал, в котором злоумышленники публикуют базы данных. Скриншот Telegram-канала представлен на рис. 46.

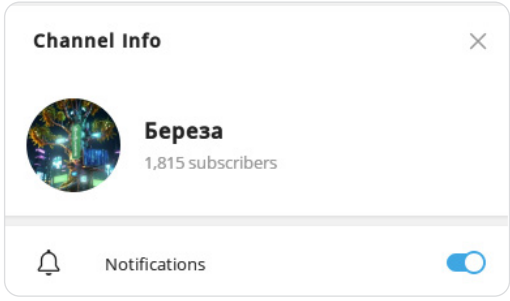


Рис. 46 — Скриншот канала «Береза» в Telegram

Telegram-канал «Береза» публикует как уже ранее слитые базы данных, так и те, которые прежде были приватными. В 2025 году специалистами F6 Threat Intelligence было зафиксировано **7** случаев публикаций баз данных российских компаний в канале «Береза» из отраслей ретейла, государственных услуг и образования, содержащих в общей сложности **56 млн строк**.

Kingsman

Telegram-канал Kingsman, в котором публикуются различные базы данных российских компаний или граждан России, активен с мая 2022 года. Kingsman сотрудничает с другими злоумышленниками, специализирующимися на утечках баз данных. В частности, киберпреступники приватно выкупают базы данных у первоисточников для последующей перепродажи.

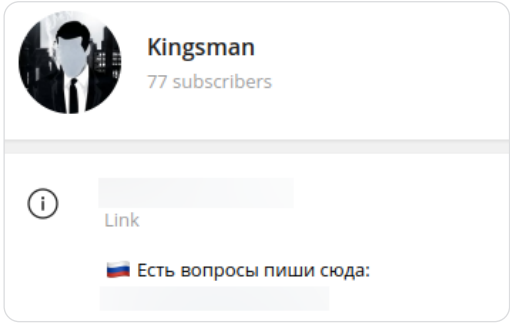


Рис. 47 — Скриншот канала злоумышленника Kingsman в Telegram

В Telegram-канале выкладываются как уже ранее опубликованные утечки баз данных, так и те, которые были только в приватном доступе. В 2025 году специалистами F6 Threat Intelligence было зафиксировано **5** случаев публикаций баз данных (или образцов баз данных) российских компаний злоумышленником Kingsman из отраслей ретейла и образования, содержащих в общей сложности **117 тыс. строк**.

Kedr

Kedr — это закрытый канал в Telegram, который публикует информацию о слитых базах данных из других источников, в том числе полученных от сторонних злоумышленников. Данный канал появился 30 сентября 2025 года. Администратором является злоумышленник под псевдонимом IncognitoBase. Скриншоты канала и профиля администратора представлены на рис. 48 и 49.

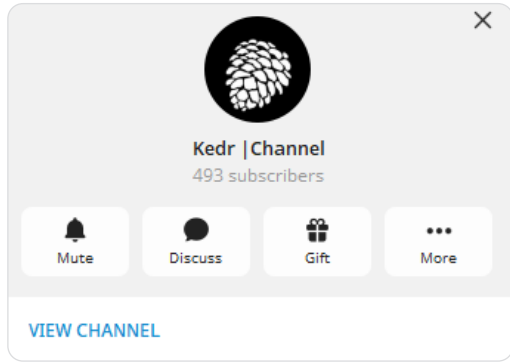


Рис. 48 — Скриншот канала Kedr в Telegram

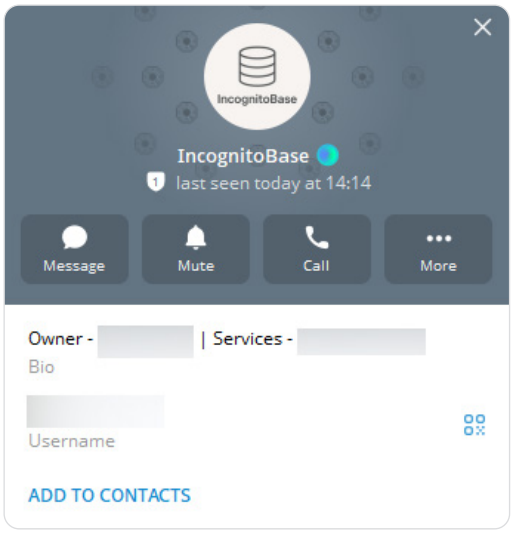


Рис. 49 — Скриншот профиля злоумышленника IncognitoBase в Telegram

В 2025 году специалистами F6 Threat Intelligence было зафиксировано **8** случаев публикаций баз данных российских компаний в канале Kedr из отраслей ретейла и государственных услуг, содержащих в общей сложности **8,67 млн строк**.

Ряд публикаций баз данных, полученных в результате парсинга веб-сайтов

В 2025 году специалистами F6 Threat Intelligence было зафиксировано **7** случаев публикаций баз данных, содержащих порядка **43 млн** записей, которые были собраны путем парсинга веб-страниц с сайтов. Изначально злоумышленниками, публикующими подобные базы, утверждалось, что это результат утечки, однако информация в действительности была получена из открытых источников. Следует учесть, что количество записей, полученных в результате парсинга открытых ресурсов, не включалось в статистику непосредственно по утечкам баз данных.

Утечки баз данных в странах СНГ

В 2025 году аналитики Threat Intelligence компании F6 зафиксировали на андеграундных форумах и в тематических Telegram-каналах **20** новых случаев публичных утечек баз данных компаний из СНГ. **10** из этих новых утечек касаются белорусских организаций, и еще **10** относятся к другим странам СНГ.

Silent Crow заявила об атаке на ресурсы Национальной команды реагирования на киберинциденты Республики Беларусь

26 марта 2025 года группировка Silent Crow в своем Telegram-чате опубликовала сообщение об атаке на cert.by (Национальная команда реагирования на киберинциденты Республики Беларусь), проведенной совместно с группировкой «Белорусские кибер-партизаны». Скриншот сообщения представлен на рис. 50.

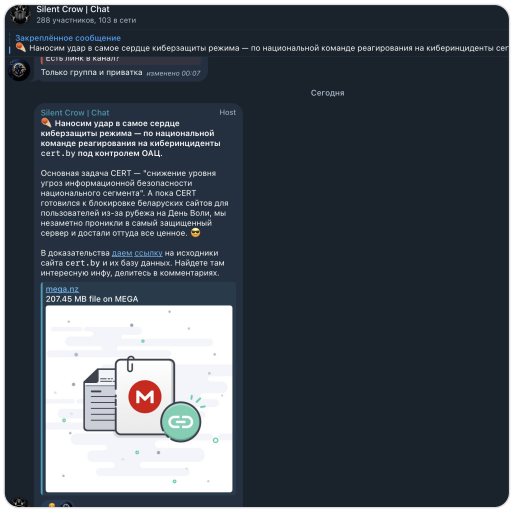


Рис. 50 — Скриншот сообщения об атаке в Telegram-чате Silent Crow

Продажа и последующая публикация данных авиакомпании из СНГ

19 августа 2025 года злоумышленник ByteToBreach опубликовал на хакерских форумах сообщение о продаже данных одной из авиакомпаний в регионе СНГ. Злоумышленник утверждал, что в результате взлома ему удалось получить доступ примерно к 300 Гб данных, в основном выгруженных с S3-сервера. Стоимость данных составляла $9000.

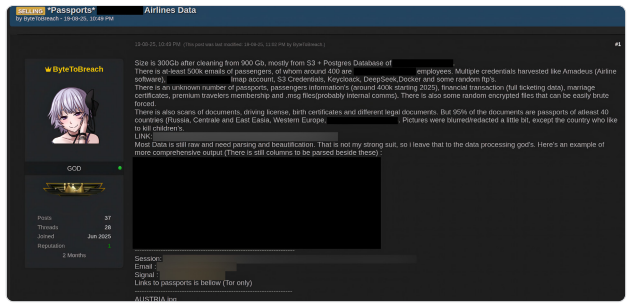


Рис. 51 — Скриншот сообщения на хакерском форуме от злоумышленника ByteToBreach

По словам злоумышленника, утечка данных содержит сканы паспортов и других документов пассажиров авиакомпании из 40 различных стран, включая Россию и другие страны СНГ, страны Западной Европы, Цент-ральной и Восточной Азии.

Среди скомпрометированных данных указывались личные данные **379 тыс.** участников бонусной программы авиакомпании, содержащие имена, даты рождения, телефоны и национальность пассажиров. Отдельно автор отметил, что список электронных почт составляют адреса пассажиров (порядка 500 тыс.) и сотрудников компании (400 корпоративных почт). Кроме того, киберпреступник указал, что получил ключи API и учетные данные для доступа

к различным внутренним сервисам, таким как ПО для аэропортов, серверам, файловым серверам, аккаунту IMAP и т. д.

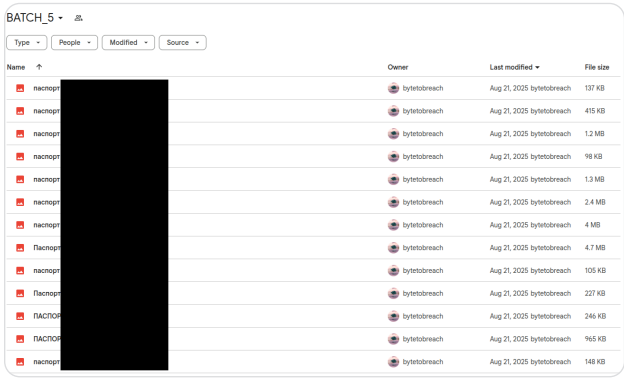


Рис. 52 — Скриншот содержимого папки, предоставленной злоумышленником

21 августа 2025 года авиакомпания в своем заявлении опровергла факт взлома, заявив, что в ходе расследования инцидента несанкционированного доступа к системам выявлено не было. Представители авиакомпании предположили, что опубликованные данные могли быть сгенерированы при помощи нейросетей. После данного заявления злоумышленник начал ежедневно публиковать новые данные из якобы утечки, чтобы опровергнуть предположение об их генерации.

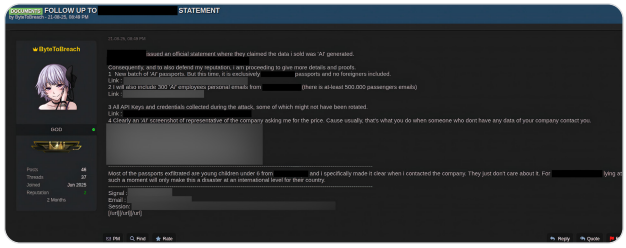


Рис. 53 — Скриншот сообщения злоумышленника о заявлении авиакомпании

Он также приложил переписку в электронной почте якобы с представителями компании, где указал, что готов не публиковать данные за €150 тыс.

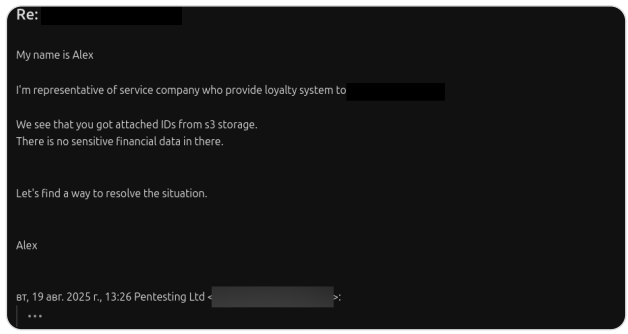


Рис. 54 — Скриншот электронного письма представителя компании, адресованного злоумышленнику

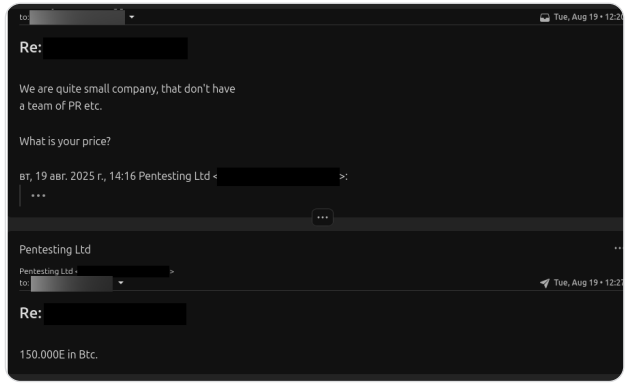


Рис. 55 — Скриншот переписки между компанией и злоумышленником

На протяжении нескольких последующих дней автор активно публиковал в своей теме данные, содержащие сведения о более чем 100 паспортах пассажиров компании.

