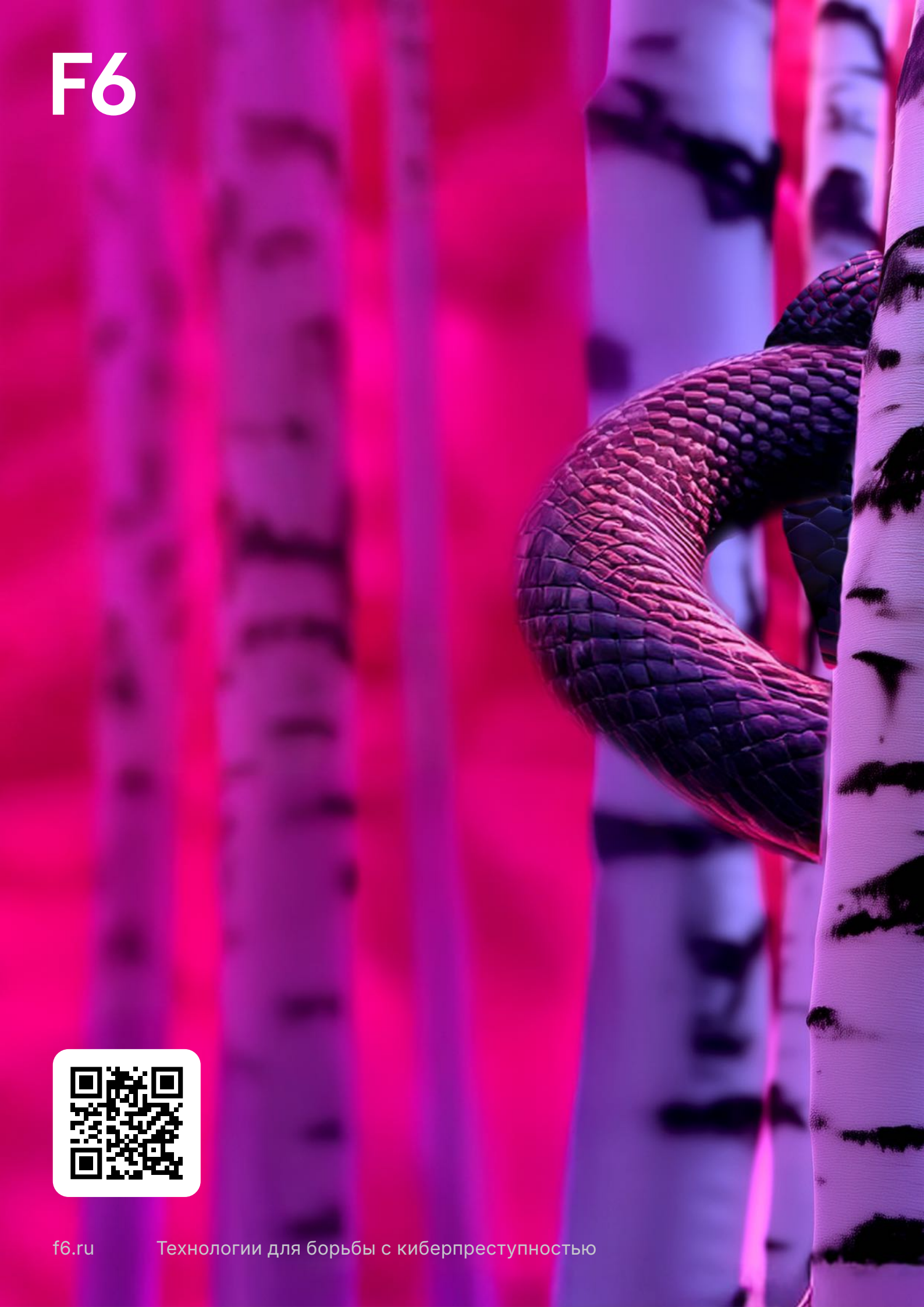

F6
Технологии для борьбы
с киберугрозами
Киберугрозы
в России
и СНГ
Аналитика и прогнозы
2024/25

Оглавление

F6



f6.ru

Технологии для борьбы с киберпреступностью

Введение

Введение

О компании F6

F6 — ведущий разработчик технологий для борьбы с киберпреступностью, предотвращения и расследования киберпреступлений в России и за рубежом. Флагманские продукты F6 основаны на знаниях, полученных в ходе многолетних реагирований на инциденты и исследований киберпреступности.

Решения компании F6 обеспечивают защиту от киберрисков, связанных с целевыми атаками, утечками данных, мошенничеством, фишингом, нелегальным использованием бренда. Продукты F6 входят в реестр отечественного ПО.