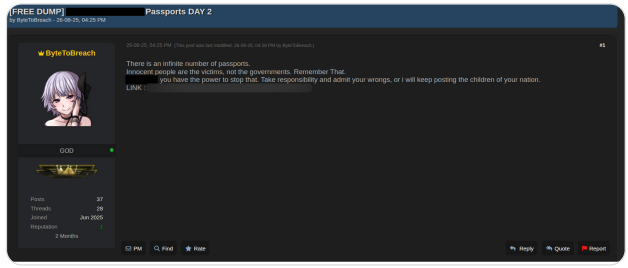


Рис. 56 — Скриншот одного из сообщений злоумышленника о публикации паспортов пассажиров компании

Впоследствии все сообщения (за исключением первых двух) были удалены с форума злоумышленником без указания причин.

Продажа и последующая публикация данных страховой компании в одной из стран СНГ

22 сентября 2025 года злоумышленник ByteToBreach опубликовал на одном из хакерских форумов сообщение о продаже данных компании, работающей в страховой отрасли на территории одной из стран СНГ.

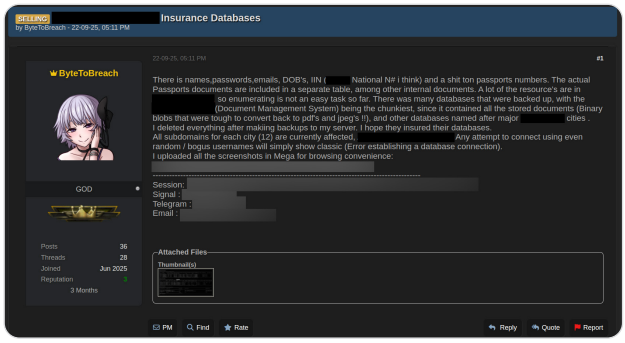


Рис. 57 — Скриншот сообщения злоумышленника на теневом форуме

По словам киберпреступника, утечка данных содержит имена, пароли, адреса электронной почты, даты рождения, национальные удостоверения личности, а также сканы внутренних документов и паспортов.

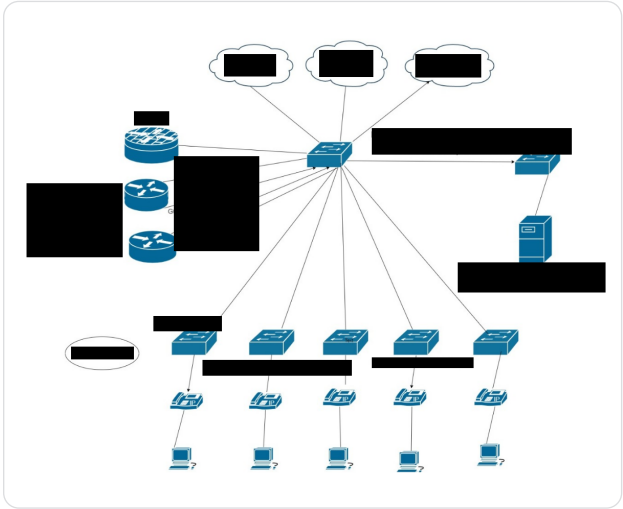


Рис. 58 — Скриншот схемы инфраструктуры, атакованной злоумышленником

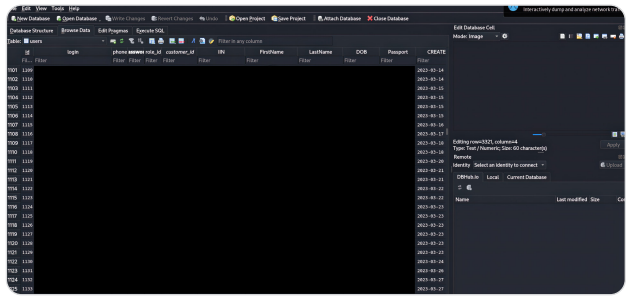


Рис. 59 — Скриншот данных, полученных злоумышленником при атаке компании

Злоумышленник удалил данные с серверов внутренней системы управления документами после создания резервной копии. По его словам, ему удалось конвертировать некоторые двоичные данные в файлы PDF и PNG.

Объявление группировки DumpForums об утечке баз данных Национального банка Республики Беларусь (nbrb.by)

14 ноября 2024 года в Telegram-канале DumpForums было опубликовано заявление злоумышленников о взломе государственного ресурса Национального банка Республики Беларусь (nbrb.by) рис. 60.

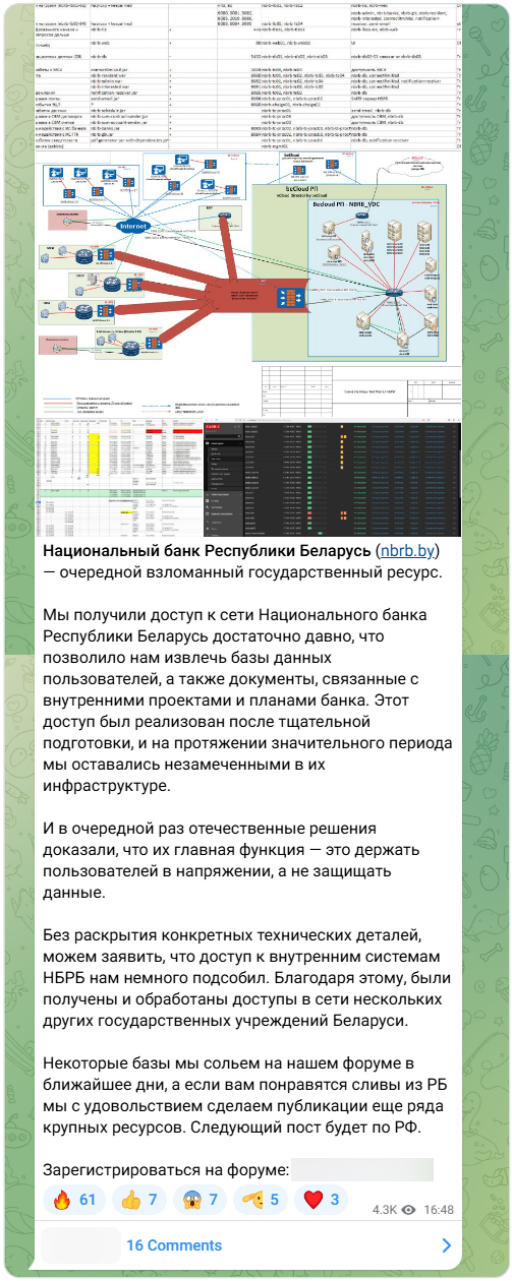


Рис. 60 — Скриншот сообщения об утечке в Telegram-канале злоумышленника

6 марта 2025 года злоумышленник под ником Станислав Дмитриевич опубликовал образец базы данных в одной Telegram-группе, предложив **100 тыс.** доступных записей на продажу. Образец, по его словам, содержит 100 строк данных пользователей: полные имена, номера телефонов, даты рождения и места работы.

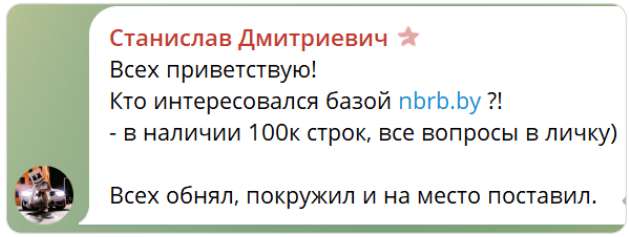


Рис. 61 — Скриншот сообщения о продаже базы данных в Telegram

Продажа баз данных правительственных сервисов других стран СНГ

Продажа данных сайта электронных виз

В сентябре 2025 года произошла утечка данных сайта электронных виз одной из стран СНГ. Данные были выставлены на продажу на теневом ресурсе. Злоумышленником было заявлено, что утечка содержит информацию о людях, пересекающих границу данной страны. По словам продавца, полная база данных содержит порядка **220 млн строк**.

Продажа данных лиц, пересекающих государственную границу

В сентябре 2025 года произошла утечка данных сайта министерства иностранных дел еще одной из стран СНГ. На продажу были выставлены сведения о лицах, въезжавших и выезжавших из страны в период с 2023 по 2025 год. Злоумышленник заявил, что полная база данных содержит около **100 тыс. строк**.

Ряд публикаций злоумышленника TEST

Как было отмечено ранее, злоумышленник TEST активно публикует и выставляет на продажу базы данных различных компаний в своем приватном Telegram-канале. В 2025 году специалистами F6 Threat Intelligence было зафиксировано **6** случаев публикации баз данных злоумышленником TEST по компаниям из стран СНГ, кроме России. Во всех случаях данные были, предположительно, выгружены из CRM-систем пострадавших ресурсов.

- В августе 2025 года злоумышленником TEST были опубликованы данные одного из интернет-магазинов электроники. В результате публикации было раскрыто около **63 тыс. строк** данных: адреса электронной почты, ФИО, даты рождения, физические адреса, номера телефонов, а также системные данные. Из общего числа **1,3 тыс. строк** — это уникальные электронные адреса пользователей.
- welder.by. В июне 2025 года злоумышленником TEST были опубликованы данные ресурса welder.by. Это белорусский сайт Объединенной сварочной компании. В результате публикации было раскрыто около **6,5 тыс. строк** данных: имена, номера телефонов, а также системные данные.
- sitibeton.by. В июне 2025 года злоумышленником TEST были опубликованы данные ресурса sitibeton.by. Это белорусский сайт бетонного завода «СитиБетонСтрой». В результате публикации было раскрыто около **23,6 тыс. строк** данных: имена, номера телефонов, а также системные данные.
- 7video.by. В июне 2025 года злоумышленником TEST были опубликованы данные ресурса 7video.by. Это белорусский сайт компании по продаже и установке видеонаблюдения 7Video. В результате публикации было раскрыто около **149 тыс. строк** данных: адреса электронной почты, ФИО, номера телефонов, а также системные данные.
- alkid.com. В июне 2025 года злоумышленником TEST были опубликованы данные ресурса alkid.com. Это белорусский сайт компании по производству и оптовой продаже битумно-полимерных материалов «Алкид». В результате публикации было раскрыто около **3,3 тыс. строк** данных: адреса электронной почты, ФИО, номера телефонов, а также системные данные. Из общего числа **1 тыс. строк** — это уникальные электронные адреса пользователей.
- artelmebel.by. В мае 2025 года злоумышленником TEST были опубликованы данные ресурса artelmebel.by. Это белорусский сайт фабрики мебели «Артель». В результате публикации было раскрыто около **1,7 тыс. строк** данных: ФИО, номера телефонов, а также системные данные.

Ряд публикаций Telegram-канала «Береза»

Telegram-канал «Береза» публикует как уже ранее известные утечки баз данных, так и те, которые прежде были только в приватном доступе. За период исследования специалистами F6 Threat Intelligence было выявлено **3** публикации баз данных в данном источнике, относящихся к Беларуси.

- 1belagro.by (1belagro.com). В феврале 2025 года была опубликована база

данных, предположительно принадлежащая 1belagro.by — белорусскому сайту группы компаний «Белагро». В июне 2023 года база данных была выставлена на продажу в приватном Telegram-чате. В результате публикации было раскрыто около **21 тыс. строк** данных пользователей: имена, хешированные пароли, электронные почтовые адреса, телефонные номера, а также системные данные. Согласно заявлению злоумышленника, данные актуальны до июня 2023 года.

- yurkas.by. В феврале 2025 года была опубликована база данных, предположительно принадлежащая yurkas.by — белорусскому интернет-магазину входных и межкомнатных дверей «Юркас». В июне 2023 года база данных была выставлена на продажу в приватном Telegram-чате. В результате публикации было раскрыто около **14 тыс. строк** данных пользователей: ФИО, электронные почтовые адреса, телефонные номера, хешированные пароли, даты рождения, а также системные данные. Согласно заявлению злоумышленника, данные актуальны до июня 2023 года.
- alloplus.by. В феврале 2025 года была опубликована база данных, предположительно принадлежащая alloplus.by — белорусскому интернет-магазину смартфонов «Алло». В июне 2023 года база данных была выставлена на продажу в приватном Telegram-чате. В результате публикации было раскрыто около **16 тыс. строк** данных пользователей: ФИО, электронные почтовые адреса, телефонные номера, хешированные пароли, а также системные данные. Согласно заявлению злоумышленника, данные актуальны до июня 2023 года.

Ряд публикаций от разных злоумышленников

- В апреле 2025 года произошла утечка данных сайта посольства одной из стран СНГ в Российской Федерации. В результате публикации было раскрыто около **91 тыс. строк** данных пользователей: полные имена, адреса электронной почты, номера телефонов, физические адреса, даты рождения и IP-адреса. Из общего числа строк **32 тыс.** — это уникальные электронные адреса пользователей.
- В марте 2025 года произошла утечка данных сайта логистической компании из СНГ. В результате публикации было раскрыто **956 строк** данных пользователей: адреса электронной почты и хешированные пароли.
- В декабре 2025 года произошла утечка данных сайта розничных интернет-магазинов. В результате публикации было раскрыто около **835 тыс. строк** данных пользователей: полные имена, адреса электронной почты, номера телефонов и физические адреса.
- В ноябре 2025 года произошла утечка данных интернет-магазина цветов. В результате публикации было раскрыто около **2,8 тыс. строк** данных пользователей: полные имена, адреса электронной почты, номера телефонов, физические адреса, хешированные пароли и IP-адреса.
- В ноябре 2025 года произошла утечка данных сайта цифровой платформы физической культуры и спорта одной из стран СНГ. В результате публикации было раскрыто около **287 тыс. строк** данных пользователей: полные имена, адреса электронной почты, номера телефонов и физические адреса.

- В ноябре 2025 года произошла утечка данных сайта сети аптек. В результате публикации было раскрыто около **28 тыс. строк** данных пользователей: полные имена, адреса электронной почты, номера телефонов, хешированные пароли и физические адреса. Из общего числа строк **1,3 тыс.** — это уникальные электронные адреса пользователей.
- В октябре 2025 года произошла утечка данных сайта производственной компании. В результате публикации было раскрыто около **12 тыс. строк** данных пользователей: полные имена, адреса электронной почты, физические адреса, номера телефонов, хешированные пароли и даты рождения. Из общего числа строк **8 тыс.** — это уникальные электронные адреса пользователей.
- В августе 2025 года произошла утечка данных сайта объявлений. В результате публикации было раскрыто около **9,5 тыс. строк** данных пользователей: физические адреса, адреса электронной почты, номера телефонов и имена рекламодателей.
- Публикация приватной базы, содержащей порядка 16 млн строк данных жителей одной из стран СНГ. 14 июня 2025 года злоумышленник obladaet опубликовал в приватном Telegram-канале Umbrella Forum RAR-архив, содержащий **16 млн строк** данных: ФИО, пол, дата рождения, ИНН, телефонные номера, гражданство, национальность, физический адрес, дата начала проживания, дата конца проживания.

Андеграундные угрозы

В данном разделе рассматриваются угрозы, обнаруженные в андеграунде за 2025 год и представляющие потенциальную опасность для компаний из России и стран СНГ.

Продажа скомпрометированных данных российской телеком-компании

1 октября 2025 года злоумышленник ByteToBreach опубликовал на известном хакерском форуме сообщение о продаже 3 Тб данных российской телеком-компании.

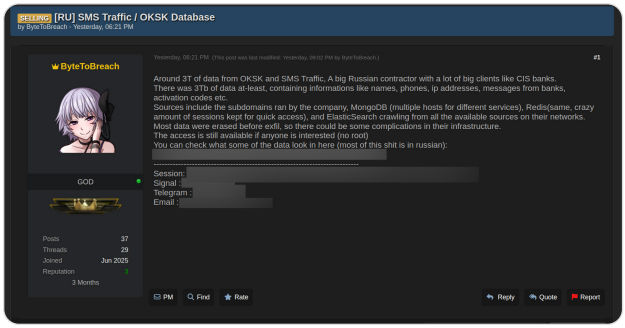


Рис. 62 — Скриншот сообщения злоумышленника на хакерском форуме о продаже данных

По словам злоумышленника, утечка данных содержит имена, номера телефонов, IP-адреса, сообщения от банков и коды активации. Источниками утечки являются несколько внутренних систем компании, включая:

- MongoDB,
- Redis,
- ElasticSearch и другие ресурсы.

Например, автор отметил, что в Redis содержится большое количество активных сессий, сохраненных для быстрого доступа. Также злоумышленник указал, что на момент публикации у него имелся к системам доступ, не имеющий root-привилегий.

ByteToBreach приложил ссылку на файлообменник Mega, где было опубликовано 12 файлов, содержащих семплы данных. Четыре JSON-файла содержат в себе данные других компаний, а именно:

- `messages_mcplat.data.json`: файл, содержащий экспорт индекса ElasticSearch "messages_mcplat". В файле 652 300 сообщений.

Рис. 63 — Скриншот структуры файла "messages_mcplat.data.json"

- `messages_smart_01.data.json`: файл, содержащий экспорт индекса ElasticSearch "messages_smart_01". В файле 359 800 сообщений.

Рис. 64 — Скриншот структуры файла "messages_smart_01.data.json"

- `messages_sms_01.data.json`: файл, содержащий экспорт индекса ElasticSearch "messages_sms_01". В файле 632 500 сообщений.

Рис. 65 — Скриншот структуры файла "messages_sms_01.data.json"

- `txm_merchant_message.data.json`: файл, содержащий экспорт индекса ElasticSearch "txm_merchant_messages". В файле 581 700 сообщений.

Рис. 66 — Скриншот структуры файла "txm_merchant_message.data.json"

Позже, 16 октября 2025 года, злоумышленник полностью удалил свое сообщение о продаже на форуме без указания причины.

Публикация 10 Тб данных российских компаний группой хактивистов Anonymous France

15 апреля 2025 года в профиле Anonymous France (@YourAnonFrench_) в известной социальной сети появилось сообщение о публикации 10 Тб данных российских компаний.

Рис. 67 — Скриншот сообщения об утечке, опубликованного группировкой Anonymous France

К сообщению была прикреплена ссылка на загрузку архива Leaked Data of corrupt officials.rar. Скриншот файлообменника представлен на рис. 68.

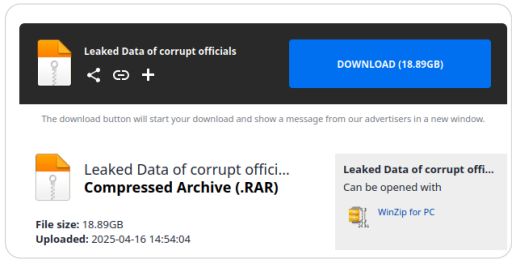


Рис. 68 — Скриншот архива утечки на файлообменном сайте

16 апреля 2025 года Anonymous (@YourAnonCentral) также распространил информацию об утечке.

Рис. 69 — Скриншот сообщения от Anonymous об атаке

В сообщении был указан список содержимого опубликованного архива.

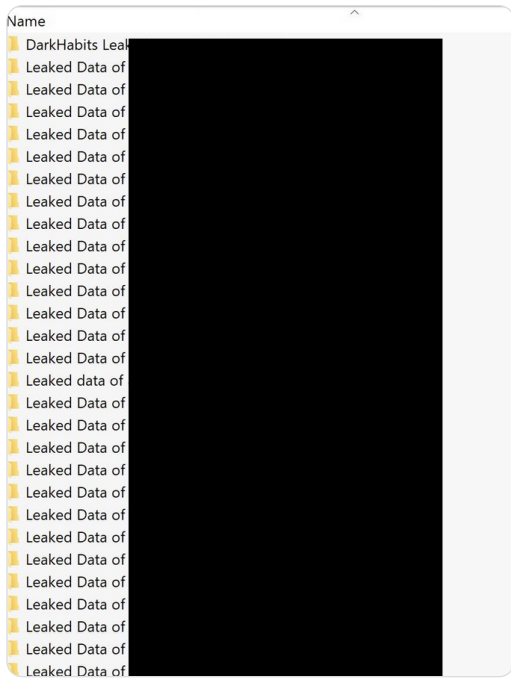


Рис. 70 — Скриншот сообщения от Anonymous об атаке

В опубликованном архиве Leaked Data of corrupt officials.rar содержалось 24,9 Гб данных. Согласно заявлению злоумышленников, всего в их распоряжении находилось порядка 10 Тб данных. Каждая из папок, представленных в архиве, названа по имени предполагаемой жертвы, однако среди файлов не содержалось никаких фактических данных, относящихся к указываемой компании. Каких-либо других публикаций от имени хактивистов, раскрывающих более полные данные о компаниях, обнаружено не было.

Silent Crow опубликовала архив с данными, предположительно относящимися к «Аэрофлоту»

9 августа 2025 группировка Silent Crow заявила о том, что начинает публиковать данные, похищенные ими в результате атаки на «Аэрофлот».

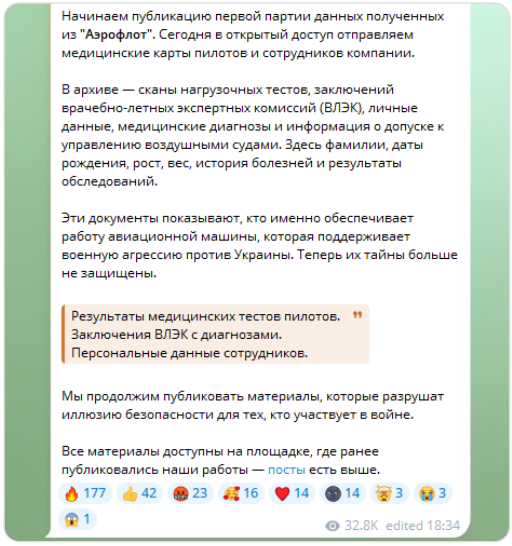


Рис. 71 — Скриншот сообщения об атаке в Telegram-канале Silent Crow

Сам архив злоумышленники опубликовали на известном андеграундном форуме, разместив ссылку на файлообменник.

Внутри находились следующие данные (3,7 Гб):

- 7380 файлов PDF;
- 1316 файлов в формате RTF;
- 447 файлов изображений;
- 21 файл DOCX;
- 2 файла Excel;
- 1 файл RAR (содержит 7 файлов PDF).

Напомним, что Silent Crow заявляла о совместной с Belarusian Cyber-Partisans (aka «Белорусские кибер-партизаны») атаке на «Аэрофлот» ранее — 28 июня 2025 года.

Группировка Cyber.Anarchy. Squad заявила об атаке на платформу «Инвестпроекты России»

17 августа 2025 года Cyber.Anarchy. Squad (CAS) в своем Telegram-канале сообщила об атаке на платформу «Инвестпроекты России».

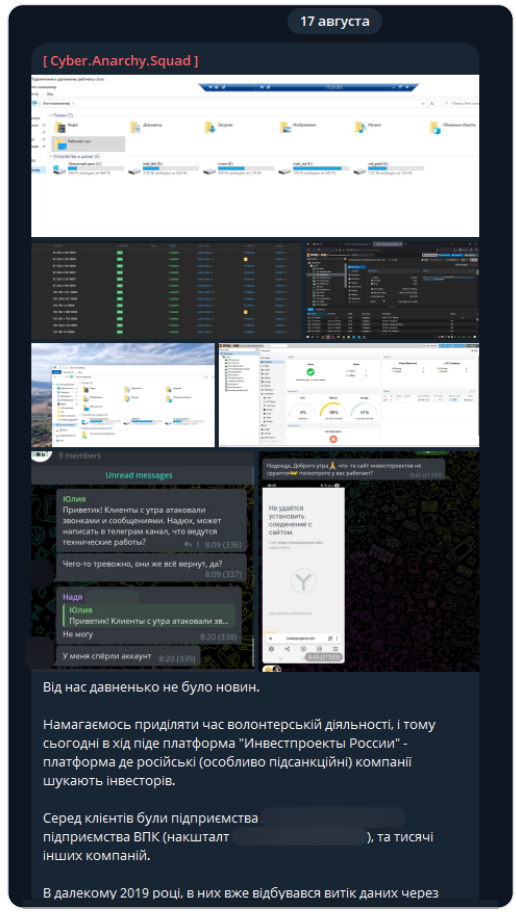


Рис. 72 — Скриншот сообщения об атаке от злоумышленников Cyber.Anarchy.Squad в их Telegram-канале

Злоумышленники заявили, что им якобы удалось получить доступ к Proxmox Virtual Environment и личным переписка сотрудников.