Компания F6 создана при поддержке фонда развития результативной кибербезопасности Сайберус.

Перед вами — первый ежегодный отчет, подготовленной командой F6, ведущего разработчика технологий для борьбы с киберпреступностью. Хотя F6 — новый бренд в сфере кибербезопасности, за плечами у нас — более чем 20-летний практический опыт расследований киберпреступлений и реагирования на инциденты информационной безопасности по всему миру. И наши прогнозы имеют обыкновение сбываться.

В начале января авторитетный журнал Politico включил в список «черных лебедей» — «непредсказуемых, маловероятных» событий 2025 года, которые еще не происходят, но могут начаться, — потенциально крупнейшую в истории человечества кибератаку. Не нужно быть футурологом, чтобы предсказать высокую вероятность подобного прогноза. За последние годы не только прогосударственные хакеры, но и киберкриминальные группы, а с недавнего времени еще и хактивисты стали обладателями кибероружия, способного погрузить планету в цифровой хаос.

В 2024 году почти в два раза увеличилось число прогосударственных APT-групп, атакующих цели в России. Выросло количество кибератак программ-вымогателей. DDoS-атаки становились мощнее. Количество утечек баз данных у отечественных компаний побило рекорд 2023 года. На фоне геополитической нестабильности пробудилось «древнее зло» — активизировались старые криминальные группы Buhtrap и OldGremlin, наблюдались всплески кибератак на пользователей Android. Финансовый ущерб от деятельности мошенников, в первую очередь телефонных, достиг космического размаха.

В то же время трансформировался привычный для исследователей ландшафт киберугроз. Размываются границы классификации преступных групп — хактивистов, прогосударственных хакеров, киберкриминала. Хактивисты-диверсанты атакуют госорганы и компании России, используя в атаках программы-шифровальщики. У русскоговорящих преступников полностью снимается или размывается правило «не работаем по Ру» (то есть не атакуем Россию): в андеграунде можно найти выставленные на продажу базы данных и корпоративные доступы в инфраструктуру компаний из стран СНГ.

Наступивший 2025 год может преподнести множество неприятных сюрпризов. В связи с проектом внедрения цифрового рубля в России и расширением системы ЕРИП в Беларуси повышаются риски кибератак на национальные платежные системы и банки, что угрожает безопасности платежных данных и может нарушить работу финансовых систем. Целевые атаки на IT-интеграторов, разработчиков ПО станут одним из вероятных путей для получения доступов в крупные IT-компании и госучреждения. И, разумеется, в 2025 году программы-вымогатели и утечки баз данных будут оставаться в топе главных киберугроз.

Собранные в новом аналитическом отчете данные о тактиках, инструментах и активности атакующих получены благодаря совместной работе нашей команды — специалистов Департамента киберразведки, Лаборатории цифровой криминалистики, Центра кибербезопасности, Департамента защиты от цифровых рисков Digital Risk Protection. Технические данные получены непосредственно во время реагирований на инциденты информационной безопасности, а также от наших флагманских систем — **Threat Intelligence** и **Managed XDR**.

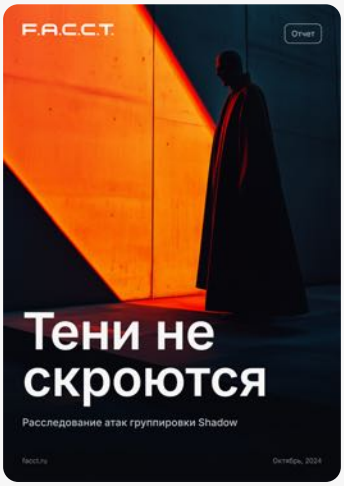
Уверен, что тренды, прогнозы и рекомендации из нашего отчета станут незаменимым источником стратегических и тактических данных об актуальных киберугрозах для CISO и руководителей групп кибербезопасности, аналитиков SOC, CERT, специалистов по реагированию на инциденты, Threat Intelligence и Threat Hunting. А значит, одним «черным лебедем» может стать меньше.