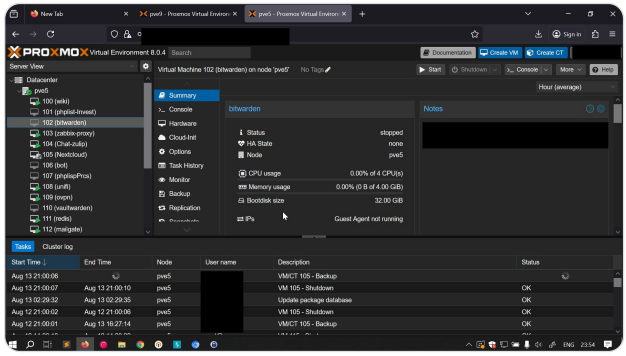


Рис. 73 — Скриншот доступа злоумышленника к Proxmox Virtual Environment

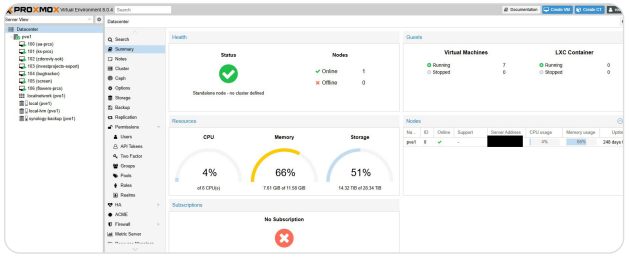
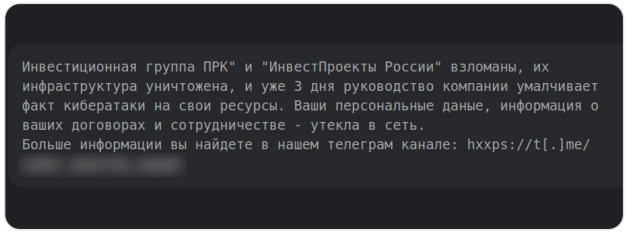


Рис. 74 — Скриншот доступа злоумышленника к Proxmox Virtual Environment

Имеется информация, что некоторые сотрудники российских компаний получили электронные письма о кибератаке.



```
Инвестиционная группа ПРК" и "ИнвестПроекты России" взломаны, их
инфраструктура уничтожена, и уже 3 дня руководство компании умалчивает
факт кибератаки на свои ресурсы. Ваши персональные даные, информация о
ваших договорах и сотрудничестве - утекла в сеть.
Больше информации вы найдете в нашем телеграм канале: hxxps://t[.]me/
```

Рис. 75 — Скриншот текста электронного письма, отправленного сотрудникам компании

Группировка Cyber.Anarchy. Squad заявила об атаке на транспортный холдинг

17 августа 2025 года Cyber.Anarchy. Squad (CAS) сообщила об атаке на транспортный холдинг в своем Telegram-канале.

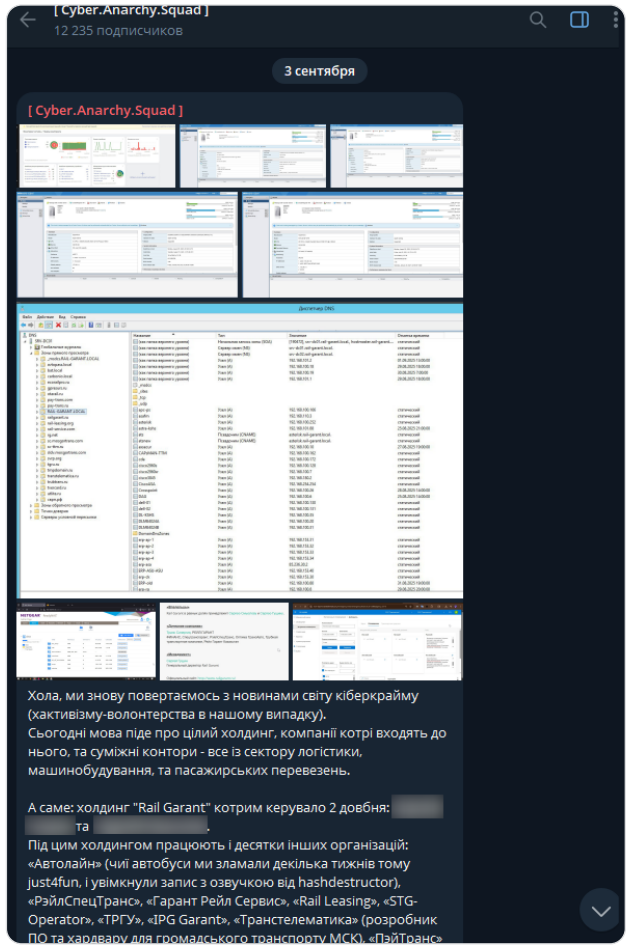


Рис. 76 — Скриншот сообщения об атаке в Telegram-канале злоумышленников

Злоумышленники заявили, что получили доступ к таким системам, как VmWare ESXi, Netgear Ready NAS, Teampass и т. д. Киберпреступники опубликовали 33 Гб архивных файлов, содержащих **125 тыс. строк** данных пользователей: имена, электронные почтовые адреса, телефонные номера, хешированные пароли, IP-адреса.

«Хакерський кіт» заявила об атаке на российские компании

17 октября 2025 года группировка «Хакерський кіт» заявила об атаке на неназванную российскую компанию.

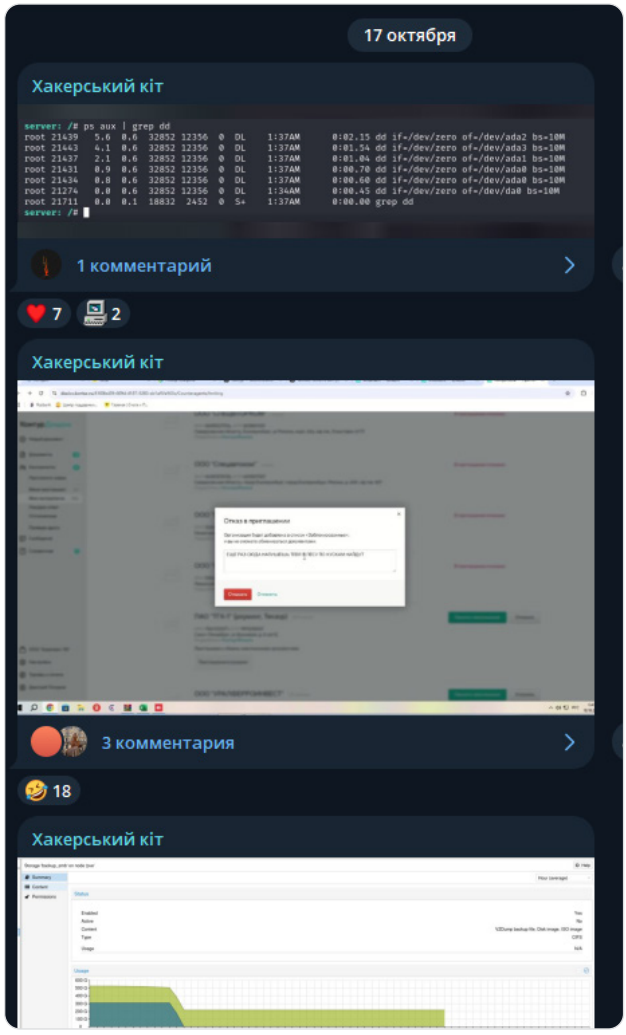


Рис. 77 — Скриншот сообщения группировки «Хакерський кіт» об атаке в ее Telegram-канале

Злоумышленники получили доступ к системе электронного документооборота, после чего зашифровали ее инфраструктуру.

Позднее, 20 октября 2025 года, группировка опубликовала сообщения об атаке на еще одну компанию.

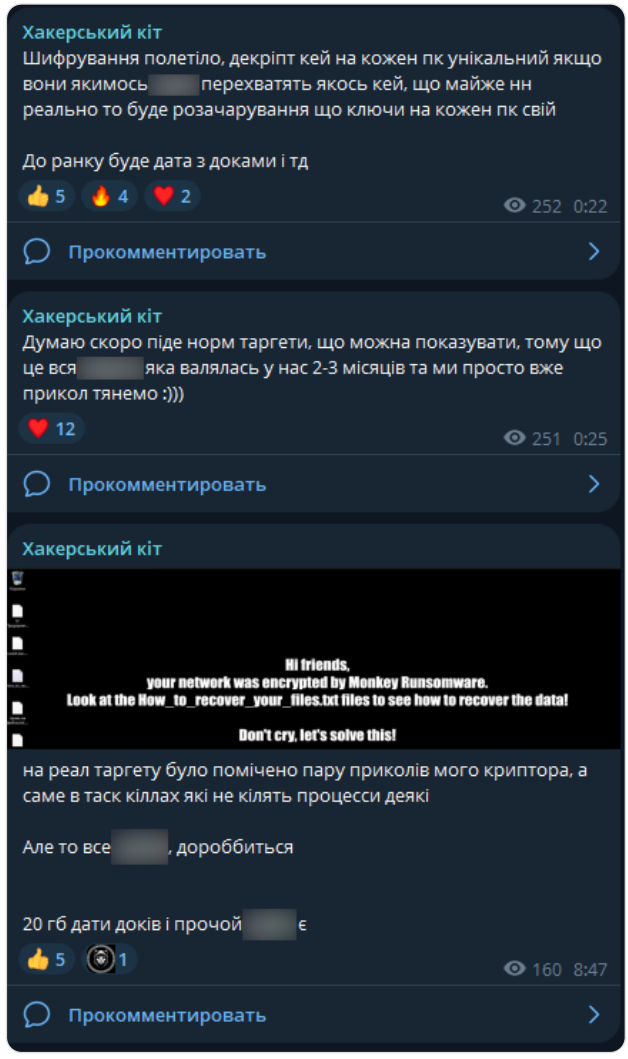


Рис. 78 — Скриншот сообщения группировки «Хакерський кіт» об атаке

Также злоумышленники опубликовали файлы одной из компаний в качестве доказательства рис. 79.

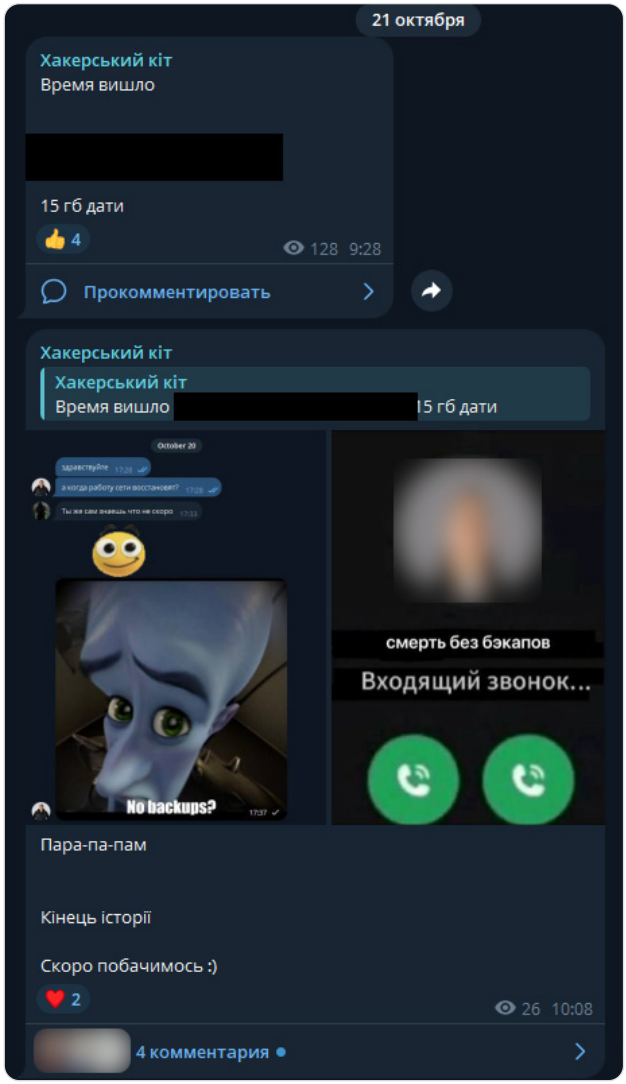


Рис. 79 — Скриншот сообщений о контакте с жертвой и предоставлении ссылки на файл

Название архива — `riocompany.rar`. Одной из жертв стала дочерняя компания концерна, занимающаяся предоставлением ИТ-услуг. Доступ, по заявлениям злоумышленников, был получен через учетные записи системных администраторов, что позволило им несколько дней находиться внутри инфраструктуры компании. Среди похищенных данных — персональные сведения сотрудников, учетные записи и фрагменты резервных копий. Общий объем похищенных файлов составил около 15 Гб.

Блокировка андеграундных форумов

В 2025 году правоохранительными органами было проведено несколько успешных операций по закрытию андеграундных форумов. В ходе длительного расследования представители полиции и спецслужб собирали и анализировали переписку между участниками площадок, отслеживали их финансовые транзакции, а затем проводили совместные рейды с последующими арестами участников форумов, изъятием серверов и резервных копий. После этого на главных страницах форумов появлялись сообщения об изъятии ресурса. В результате скоординированных действий полиции и спецслужб несколько популярных андеграундных площадок были частично или полностью ликвидированы. Пример публикации объявления о закрытии на странице одного из известных теневых форумов представлен на рис. 80.

Рис. 80 — Скриншот объявления об изъятии форума

Администраторы форумов на действия правоохранительных органов реагировали по-разному. Часть из них перезапускали форумы на новых доменах и серверах, сохраняя аккаунты и репутацию пользователей. Например, в ходе аналогичной операции по закрытию другой популярной теневой площадки стало известно о том, что форум какое-то время находился под контролем представителей правоохранительных органов. После перезапуска форума многие участники, обладающие репутацией, выразили недоверие администрации и объявили о своем уходе с него. Некоторые из них предприняли попытку создания двух новых площадок: одна из них является восстановленной копией форума предыдущих лет, в то время как другая представляет собой новый ресурс, куда перешла часть участников оригинального ресурса.

Другие же модераторы открыто заявляли о полном закрытии площадки якобы из-за уязвимости форума или вовсе отказывались от попыток повторного восстановления проекта на новых доменах.