Валерий Баулин, генеральный директор F6

Ключевые выводы

- Рост **количества APT-группировок**: всего в 2024 году удалось обнаружить **27** прогосударственных групп, атакующих Россию и СНГ, что почти в два раза превышает количество групп, деятельность которых была раскрыта в 2023 году — тогда мы наблюдали **14** группировок. В 2024 году в исследуемых регионах мы не зафиксировали вредоносную активность со стороны пяти групп, указанных в прошлогоднем отчете, но при этом обнаружили активность **12** новых (**Unicorn**, **Dante**, **PhantomCore**, **ReaverBits**, **Sapphire Cat**, **Lazy Koala**, **Obstinate Mogwai**, **TaxOff** и др.).
- Рост числа **атак на крупных игроков рынка**, цель которых — последующая компрометация клиентов этих компаний.
- В 2024 году не менее **17** группировок **хактивистов** атаковали российские и белорусские организации. Годом ранее таких групп было как минимум **13**.
- Обнаружено **9 финансово-мотивированных** группировок, которые не используют программы-вымогатели.
- Наблюдается **размытие классификации хактивистов**, **прогосударственных атакующих и вымогателей**, их целью является проведение кибердиверсий — нарушение работы крупных, в том числе государственных организаций России, в своих атаках они могут использовать программы-шифровальщики.
- За 2024 год выявлено **455** новых баз данных по компаниям из России и Беларуси, они выложены в публичный доступ. Количество строк в утечках составляет **более 457 миллионов**. Помимо публикации в открытом доступе, злоумышленники используют такие данные для последующего проведения каскадных атак на крупных игроков коммерческого и государственного секторов.
- Периодические **всплески утечек данных**. Было замечено, что время от времени появляется злоумышленник, который активно «сливает» данные нескольких компаний. Его активность продолжается некоторое время, потом такой злоумышленник исчезает. Вероятно, подобная активность связана с тем, что новые никнеймы — это всего лишь маски одной и той же киберпреступной группы.
- **Количество DDoS-атак** выросло как минимум на **50%** как по количеству, так и по числу задействованных в ботнетах устройств. Наиболее активно атакующей группировкой остается **IT Army of Ukraine**.

- В 2024 году наблюдался всплеск мошеннической и вредоносной активности, нацеленной на пользователей **Android**. Мы выделили несколько преступных групп в этой категории. Новыми вредоносными программами, направленными на клиентов банков, являются **CraxsRAT** и **PhotoAndroidMalware**. Также в конце года был обнаружен злоумышленник **NfcGateCIS**, который совершал атаки с помощью ВПО для Android, использующего чип NFC для кражи денег жертвы.
- Растёт число группировок, использующих шифровальщики в атаках на российские компании, увеличивается и количество таких атак. Как и в предыдущие годы, злоумышленники не используют новые уникальные программы и обходятся шифровальщиками на основе **Lockbit 3.0 Black** (чаще всего), **Conti**, **Babuk**, а иногда шифруют данные легитимными инструментами.
- Группировки-вымогатели по-прежнему **не используют технику создания DLS-ресурсов** и размещения слитых данных на них: если злоумышленники хотят опубликовать похищенные данные, они делают это в Telegram-каналах.
- В 2024 году в России и СНГ были выявлены **атаки группировок-вымогателей** Shadow (под новым брендом **DarkStar**), **HsHarada**, **DCHelp**, **RCRU64**, **GazpromLocker**. Также год запомнился появлением **ряда новых группировок**: **Masque**, **TeslaRVNG (Secles)**, **ToxUnit**, **Sauron**, **Muliaka**, **Head Mare**.
- Активность нашумевших в 2023 году группировок-вымогателей **HardBit**, **BlackShadow** была низкой, активность **Werewolves** отсутствовала.
- **Жертвами вымогателей** чаще всего становились российские производственные, строительные, фармацевтические и ИТ-компании, предприятия добывающей промышленности, ВПК, организации из сферы услуг.
- **Персональные данные** остаются одной из главных целей вымогателей — атакующие похищают чувствительные данные и лишь затем шифруют инфраструктуру жертвы.
- Несмотря на мнение, что на даркнет-форумах существует запрет для работы против России и СНГ, мы находили объявления о продаже доступов в компании в этих регионах. В 2024 году мы обнаружили в продаже **9 корпоративных доступов** стран СНГ.
- Возвращение финансово-мотивированных преступных групп, которые не были активны долгое время — **Buhtrap** и **OldGremlin**. Причем **Buhtrap** расширили арсенал вредоносной программой для Android.
- Рост количества **атак на физических лиц с помощью социальной инженерии** (схемы FakeBoss, «Мамонт» и подобные вариации). Используя социальную инженерию при совершении атак, злоумышленники применяют разные сценарии общения и способы кражи денежных средств, тем самым увеличивают свою прибыль. Обычно такие схемы нельзя осуществить, привлекая пользователей на шаблонные мошеннические сайты с помощью рекламных кампаний.
- **Комбинация разных типов киберугроз** в мошеннических схемах: например, в определенных сценариях происходит распространение Android-троянов через фишинговые страницы.



Тени не скроются

Расследование атак группировки Shadow

- **Увеличение минимальной единоразовой суммы списания с карты** жертвы из-за возросших затрат кибепреступников на закупку банковских карт для приема платежей. Возросшие затраты связаны с массовыми блокировками банковских карт кибепреступников.
- **Рост мошенничества в мессенджерах**, в частности, в Telegram. Данный мессенджер предоставляет множество способов размещения мошеннического и фишингового контента: публичные каналы, публичные чаты, Telegram-боты.
- **В 2024 году** среднее количество создаваемых **фишинговых сайтов** на один бренд **увеличилось на 52%** по сравнению с 2023 годом, среднее количество создаваемых **мошеннических ресурсов** на один бренд **увеличилось на 17%**.
- Чаще всего для компрометации данных пользователей в России и Беларуси использовали такие стилеры, как **RedLine Stealer**, **META Stealer**, **RisePro**, **Stealc**, **Phemedrone Stealer**.

Прогнозы на 2025 год

Введение

- В условиях политического конфликта **будут продолжаться атаки как хактивистов, так и прогосударственных APT** на российские государственные и коммерческие организации. Вырастет как количество атак, так и число групп атакующих.
- В 2025 году, по прогнозам экспертов, ожидается также увеличение числа атак на цепочки поставок (Supply Chain attack) и атак типа Trusted Relationship. В ходе последних хакеры могут получить и использовать легитимные учетные записи для входа в корпоративные сети клиентов поставщиков. В роли поставщиков могут выступать IT-интеграторы, разработчики ПО и другие компании.
- **Количество утечек баз данных будет расти или останется на текущем высоком уровне**. Это связано с геополитической обстановкой: хактивистам выгодно проводить «громкие» кампании, выкладывая большие массивы данных россиян.
- Аналогичная параллель с **DDoS-атаками**: пока продолжается геополитическое противостояние, атакующие будут продолжать атаки на российские ресурсы, наращивая мощности проводимых атак. Под угрозой остаются ресурсы всех отраслей экономики.
- **Программы-вымогатели останутся в топе главных киберугроз для российских компаний**. Целью шифровальщиков будет не только получение выгоды, но и причинение жертвам максимального ущерба.
- **Увеличение количества атак на мобильные устройства и ущерба от них**: растет число новых вредоносных программ для Android, появляются новые модификации старых вредоносных программ. Растет и количество выявляемых атак. Мы предполагаем, что в 2025 году рост продолжится, соответственно, увеличится и число хищений у пользователей мобильных устройств.
- Больше мошеннических и фишинговых сайтов **будут распространять ВПО для Android**.
- В 2024 году возобновили деятельность финансово-мотивированные преступные группы, которые не были активны долгое время. Это **Buhtrap** и **OldGremlin**. Мы предполагаем, что эти группы продолжат совершать атаки и в 2025 году.
- **Рост количества атак на национальные платежные системы и банки**: в связи с проектом по внедрению цифрового рубля в России и расширением системы ЕРИП в Беларуси возможны новые атаки на финансовые системы, что угрожает безопасности платежных данных и может нарушить работу этих систем.
- **Расширение фишинговых атак на многофакторную аутентификацию (MFA)**: с ростом использования MFA атакующие будут искать способы обхода этой защиты, используя фишинговые схемы для получения доступа к защищённым системам и аккаунтам.

- **Появление новых мошеннических схем и модификации уже известных** («Мамонт»). Эти схемы будут включать в себя различные механизмы: атаки через мессенджеры, с помощью сети мошеннических ресурсов, атаки на пользователей мобильных устройств с помощью мошеннических приложений.
- **Рост атак с использованием искусственного интеллекта**: ожидается увеличение использования ИИ в кибератаках, включая создание более совершенных дипфейков, автоматизацию фишинга для массовых атак, а также улучшение методов поиска уязвимостей в системах и приложениях.
- Мы предполагаем, что **мир андеграунда будет постепенно снимать запреты на работу по определенным регионам**. Сейчас активно развиваются и востребованы у киберпреступников ресурсы, где таких ограничений нет. Там они продают базы данных и корпоративные доступы компаний из СНГ.
- Прогосударственные атакующие **начнут активнее использовать массовое ВПО**, в том числе распространяемое в открытом доступе или продаваемое в андеграунде, вместо уникальных разработок. Это усложнит классификацию прогосударственных APT и финансово-мотивированных группировок.
- **Мошеннические сообщества продолжат развиваться**, из-за этого стоит ожидать роста создаваемых фишинговых и мошеннических ресурсов.
- Продолжится рост числа фишинговых атак с использованием шпионского ПО, работающего по модели **Malware-as-a-Service (MaaS)**, направленного на хищение корпоративных и личных данных атакованных пользователей — получателей писем.
- **Вредоносные фишинговые рассылки** в 2025 останутся одним из самых популярных векторов проникновения со стороны различных атакующих — компрометации устройства получателя вредоносного письма в атакуемой инфраструктуре. Главная цель фишинговых почтовых рассылок — доставка и выполнение вредоносного кода на устройстве получателя. Функционал вредоносного ПО будет зависеть от целей/мотивов киберпреступников: хищения конфиденциальных данных в рамках шпионажа, компрометации рабочих учетных данных или обеспечения удаленного доступа к зараженному устройству в рамках развития более сложной атаки на всю инфраструктуру компании, ее клиентов и подрядчиков.