Помимо тех пользователей, которые покидали восстановленные площадки с целью создания новых с аналогичной функциональностью, также встречались и мошенники, создававшие поддельные копии форумов. Стоит отметить, что мошеннические ресурсы не возымели особой популярности и были закрыты вскоре после публикации.

В результате у пользователей андеграундных площадок формировалось недоверие к администрации и ресурсам в целом. Обнуление балансов, блокировка прежних администраторов или их исчезновение воспринимались как признак потери контроля и привели к разделению сообщества. Кто-то ушел на альтернативные форумы и в приватные каналы, кто-то пытался восстановить старые проекты. Итогом стал спад активности на крупных андеграундных форумах, что, в свою очередь, привело к усилению миграции членов теневых сообществ в более закрытые, нишевые и распределенные каналы и расширило пространство для мошенников.

Продажа вредоносного ПО

В последние годы становится довольно популярной практика коммерциализации вредоносного программного обеспечения, при которой разработчики предпочитают монетизировать свои инструменты через продажу другим злоумышленникам вместо самостоятельного проведения атак. Данная модель бизнеса приобрела особую популярность среди создателей ВПО, что привело к формированию рынка с четкой специализацией и большим количеством предложений.

В андеграунде отмечается значительный рост предложений комплексных решений, включающих не просто отдельные образцы вредоносного кода, а полнофункциональные наборы с различными модификациями, загрузчиками, модулями обхода защиты и инфраструктурой управления. Такие наборы часто адаптированы под разные операционные системы и сценарии атак, что делает их востребованными среди злоумышленников с различным уровнем технической подготовки.

Особую динамику приобрела модель распространения ВПО как услуги (Malware-as-a-Service), когда покупатели получают не только сам инструмент, но и техническую поддержку, регулярные обновления и возможность аренды инфраструктуры для управления зараженными устройствами. Данная тенденция значительно снижает порог входа в киберпреступную деятельность и позволяет злоумышленникам, не имеющим должных технических навыков, осуществлять сложные атаки.

Рост рынка ВПО напрямую связан с увеличением масштабов киберпреступности и появлением специализированных группировок, которые фокусируются на конкретных типах атак. При этом многие разработчики рассматривают создание вредоносного ПО как основной источник дохода, а не как инструмент для собственных атак, что способствует дальнейшей профессионализации и коммерциализации данного сегмента.

Важным изменением в динамике рынка стало ослабление ранее существовавших географических ограничений. До этого на большинстве андеграундных площадок действовали правила, запрещающие атаки на пользователей из России и стран СНГ. Однако на практике атаки с использованием купленного ВПО также затрагивают эти страны, несмотря на запреты.

Специалистами нашего подразделения Threat Intelligence в 2025 году зафиксировано значительное увеличение количества объявлений о продаже ВПО на теневых форумах. Злоумышленники активно ищут покупателей для своих разработок, размещая рекламные сообщения с подробным описанием функциональности и демонстрацией возможностей. Ниже приводятся основные случаи продаж нового ВПО на форумах, несущие в себе потенциальную угрозу для пользователей и компаний из СНГ.

Продажа троянов удаленного доступа (RAT)

Данный тип ВПО представляет собой одну из наиболее многофункциональных категорий вредоносного программного обеспечения, предоставляющих злоумышленникам практически полный контроль над скомпрометированными системами.

Современные RAT-решения стали настоящими мультитулами киберпреступника, объединяющими в себе функции кейлоггера, модулей для кражи учетных данных, пере-

хвата мультимедийного контента, скрытого удаленного управления и даже встроенных механизмов вымогательства. Также примечательна тенденция коммерциализации таких решений через модель подписки (Malware-as-a-Service, MaaS), что ранее в основном было присуще ВПО типа стилер.

Распространение ВПО Snowdog по модели MaaS

Так, например, 4 февраля 2025 года на одном известном андеграундном форуме злоумышленником с псевдонимом SeverusSnape было опубликовано объявление о продаже приватного ВПО Snowdog в формате MaaS стоимостью $7000 за месяц. Автор предлагал готовое решение для совершения целевых атак на компании, включающее в себя доступ к веб-панели для создания вредоносных сборок и готовые методы доставки самописного ВПО.

30 марта 2025 года тот же злоумышленник создал дополнительную тему на этом же форуме с предложением бесплатного 7-дневного тестового периода для своего ВПО.

В ходе анализа ВПО Snowdog, включающего в себя модуль RAT с лоадером, веб-панель для генерации сборок (HTML → DOCM, ISO) и интеграцию шифровальщика Venon, наши аналитики выяснили, что панель позволяет создавать уникальные зашифрованные сборки в реальном времени, управлять зараженными системами через PowerShell и загружать файлы. ВПО написано на языке программирования C, запускается из памяти доверенных процессов, использует Tor для связи с C2-сервером и автоматически блокирует активацию в странах СНГ для минимизации рисков преследования. Позже злоумышленником были оптимизированы модули доставки и сокрытия действий в системе, что сделало данное ВПО еще более опасной угрозой.

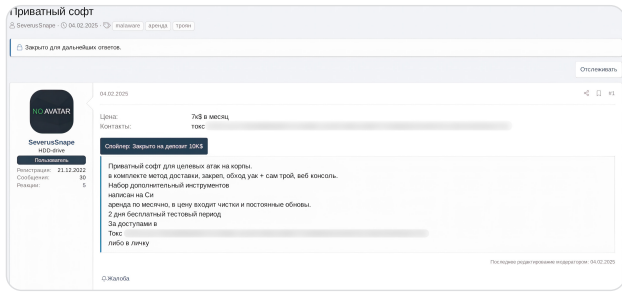


Рис. 81 — Объявление о продаже приватного ВПО Snowdog

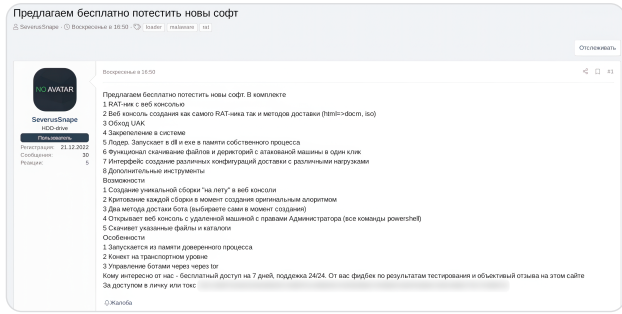


Рис. 82 — Объявление о предоставлении тестового периода ВПО Snowdog

Продажа ВПО QatarRat

Еще одним примером MaaS-решения может послужить ВПО QatarRat. Предложение было опубликовано 8 апреля 2025 года пользователем QRhades в Telegram-канале злоумышленника, а также на нескольких андеграундных форумах. Пример одного из таких объявлений представлен на скриншоте рис. 83.

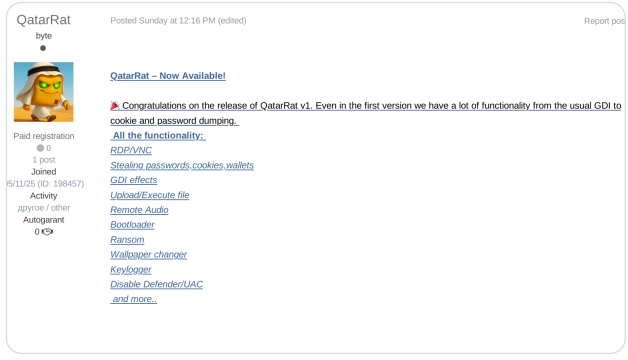


Рис. 83 — Объявление о продаже ВПО QatarRat на теневом форуме

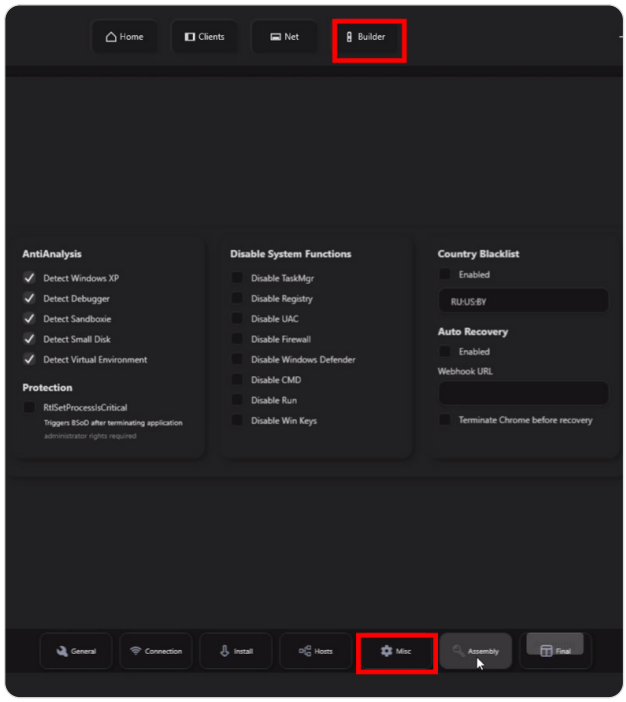


Рис. 84 — Демонстрация веб-панели ВПО QatarRat

Данное RAT-решение имеет такие функциональные особенности, как кейлоггер, модули для кражи паролей, cookie-файлов и данных криптокошельков, а также получение удаленного доступа через RDP/VNC, внедрение дополнительных вредоносных модулей, автозагрузка при старте системы и реализация вымогательских сценариев через шифрование файлов. Программа включает инструменты для отключения Microsoft Defender и UAC, а также предоставляет расширенные возможности наблюдения: скрытый VNC-доступ, перехват аудио/видео с устройств, управление системой через PowerShell-скрипты и C#-модули, манипуляции с настройками сети и хост-файлом.

ВПО распространялось по подписке:

- 1 месяц — $75;
- 3 месяца — $125;
- 6 месяцев — $300;
- 1 год — $600.

Также в теме о продаже данного ВПО неоднократно публиковались сообщения с позитивными отзывами о нем, что может повлечь за собой его широкое распространение.

Продажа ВПО Android Botnet Maradona

25 февраля 2025 года злоумышленником с псевдонимом bellygen было опубликовано объявление о продаже Android Botnet Maradona на теневом форуме.

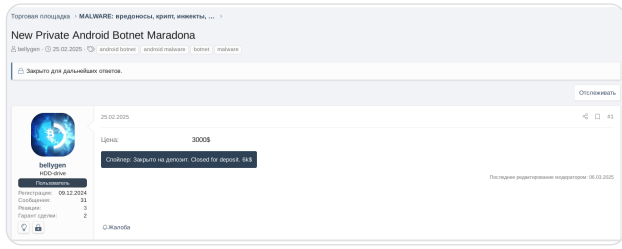


Рис. 85 — Объявление о продаже Android Botnet Maradona

Это многофункциональное вредоносное ПО для ОС Android, включающее HVNC/VNC для скрытого управления экраном (включая разблокировку PIN / графических ключей), офлайн-кейлоггер, перехват пуш-уведомлений и буфера обмена, инъекции веб-форм, имитацию экранов аккаунтов Google для кражи платежных данных, а также модули для управления SMS, приложениями и системными настройками. В описании подчеркивалась поддержка устройств Samsung, Google, Xiaomi и других брендов на ОС Android версий 9–15, а в разработке находился NFC-контроллер. 6 марта 2025 года тема была закрыта модераторами площадки до внесения депозита.

На рис. 86 представлен интерфейс ВПО из видео, предоставленного злоумышленником.

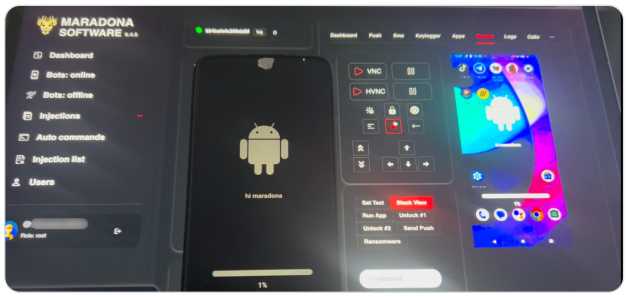


Рис. 86 — Скриншот видео, демонстрирующего работу ВПО Android Botnet Maradona

На демонстрационном видео показана работа веб-панели управления, включая удаленное выполнение команд и VNC-трансляцию. Аналогичное объявление от 25 февраля было размещено с аккаунта Eto_Ya_Ministr, однако 18 марта тема была также закрыта из-за отсутствия депозита.

Продажа ВПО типа NFC-ретранслятор

Современные банковские трояны представляют собой высокоспециализированные мошеннические инструменты, предназначенные для прямого хищения денежных средств с банковских счетов и платежных карт жертв. В отличие от традиционных вредоносных программ общего назначения такие решения фокусируются на компрометации финансовых операций через банкоматы и мобильные банковские приложения, используя комбинацию скрытого контроля устройства, кражи аутентификационных данных и технологий перехвата транзакций в реальном времени.