Хактивизм

Введение

В 2024 году активность хактивистов в России и Беларуси была чрезвычайно высокой. Напомним, что к хактивистам мы относим злоумышленников, целью которых является привлечение внимания к политической ситуации и саботаж. Как правило, они не нацелены на получение финансовой выгоды. В своих атаках они используют различные методы — как DDoS-атаки, так и шифрование/уничтожение данных.

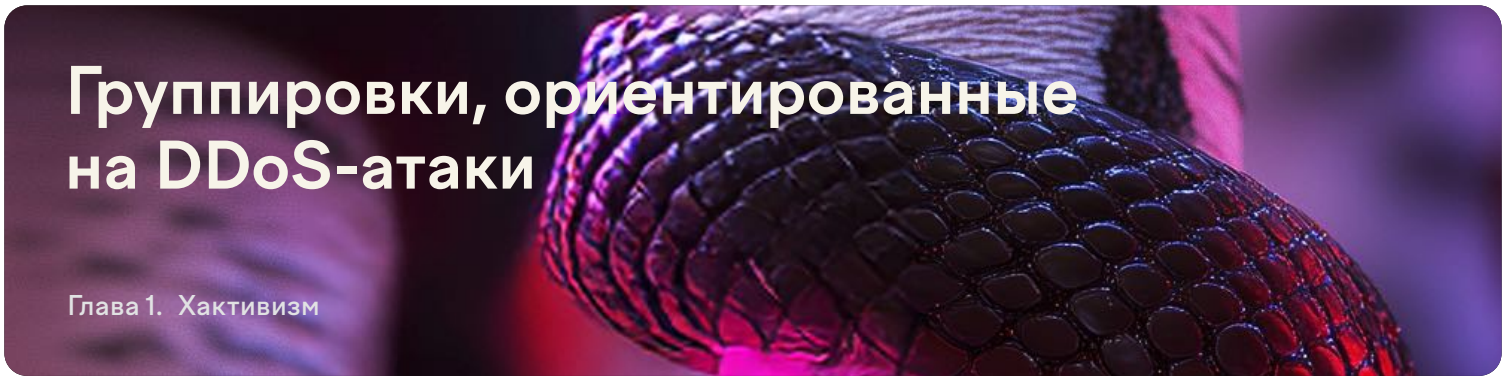
В 2024 году в атаках на Россию и Беларусь были замечены следующие группы злоумышленников:

- IT Army of Ukraine,
- Himars DDoS,
- Nebula,
- Head Mare,
- Blackjack,
- Cyber Anarchy Squad,
- CyberUnknown,
- BO Team,
- FtheSociety,
- Cybersec's,
- dumpforums,
- DC8044,
- Ukrainian Cyber Alliance (RUH8),
- Altrox,
- PANDEM1YA24,
- Ukrainian Hacker Group,
- sudo rm -RF.

Таким образом, в 2024 году **не менее 17 группировок** хактивистов атаковали российские и белорусские организации. Годом ранее таких групп было как минимум 13.

Отметим появление новых группировок: **Head Mare**, **CyberUnknown**, **BO Team**, **PANDEM1YA24**. Подчеркнем, что мы указали те группировки, которые при совершении атак попали в область нашего внимания. О некоторых из них мы расскажем подробнее. Существует также ряд хактивистов, которые в основном публикуют данные, полученные другими злоумышленниками, и большая часть их деятельности сводится к репостам в Telegram-каналах.

В последнее время у исследователей меняются подходы к классификации: в настоящее время наблюдается пересечение деятельности хактивистов, прогосударственных атакующих и группировок, использующих программы-вымогатели.



Группировки, ориентированные на DDoS-атаки

По итогам 2024 года можно заключить, что опасность DDoS-атак растет, атаки становятся мощнее и продолжительнее. Многие атаки на росийские ресурсы связаны с развитием геополитической напряженности вокруг России. Самыми заметными по активности были группировки IT Army of Ukraine, Himars DDoS, CyberSec's. Отметим, что две первые группы проводили также DDoS-атаки против ресурсов в Беларуси.

Если говорить про статистику зафиксированных атак, поставщики решений по защите от DDoS в течение года предоставляли следующие данные:

- Самая продолжительная из отраженных **DDoS-атак длилась свыше 72 часов**
- Максимальные мощности зафиксированных атак **были в сегментах онлайн-букмекеров** (446 Гбит/с), банков (316 Гбит/с), хостинговых платформ (313 Гбит/с), платежных систем (300 Гбит/с)
- По сравнению с прошлым годом количество атак **в 2024 году выросло на 53%**
- Одной из крупнейших и самых заметных для населения России стала атака **IT Army of Ukraine** на банковский сектор в июле 2024 года.

IT Army of Ukraine

IT Army of Ukraine — лидер по совершенным DDoS-атакам в 2024 году. Почти в половине случаев жертвами IT Army of Ukraine становились региональные интернет-провайдеры, в остальных случаях от действий группы пострадали предприятия из разных секторов экономики: медиа, ритейл, финансовый и банковский сектор, авиакомпании, информационные технологии и другие отрасли.

Среди основных инструментов совершения атак Distress, MHDdos, db1000nx100. Эти утилиты разворачиваются у участников группировки, в определенный момент централизованно получают список целей, вероятно, в организационной структуре IT Army of Ukraine имеется некий диспетчер, который выбирает цели и координирует атаку, далее начинается DDoS-атака.

Волна атак на новые цели обычно начинается в понедельник утром — именно в это время зачастую происходит обновление конфигураций для инструментов. На протяжении большей части 2024 года цели атак этих утилит совпадали, однако примерно с сентября злоумышленники несколько поменяли тактику и иногда стали разделять цели для разных инструментов. В ноябре-декабре 2024 года группа вернулась к прежней тактике единых целей для всех утилит.

Злоумышленники постоянно обновляют утилиты для противодействия исследователям, чтобы было сложнее выявлять цели атак и блокировать их. По оценкам аналитиков нашей компании, некоторые группы, которые ранее позиционировали себя как самостоятельные, позже влились в IT Army of Ukraine — так, например, произошло с CyberPalyanitsa.

CyberSec's

Cybersec's — хактивистская группа, которая нацелена на разрушение инфраструктуры российских организаций и саботаж их работы. Основатель группировки — пользователь под псевдонимом badb.

Методы группировки: DDoS-атаки, компрометация инфраструктуры, публикация скомпрометированных данных, атаки через подрядчиков. С конца 2024 года злоумышленники также совершают атаки с использованием шифровальщиков.

Вероятна связь данного атакующего с группировкой Shadow/Comet с 2023 года: некоторые из компаний были зашифрованы группировкой Shadow/Comet, а скомпрометированные данные впоследствии опубликованы в источниках, связанных с Cybersec's.

Для DDoS-атак группировка использует собственный инструмент — «Gorgon stress», распространяемый в Telegram-канале и имеющий веб-интерфейс и документацию. Этот инструмент постоянно обновляется, выходят новые версии. Например, 9 декабря 2024 года опубликована версия gorgon-stress-1.9.9.8, в которой злоумышленники изменили работу HTTP Flood, добавили новый тип атаки Flood WS (WSL7), использовали PROXY Protocol в HTTP Flood, что может ввести в заблуждение средства защиты от DDoS-атак.

В отличие от утилит IT Army Of Ukraine, «Gorgon stress» не предполагает механизма централизованного получения жертв и сценария работы «запустил и забыл». Для работы утилите необходимо передать параметр с целью.

Группировка CyberSec's также активно занималась саботажем. Излюбленная тактика атакующих — публикация скомпрометированных данных атакованных компаний и призывы использовать эти данные для совершения дальнейших атак через подрядчиков.

Himars DDoS

Himars DDoS — хактивистская группа, действующая с середины 2022 года. По состоянию на июнь 2023 года группа подтвердила только DDoS-атаки, направленные на информационные ресурсы России и Беларуси. При анализе жертв не выявлено секторов экономики, предпочитаемых группой. Атаки Himars DDoS малозаметны на общем фоне. Атакующие сообщают о них в своем Telegram-канале. Отметим, что периодически злоумышленники «затихают» на несколько месяцев, и активность в их Telegram-канале также прекращается. Судя по статистике, которая опубликована атакующим, мощность атак может достигать 800 Гбит/с.