Особую опасность представляет тенденция к специализации и модульности таких инструментов, когда злоумышленники разрабатывают узконаправленные решения для конкретных векторов атак, таких как снятие средств через NFC. Коммерциализация подобных инструментов через модели подписки (MaaS) с высокой стоимостью доступа ($3000–5000 в месяц) указывает на формирование устойчивого рынка профессионального вредоносного ПО, ориентированного на получение финансовой выгоды при минимальных рисках для организаторов.

Так, например, 11 марта 2025 года злоумышленник с псевдонимом nikolakitip анонсировал на форумах продажу самописного NFC-ретранслятора в формате APK, предназначенного для перехвата средств через банкоматы.

Рис. 87 — Объявление о продаже самописного NFC-ретранслятора в формате APK

Управление ведется с Android-устройства злоумышленника, к которому привязана карта подставного лица: при снятии денег жертвой средства автоматически переводятся на этот счет. ВПО включает модули HVNC/VNC для скрытого контроля экрана, офлайн-кейлоггер, перехват 2FA-кодов Google, пуш-уведомлений и буфера обмена, функции банкера (оверлеи для банковских приложений), клиппер для различных криптокошельков, а также модули для сбора геолокации, файлов, контактов и управления камерой/микрофоном. Стоимость подписки — $3500 в месяц без географических ограничений.

Киберпреступник активно продвигал это ВПО через приватный Telegram-канал, периодически публикуя в нем обновления. Среди них — релиз ботнета, разработка Telegram-бота для генерации сборок и исправления ошибок совместимости с устройствами под управлением ОС Android версий 14–15. Пример публикации обновлений в приватном канале злоумышленника представлен на рис. 88.

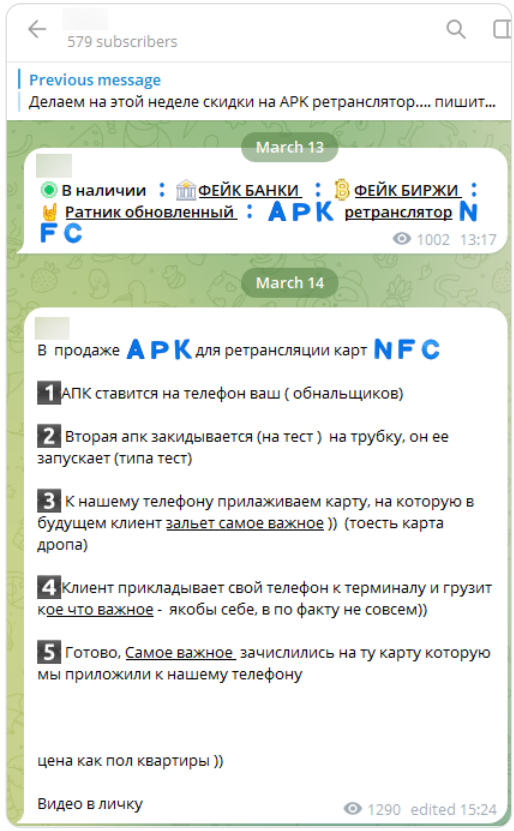


Рис. 88 — Скриншот из приватного Telegram-канала

По функциональности ВПО схоже с инструментами, продаваемыми злоумышленником bellygen, а также с тактиками группировки NFCGateCIS, специализирующейся на хищениях денежных средств через NFC-снятие. Активность nikolakitip в темах на форумах по обналичиванию незаконных средств с использованием NFC косвенно подтверждает связь с подобными схемами.

Рис. 89 — Скриншот сообщений автора в темах по обналичиванию средств через NFC

Данные о тестировании и доработке вредоносного ПО указывают на потенциальную подготовку к массовому использованию в атаках на пользователей и обналичиванию незаконно полученных денежных средств, а отсутствие ограничений по регионам несет в себе прямую угрозу для пользователей по всему миру, включая Россию и другие страны СНГ.

Продажа ВПО типа стилер

Стилеры представляют собой одну из наиболее популярных категорий вредоносного ПО, специализирующегося на массовой краже конфиденциальных данных пользователей. Благодаря доступности и кастомизации функциональности стилеры широко используются киберпреступниками для проведения атак по всему миру.

Современные стилеры перестали быть инструментом исключительно для опытных злоумышленников: благодаря модели распространения ВПО по подписке (MaaS) и настраиваемым веб-панелям они стали доступны широкому кругу киберпреступников с различным уровнем технической подготовки. Снижение минимального уровня навыков при использовании ВПО представителями киберпреступности, в свою очередь, привело к значительному увеличению числа атак, направленных на хищение персональных данных, финансовой информации и учетных записей пользователей.

Распространение ВПО mac.c Stealer

14 марта 2025 года злоумышленником с псевдонимом mentalpositive было опубликовано объявление на теневом форуме о продаже стилера mac.c Stealer. В своем объявлении

автор представил инструмент для кражи данных с macOS-устройств начиная с версии Sierra (>10.12.6), поддерживающий обе архитектуры процессоров и обладающий функциональностью по сбору паролей, cookie-файлов, сессий Telegram, криптокошельков и расшифровке системной связки ключей устройства.

Рис. 90 — Объявление о продаже стилера mac.c Stealer на теневом форуме

Анализ показал, что mac.c Stealer, написанный на языке C, с размером билда всего ~86 Кб представляет собой легковесное решение для компрометации macOS-устройств. Особенностью инструмента является возможность изменения текста в модальных окнах при запросе системного пароля, что повышает эффективность социальной инженерии. Все украденные данные расшифровываются на сервере злоумышленника, что снижает нагрузку на зараженное устройство и уменьшает шансы детектирования. Для управления используется PHP-панель в сети Tor, а при запуске ВПО автоматически скрывается окно терминала для маскировки активности.

20 июня 2025 года тот же разработчик сообщил о значительных обновлениях своего инструмента, расширяющих его возможности.

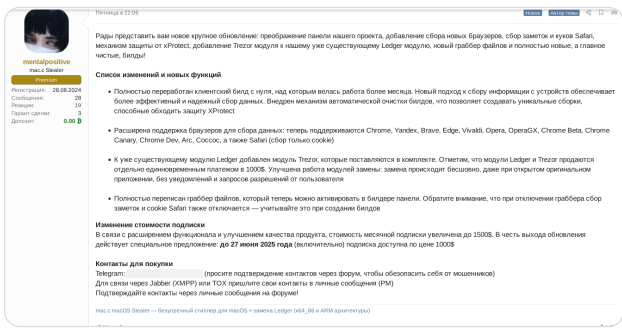


Рис. 91 — Объявление об обновлении стилера mac.c Stealer

Злоумышленник существенно расширял функциональность mac.c Stealer: к июню программа поддерживала 12 браузеров (включая Safari для сбора cookie), а также получила платные модули ($1000 за каждый) для работы с аппаратными криптокошельками Ledger и Trezor. Функция сбора файлов была полностью переписана с возможностью отключения по желанию покупателя. Важно отметить, что данное вредоносное ПО имеет встроенные ограничения при проведении атак на пользователей России и Беларуси, однако не исключено, что впоследствии оригинальный код ВПО может быть изменен, помимо прочего, для проведения атак и на указанные регионы.

Продажа ВПО Gremlin Stealer

15 марта 2025 года злоумышленником с никнеймом CoderSharp было опубликовано первое объявление о продаже стилера Gremlin Stealer в одноименном Telegram-канале, где демонстрировались возможности инструмента при краже данных из браузеров, криптокошельков, FTP-/VPN-сервисов и мессенджеров с отправкой украденной информации на C2-сервер.

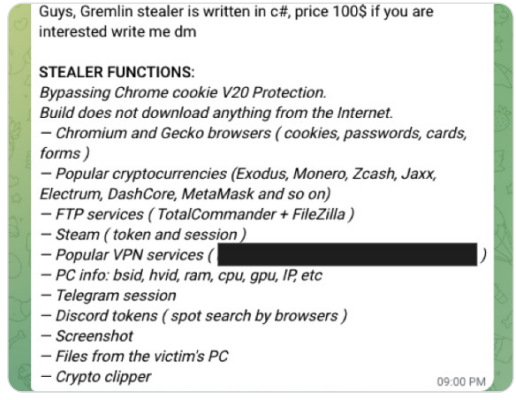


Рис. 92 — Объявление о продаже стилера Gremlin Stealer

Анализ объявления показал, что Gremlin Stealer, написанный на языке C#, представляет собой разновидность Sharp Stealer и имеет кодовую базу, сопоставимую с Hannibal Stealer. Особое внимание разработчик уделил обходу защиты Chrome cookie V20 и автономному процессу сборки, не требующему загрузки компонентов из интернета во время компиляции. Вредоносное ПО собирает широкий спектр данных: пароли и файлы cookie из всех популярных браузеров (Chromium и Gecko), информацию о кредитных картах, данные криптокошельков (включая Litecoin), учетные данные FTP и VPN, сессии Telegram и Discord, а также делает скриншоты и собирает детальную системную информацию (BSID, HVID, RAM, CPU, GPU, IP-адрес).

Рис. 93 — Скриншот работы Greamlin Stealer

Группировка, стоящая за Gremlin Stealer, предоставляет покупателям настраиваемый веб-интерфейс для управления украденными данными. Получив доступ, злоумышленники могут просматривать, загружать и удалять ZIP-архивы с данными жертв. Временные метки на сервере подтверждают активность стилера с марта 2025 года. После компрометации устройства ВПО создает ZIP-архив со всеми украденными данными и отправляет его на сервер, а также дублирует информацию через Telegram-бота с использованием жестко закодированного API-ключа.

Продажа эксплойтов уязвимостей

Помимо продаж готового ВПО, рынок эксплойтов уязвимостей нулевого дня (0-day) также представляет собой один из наиболее специализированных и высокодоходных сегментов андеграунда, где стоимость отдельных инструментов может достигать сотен тысяч долларов. В 2025 году наблюдается устойчивая тенденция к коммерциализации уязвимостей, когда их обнаружение и эксплуатация превращаются в отдельный бизнес с четкой сегментацией по типам платформ, уровням критичности и целевым сценариям применения.

Современный рынок эксплойтов характеризуется высокой дифференциацией: от относительно доступных уязвимостей для отдельных приложений (WinRAR, драйверов) до эксклюзивных решений для критически важных компонентов операционных систем (Windows, Android) стоимостью до полумиллиона долларов. Особое внимание привлекают эксплойты, предоставляющие удаленное выполнение кода (RCE) и локальное повышение привилегий (LPE), которые становятся ключевыми инструментами для проведения целевых атак на корпоративную инфраструктуру и кражи конфиденциальных данных.

Продажа уязвимости 0-day для веб-редакторов TinyMCE и CKEditor

Так, например, 7 февраля 2025 года злоумышленником с псевдонимом Valerie было опубликовано объявление о продаже эксплойта RCE-уязвимости нулевого дня.

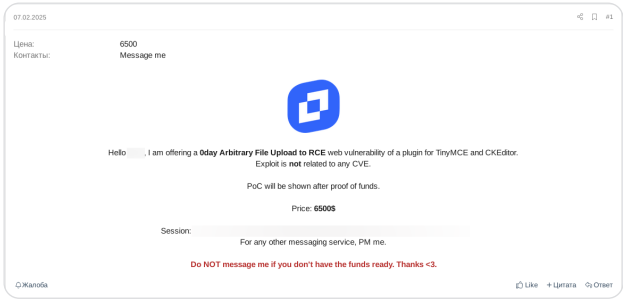


Рис. 94 — Объявление о продаже уязвимости нулевого дня злоумышленником Valerie

Данная уязвимость реализована в виде плагина для веб-редакторов TinyMCE и CKEditor. В описании подчеркивалось, что она не связана ни с одной из известных в CVE, а дополнительные технические детали предоставлялись исключительно после подтверждения платежеспособности покупателя.

Продажа уязвимости 0-day в драйвере для Windows

4 марта 2025 года злоумышленником с псевдонимом Nightf4ll_dll было опубликовано объявление о продаже уязвимости нулевого дня в драйвере Windows, обеспечивающей неограниченное чтение и запись физической памяти.

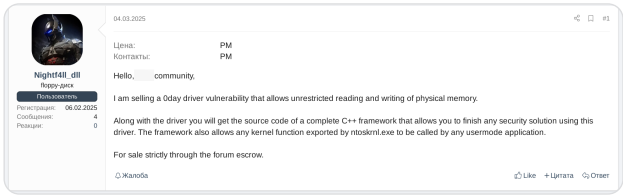


Рис. 95 — Объявление о продаже уязвимости нулевого дня в драйвере Windows

В комплект входит исходный код C++ фреймворка, позволяющего пользовательским приложениям вызывать любые экспортируемые функции ядра из `ntoskrnl.exe` и обходить механизмы безопасности. Уточнение цены и деталей происходит исключительно через личные сообщения, сделка осуществляется строго через эскроу-сервис форума.