В 2024 году группа сообщила в своём Telegram-канале о 104 атаках на российские организации. Для сравнения в 2022 году они провели 290 атак, а в 2023 — 360. Что меньше, чем было в 2022 и 2023 — 290 и 360 соответственно.

Cyber Anarchy Squad (C.A.S)

Одна из заметных группировок, действующих с целью кражи данных и нанесения максимального ущерба, — Cyber Anarchy Squad (C.A.S). Преступники атакуют организации в России и Беларуси с 2022 года. В 2024 году C.A.S отметилась атаками на компании из секторов ритейла, информационных технологий, производства, медиа и других сфер.

В своем Telegram-канале злоумышленники из C.A.S заявляют, что в некоторых атаках сотрудничают с другими группировками на российском и белорусском направлениях, включая U.C.A (Ukrainian Cyber Alliance), RUH8, RM-RF и др. Также при расследовании одного из инцидентов специалисты обнаружили в инфраструктуре жертвы C.A.S следы компрометации, ведущие к группировке вымогателей Shadow (Darkstar). Можно предположить, что в рамках совместной работы участники групп делятся доступами к сетям своих жертв, инфраструктурой C2 и инструментами. Для получения первоначального доступа C.A.S эксплуатирует публично доступные приложения и атаки Trusted Relationship. Для дальнейшего продвижения по инфраструктуре, удаленного управления и выполнения команд в зараженных системах атакующие использовали ВПО из открытых источников: Revenge RAT и Spark RAT. Также в атаках использовались инструменты XenAllPasswordPro, BrowserThief, Mimikatz, Metasploit, Meterpreter. С целью нанесения ущерба жертвам группировка шифрует инфраструктуру, используя слитые билдеры шифровальщика LockBit 3 Black для Windows и Babuk для Linux. Помимо шифрования, злоумышленники могут уничтожать данные в различных сегментах сети жертвы или на определенных серверах.

Head Mare

Группировка Head Mare впервые заявила о себе в конце 2023 года. Изначально злоумышленники атаковали предприятия РФ из сфер ВПК, ТЭК, IT, телекома, машиностроения, организуя утечки внутренней документации и публикуя их в социальной сети X. Однако в третьем квартале 2024 года также обнаружены атаки группы на российские коммерческие предприятия без публикации внутренних документов и с требованиями выкупа за расшифровку. Из-за действий злоумышленников работа атакованных компаний была парализована на несколько суток.

Также злоумышленники проводили deface-атаки на сайты жертв. Всплеск активности пришелся на октябрь 2024 года, тогда в течение пяти дней были атакованы пять компаний. В своих атаках Head Mare в основном использует общедоступное программное обеспечение. Для первоначального доступа и эксплуатации злоумышленники начали применять фишинговые письма, содержащие архивы с вредоносным ПО PhantomDL и PhantomRAT, а для связи с жертвами — аккаунты в мессенджере Telegram. Стоит отметить, что в арсенале злоумышленников также есть инструмент, получивший название Persey и позволяющий атакующим создавать задачи в планировщике Windows для запуска целевого файла.

Рис. 1. Пример Deface-страницы, созданной группировкой Head Mare

BO TEAM

BO TEAM — проукраинская хактивистская группировка, которая начала активно действовать в январе 2024 года. Группировка стала известна кибератаками на российские ресурсы в контексте текущей политической ситуации. Однако в ходе анализа обнаружены следы более ранней активности, которые могут быть атрибутированы этой группе.

Группировка проводила deface-атаки и использовала вредоносное ПО в виде вайпера, созданного на основе известного вымогателя Babuk. Такие программы предназначены для разрушения и шифрования данных на зараженных системах, что наносит серьезный ущерб инфраструктуре жертв. С января 2024 года группировка также начала частично публиковать данные, что является характерной чертой современных атак, цель таких действий — публичное давление на жертву.

Nebula

Группировка начала действовать в апреле 2023 года. Она сосредоточена на атаках на организации, связанные с Россией и Беларусью. В ходе атак Nebula оставляет текстовые сообщения, в которых подтверждает факт взлома и хищения данных, а также призывает к свержению действующих властей. Все действия группировка обычно сопровождает публикациями в социальных сетях — в частности, на платформе X.

Эти действия показывают, как хактивисты используют кибератаки не только для причинения ущерба, но и для распространения политических сообщений, демонстрации своей позиции и влияния на общественное мнение через Интернет.