Продажа уязвимости 0-day в Chrome для Android

Также 9 апреля 2025 года злоумышленником с псевдонимом XLab было опубликовано объявление о продаже эксплойта RCE-уязвимости нулевого дня для Chrome на Android-устройствах (версии ≤15).

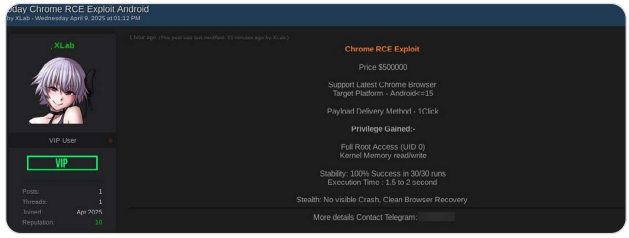


Рис. 96 — Объявление о продаже эксплойта RCE-уязвимости нулевого дня для Chrome

Стоимость эксплойта составляла $500 000, при этом автор заявлял о 100%-й стабильности (30 успешных запусков из 30), получении полного root-доступа (UID 0) с возможностью чтения/записи памяти ядра, времени выполнения 1,5–2 секунды и об отсутствии видимых крашей с автоматическим восстановлением браузера. Доставка вредоносной нагрузки осуществляется one-click-методом, управление продажей — через Telegram с опцией использования гарант-сервиса.

Продажа уязвимости 0-day LPE для Windows

25 апреля 2025 года злоумышленником с псевдонимом IncredAustin было опубликовано объявление на андеграундном форуме о продаже уязвимости нулевого дня для Windows, обеспечивающей локальное повышение привилегий (LPE).

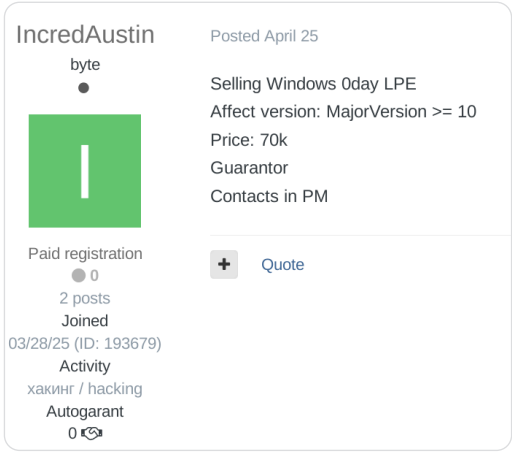


Рис. 97 — Объявление о продаже уязвимости нулевого дня для Windows, обеспечивающей локальное повышение привилегий (LPE)

Согласно объявлению, эксплойт функционирует на всех версиях ОС Windows начиная с 10-й (MajorVersion >= 10), а стоимость продажи составила $70 000 при обязательном использовании гаранта для проведения сделки.

Продажа уязвимости 0-day в WinRAR

7 июля 2025 года злоумышленником с псевдонимом zeroplayer было опубликовано объявление на форуме о продаже эксплойта RCE-уязвимости нулевого дня для WinRAR (версии ≤7.13) за $80 000.

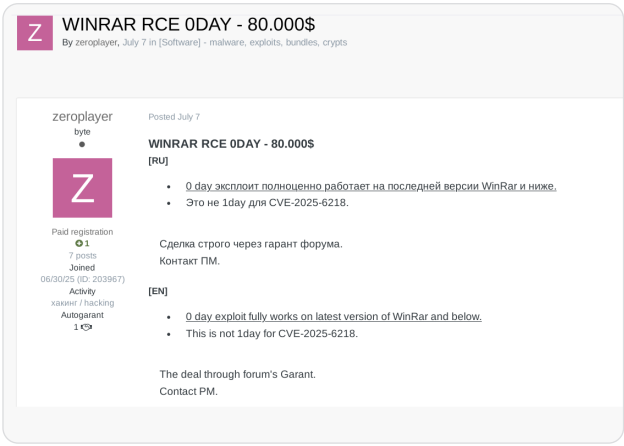


Рис. 98 — Объявление о продаже эксплойта RCE-уязвимости нулевого дня для WinRAR

Автор подчеркивал, что решение не связано с CVE-2025-6218 (опубликована 21 июня 2025 года). 13 июля 2025 года аналогичное сообщение с дополнением «В наличии другие 0/1day-эксплойты» появилось еще на одном из андеграундных форумов.

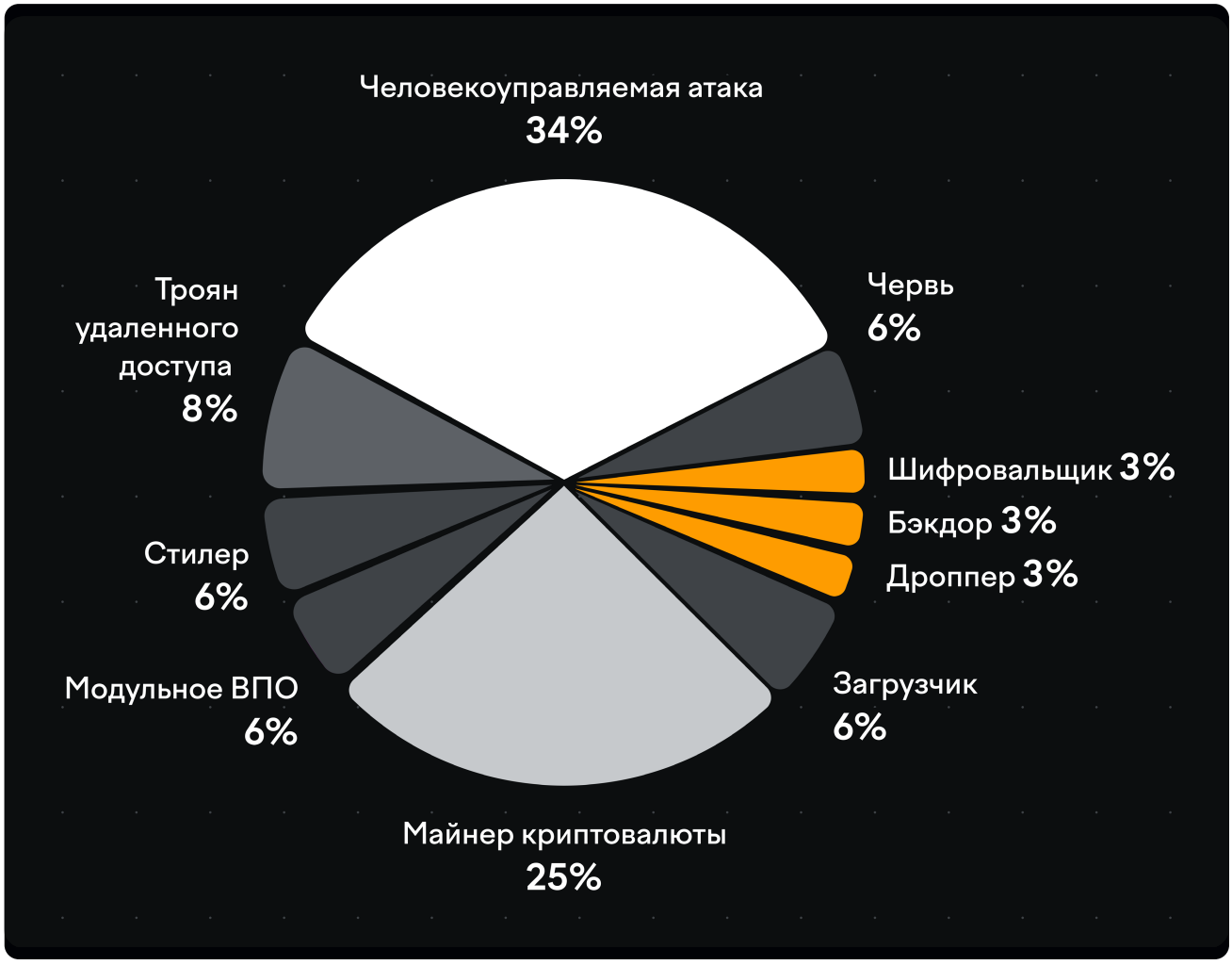
5 августа 2025 года zeroplayer закрыл продажу, отметив неактуальность предложения. Ранее, в августе 2025 года, специалистами F6 были зафиксированы атаки группировки GOFFEE с использованием CVE-2025-6218, что косвенно указывает на возможную связь между приобретенным эксплойтом и их деятельностью. Анализ показал, что в объявлении, вероятно, упоминалась уязвимость CVE-2025-8088 (зарегистрирована 8 августа 2025 года), связанная с некорректной проверкой путей при распаковке архивов. Это позволяет внедрять файлы в системные директории (например, автозагрузку) и получать RCE через перезапись критических компонентов.

Угрозы, векторы атак и тактики злоумышленников

Специалисты Центра кибербезопасности компании F6 проанализировали инциденты высокого уровня критичности[4], которые потребовали реакции в рамках предоставления сервиса мониторинга и реагирования SOC MDR в 2025 году.

Угрозы

Статистика по киберугрозам в 2025 году



4. Инциденты, нейтрализованные автоматически, в статистике не учитывались.

Среди инцидентов 2025 года, на которые реагировали специалисты Центра кибербезопасности (ЦК) компании F6, чаще всего встречались угрозы, связанные с управляемыми человеком атаками[5], — **34%** от общего количества. На втором месте — заражения майнерами криптовалют, — **25%**. На третьем месте идут инциденты, связанные с заражением троянами удаленного доступа (RAT), — **8%**.

Одной из главных тенденций стал рост во второй половине 2025 года доли человекоуправляемых атак — до **59%** — при одновременном снижении доли инцидентов с майнерами (до **17%**). При этом злоумышленники продолжали использовать RAT — это по-прежнему эффективный инструмент для получения первоначального доступа и хищения информации. Текущие тенденции показывают, что востребованность RAT у атакующих сохраняется и продолжит расти.

Векторы атак

Способы компрометации устройств в 2025 году

5. Под человекоуправляемой атакой понимается атака, при которой злоумышленник получает первоначальный доступ к системе (например, через фишинг или эксплуатацию уязвимостей) и активно действует в инфраструктуре: проводит разведку с использованием специализированных инструментов, выполняет команды, перемещается между системами и адаптирует методы обхода защитных мер.

В ходе реагирования на инциденты аналитики ЦК F6 установили, что самым распространенным способом компрометации устройств российских организаций оказалась загрузка пользователями программ с вредоносной нагрузкой — **46%** от общего количества инцидентов в прошлом году. На втором месте — использование уязвимостей на публично доступных активах (**19%** от общего количества инцидентов), на третьем — подключение зараженных съемных носителей информации (**16%**).

Как отмечают аналитики ЦК F6, на протяжении года наблюдалось выраженное перераспределение по способам компрометации устройств. Если в начале года доминировала беспорядочная загрузка пользователями вредоносного ПО (**52%** случаев в первом полугодии и **36%** во втором), то к концу года заметно возросло количество атак через эксплуатацию уязвимостей.

Такая тенденция требует смены фокуса защиты с **реактивного** подхода (реагирование после получения сигнала об инциденте) на **проактивный** (поиск угроз до получения сигналов об инциденте на основе гипотез и аномалий). В условиях увеличения случаев компрометации устройств за счет использования уязвимостей проактивная защита подразумевает особое внимание к инфраструктуре, включая непрерывный поиск угроз и, что критически важно, оперативное устранение известных уязвимостей. Такой подход позволяет предотвращать саму возможность реализации инцидента, а не просто проводить мероприятия по его устранению.

Четвертое место среди самых распространённых способов компрометации устройств занимает компрометация устройств через фишинговые письма (**11%** случаев за год). В этом сценарии злоумышленник, используя социальную инженерию, побуждает пользователя открыть вредоносное письмо, что приводит к заражению системы.

Фишинговые письма с вредоносным ПО чаще всего рассылались по вторникам: на этот день приходится **25,5%** всех рассылок. Меньше всего рассылок в 2025 году было по воскресеньям — **2%**. Это объясняется тем, что злоумышленники стараются отправлять рассылки в наиболее активные дни рабочей недели.

Также специалисты зафиксировали увеличение доли случаев проникновения злоумышленников в сеть при помощи ранее скомпрометированных легитимных учетных записей сотрудников или организаций подрядчиков — с **4%** в первом полугодии до **14%** во втором.

Рост числа атак через ранее скомпрометированные легитимные учетные записи сотрудников и подрядчиков свидетельствует о необходимости пересмотра подходов к управлению доступом сторонними лицами, особенно организациями-подрядчиками. Без внедрения системы контроля над учетными записями и механизмов мониторинга на предмет их компрометации в ближайшей перспективе можно ожидать значительного увеличения случаев компрометации устройств, реализуемых через данный вектор.

Распределение событий

В случае успешного проникновения в инфраструктуру киберпреступники переходят к следующему этапу атаки — закреплению, разведке и дальнейшему развитию атаки вплоть до деструктивного воздействия.

Тактики и техники

В 2025 году в ходе реагирования на инциденты было установлено, что злоумышленники в большинстве случаев использовали типовые, хорошо отработанные сценарии атак. После успешного первоначального доступа атакующие переходили к стадии развития атаки, соответствующей тактике исполнения TA0002 Execution, которая была зафиксирована в **30%** инцидентов. В рамках данной тактики осуществлялся запуск вредоносного кода и вспомогательных утилит на скомпрометированных узлах с целью дальнейшего развития атаки.

Злоумышленники применяли тактику обхода защитных механизмов TA0005 Defense Evasion, доля которой составила **16%**. Эта тактика использовалась для сокрытия вредоносной активности в инфраструктуре, снижения эффективности средств обнаружения и предотвращения и чаще всего реализовывалась посредством вредоносного программного обеспечения.

Кроме того, в **14%** инцидентов, связанных с человекоуправляемыми атаками, была зафиксирована реализация тактики повышения привилегий TA0004 Privilege Escalation. Ее применение позволяло атакующим получить расширенные права доступа, обойти ограничения учетных записей и политики безопасности, что в дальнейшем обеспечивало бы возможность ослабления или отключения защитных механизмов, закрепления в системе, а также упрощало выполнение последующих действий, включая горизонтальное перемещение и доступ к критически важным данным и системным компонентам.

Наиболее распространенной техникой закрепления в инфраструктуре является использование ключей автозапуска в реестре и папки автозагрузки T1547.001 Registry Run Keys / Startup Folder, доля которой составила **13%**. Изменение параметров Run в системном реестре обеспечивает автоматический запуск вредоносных исполняемых файлов при входе пользователя в систему либо при загрузке устройства. Это позволяет злоумышленникам поддерживать устойчивый и длительный доступ к скомпрометированным хостам.

Второе место по частоте применения заняла техника использования PowerShell T1059.001, зафиксированная в **10%** инцидентов. В ходе человекоуправляемых атак этот инструмент применялся для интерактивного выполнения команд, загрузки и запуска вредоносных компонентов, а также для автоматизации постэксплуатационных действий в среде Windows после компрометации системы.

Кроме того, в **5%** инцидентов были выявлены попытки реализации техники сокрытия файлов и каталогов T1564.001 Hidden Files and Directories и маскировки T1036 Masquerading. Указанные техники использовались злоумышленниками для снижения вероятности обнаружения их активности средствами защиты и сокрытия следов присутствия в инфраструктуре.

Рекомендации

Для защиты от актуальных киберугроз рекомендуем **компаниям** неукоснительно выполнять приведенные ниже рекомендации.

- Проводить регулярные тренинги и тестирования сотрудников, направленные на ознакомление и закрепление основ информационной безопасности, принципов цифровой гигиены, а также на повышение осведомленности об актуальных угрозах.
- Обеспечивать максимально возможное покрытие устройств ИТ-инфраструктуры средствами защиты.
- Проводить своевременное и регулярное обновление программного обеспечения, которое позволяет закрывать обнаруженные уязвимости, в первую очередь критические. Приоритет стоит отдать обновлениям публично доступных сервисов и операционных систем, на которых они развернуты, затем контроллеров доменов, систем резервного копирования и централизованного управления и т. д.
- Регулярно создавать резервные копии важных данных, руководствуясь лучшими мировыми практиками. За основу реализации резервного копирования можно взять стратегии «3-2-1» или «3-2-1-1-0». Последняя предпочтительнее, поскольку реализует контроль целостности резервных копий.
- Внедрять многофакторную аутентификацию на основе одноразовых кодов для входа в различные сервисы и подключения к корпоративным сетям. Эта мера позволит снизить риски получения злоумышленниками доступа с использованием скомпрометированных или подобранных аутентификационных данных.
- Использовать для защиты конечных устройств и инфраструктуры в целом решения класса EDR или XDR, например F6 Managed Extended Detection and Response (MXDR), а также антивирусное программное обеспечение. Своевременно реагировать и анализировать все сработки указанных решений.
- Внедрять решения для защиты от DDoS-атак.
- Проактивно блокировать трафик с потенциально вредоносными хостами.
- Использовать строгую парольную политику как в офисе, так и дома (при удаленной работе) для локальных и доменных учетных записей.
- Использовать различные пароли для локальных администраторов на всех хостах инфраструктуры. При компрометации отдельной машины это позволит не считать скомпрометированным весь задействованный сегмент.
- Выстраивать сетевую архитектуру ИТ-инфраструктуры с учетом возможности изоляции отдельных сегментов сети и контроля как входящего, так и исходящего трафика.
- При разграничении прав доступа руководствоваться принципом минимально необходимых привилегий в системе, уделяя особое внимание сервисным учетным записям, а также учетным записям, используемым для выполнения автоматизированных задач и удаленного доступа.
- Ограничить сетевой доступ по задачам конкретной учетной записи. К примеру, подрядчик получает доступ только к нужному ему серверу, а не ко всему сегменту или всей сети.

- Для контроля уровня информационной безопасности инфраструктуры организации, поиска уязвимостей и забытых цифровых активов использовать решение F6 Attack Surface Management (ASM).
- Настроить расширенный аудит и аудит отключенных видов событий для повышения детализации событий безопасности Windows.
- Обеспечить глубину хранения журналов событий операционной системы и средств защиты информации не менее трех месяцев. Важно: это касается не только рабочих станций и серверов, но и имеющихся средств защиты, в том числе для защиты сетевого периметра (например, межсетевого экрана).
- Настроить блокировку IP-адресов и учетных записей для защиты от брутфорс-атак.
- Регулярно проверять логины и пароли в публичных утечках и оперативно менять все пароли, которые уже находятся в утечках.
- Настроить удаленный доступ только с доверенных IP-адресов либо после успешной идентификации устройства, с которого выполняется удаленный доступ. Если такие меры невозможны, то необходимо ввести фильтрацию по Geo IP.
- Для предотвращения кибератак с использованием вредоносных рассылок внедрить решения для защиты электронной почты, например F6 Business Email Protection (BEP), способное обнаруживать, блокировать и анализировать все распространяемые угрозы: от спама и фишинга до вредоносного программного обеспечения и фишинговых атак с компрометацией деловой переписки.
- Запретить прямой доступ по RDP к рабочим станциям из-за пределов внутренней сети.
- Блокировать входящие соединения на SMB-порты от компьютеров, находящихся за пределами корпоративной сети.
- Запретить непосредственный вход на конечные устройства под учетной записью root по протоколу SSH.
- Отключить или заблокировать невостребованные удаленные сервисы.
- Уменьшать поверхность атаки. Необходимо избегать публикации сервисов удаленного управления и доступа (например, протоколы RDP, SSH, SMB, WinRM и др.) и иных сервисов без должной защиты и острой необходимости.
- Осуществлять непрерывную идентификацию теневых ИТ для управления поверхностью атаки (теневые ИТ — системы и устройства, развернутые сотрудниками без ведома или одобрения ИТ-подразделений компании).
- Выявлять признаки изначального доступа, закрепления в системе и продвижения по сети. Хотя чаще всего техники атакующих достаточно примитивны, с более сложными атаками может помочь регулярная проактивная охота за угрозами (threat hunting).
- Детектировать и регулярно проверять инфраструктуру на известные индикаторы компрометации.
- Анализировать события, зафиксированные средствами антивирусной защиты, чтобы определить обстоятельства компрометации системы.

- Запретить пользователям регистрироваться на сторонних сервисах с использованием корпоративной почты.
- Отслеживать трафик DNS: некоторые разновидности вредоносного программного обеспечения требуют связи с сервером или C2, вредоносное соединение может маскироваться под легитимный трафик, в том числе по протоколу HTTP.
- Проводить аудит нелегитимных сессий пользователей в Telegram.
- Ограничить возможность использования личных аккаунтов социальных сетей, мессенджеров в рабочих целях.
- Ограничить возможность использования личной техники сотрудников для доступа в корпоративную сеть, в том числе через VPN.
- Чтобы эффективно организационно и технически противостоять действиям атакующих и минимизировать ущерб для компании, необходимо или оперативно привлекать специалистов на аутсорсе, или заранее иметь подписку на ретейнер по реагированиям на инциденты информационной безопасности.
- Для снижения рисков атак через подрядчиков рекомендуется контролировать соблюдение подрядчиками регламентов и требований по ИБ, осуществлять Privileged Access Management (PAM) по отношению к аккаунтам подрядчиков, подключать поставщиков к инфраструктуре через собственный контролируемый VPN, блокировать неактуальные доступы подрядчиков.
- Реализовать централизованный сбор событий в инфраструктуре и их передачу в систему сбора данных (например, стек ELK, SIEM).
- В 2026 году существенно вырастет сложность, скрытность и целевой характер кибератак. Успех защиты будет зависеть не только от скорости обнаружения и устранения известных уязвимостей, но и от фундаментального перехода от реактивной к проактивной модели защиты. Критически важной станет способность не просто реагировать на инциденты, а активно выявлять скрытые угрозы через поиск аномалий в активности, анализ поведения пользователей и сущностей, а также непрерывный мониторинг и тестирование безопасности инфраструктуры на опережение.

Если **инфраструктура компании подверглась кибератаке**, следует выполнять приведенные ниже рекомендации:

- Обратиться за консультацией в компании, которые оказывают услуги по реагированию на инциденты. Специалисты профильных компаний, получив некоторые детали об атаке, при наличии возможности предоставят вам полезную информацию о злоумышленниках и характерных для них TTPs. Кроме того, у компаний можно получить инструменты и методические рекомендации для сбора криминалистически значимых данных, необходимых для реагирования на инцидент и его расследования.
- Оперативно провести реагирование на инцидент. Если недостаточно возможностей или компетенций для самостоятельного реагирования, то обратиться в профильные компании.
- При возникновении инцидентов ИБ по возможности не переустанавливать операционные системы и не удалять выявленное ВПО и инструменты атакующих на пострадавших системах, пока

не будут собраны криминалистически значимые данные. В противном случае выявление источника первоначальной компрометации, используемых средств закрепления и иных обстоятельств кибератаки будет затруднено, а в некоторых случаях невозможно.

- Перед началом восстановления необходимо локализовать инцидент и минимизировать риски повторного инцидента, что снизит ущерб и обеспечит возможность безопасного восстановления работоспособности ИТ-инфраструктуры.

Для защиты от актуальных киберугроз рекомендуем **пользователям** выполнять приведенные ниже рекомендации:

- При выборе паролей придерживаться политики установки отдельного пароля на каждый сервис, избегать простых комбинаций, содержащих даты, имена и другую личную информацию.
- Проводить периодическое обновление паролей для всех сервисов.
- Включить двухфакторную атентификацию (2FA) и облачные пароли для всех сервисов, где существует такая возможность.
- Использовать для хранения паролей менеджер паролей (например, KeePass), а для аккаунтов создавать уникальные и сложные пароли.
- Отключить автозаполнение паролей и платежных данных в браузере.
- Использовать отдельную карту для онлайн-покупок.
- Следить за своими социальными сетями. Необходимо закрыть аккаунт в социальных сетях от посторонних и удалить личную информацию.
- Отключить автозагрузку файлов в мессенджерах.
- Скачивать приложения только из официальных магазинов.
- Не скачивать подозрительные файлы и не переходить по непроверенным ссылкам, полученным из различных источников, включая почту, СМС, чаты в мессенджерах и др.
- Ограничить доступ к данным и выдаваемые права приложениям.
- Создавать резервные копии данных.
- Не подключаться к публичным Wi-Fi-сетям и не использовать непроверенные VPN.
- Включить опцию определения номеров и блокировки нежелательных звонков.
- Никому не раскрывать коды подтверждений, пароли и другую секретную информацию.
- Оперативно блокировать банковские карты, менять пароли от сервисов и т. д. при подозрении, что могла произойти их компрометация.
- Удалять неиспользуемые аккаунты и приложения.
- Удалять историю браузера и cookies.

F6

«Вы держите в руках флагманский аналитический отчет от команды F6, в котором мы подводим итоги 2025 года и делимся прогнозами на 2026 год. Над этим отчетом работали аналитики кибербразведки, эксперты Лаборатории цифровой криминалистики, специалисты Центра кибербезопасности и Департамента защиты от цифровых рисков.

Подготовленные нашими экспертами тренды, прогнозы и рекомендации станут ценным источником стратегических и тактических данных об актуальных киберугрозах для CISO и руководителей групп кибербезопасности, специалистов по реагированию на инциденты, аналитиков SOC, CERT, Threat Intelligence. Ведь все наши прогнозы имеют обыкновение сбываться».

Валерий Баулин, CEO компании F6