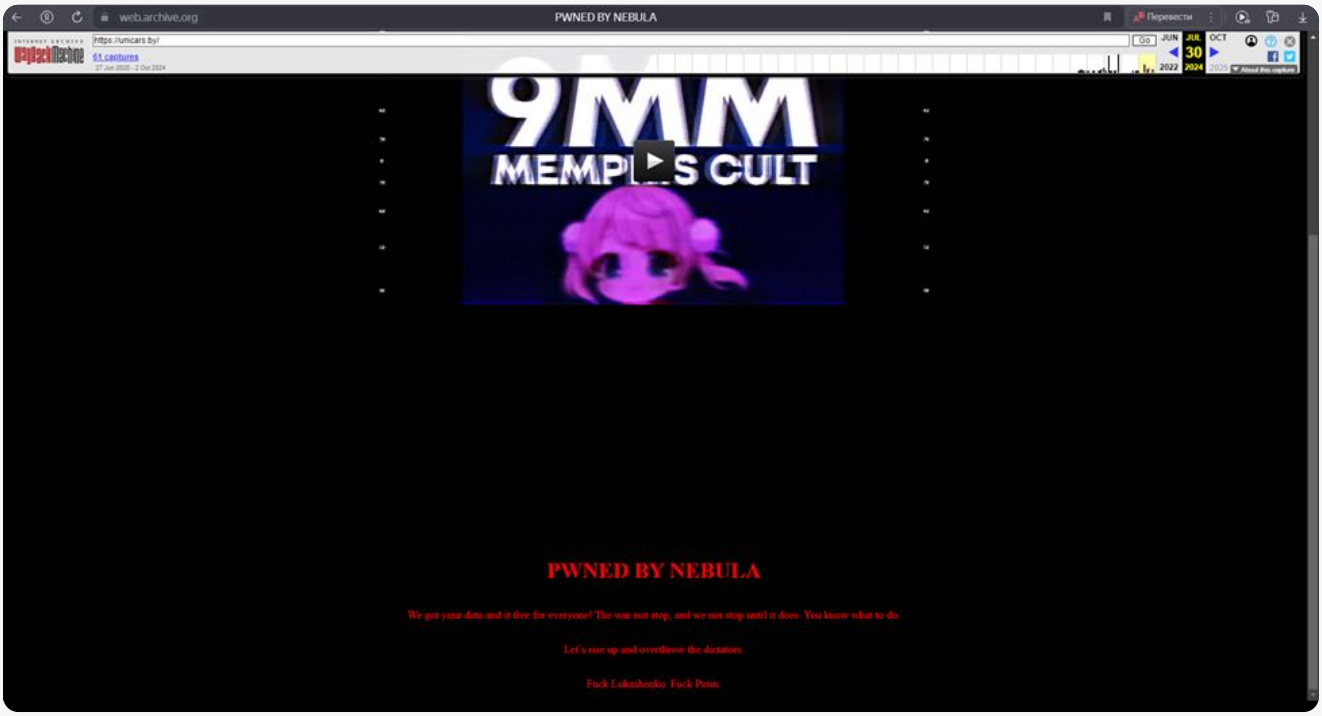


Рис. 2. Пример контента, размещаемого группировкой Nebula на атакованном ресурсе

Belarusian Cyber-Partisans

Belarusian Cyber-Partisans — это группа хактивистов, созданная 18 сентября 2020 года на фоне политических и социальных волнений в Беларуси. Группа приобрела известность благодаря атакам на правительственные системы и инфраструктуру страны. В 2024 году злоумышленники провели несколько атак на государственные и правительственные учреждения Беларуси. Как правило, эти атаки направлены на нарушение работы государственных сайтов, кражу конфиденциальных данных и создание политического давления.

Группировка активно применяла метод deface-атак для размещения политических заявлений и публикации данных, полученных в ходе атак, чтобы привлечь внимание к политическим протестам в стране.

С января по июль 2024 года группировка обнародовала информацию об атаках на инфраструктуру ряда белорусских организаций, в декабре был проведен ряд deface-атак.

Ukrainian Cyber Alliance

Ukrainian Cyber Alliance (также известная как RUH8) — группа проукраинских хакеров, появившаяся в ноябре 2015 года. Группировка известна кибератаками на российские и пророссийские цели, включая правительственные и корпоративные ресурсы. Злоумышленники проводят deface-атаки, часто изменяя содержание веб-страниц для размещения политических посланий в поддержку Украины и с осуждением действий России.

Одна из особенностей атак группы — сотрудничество с DumpForums, основным направлением деятельности которой является публикация утечек данных.

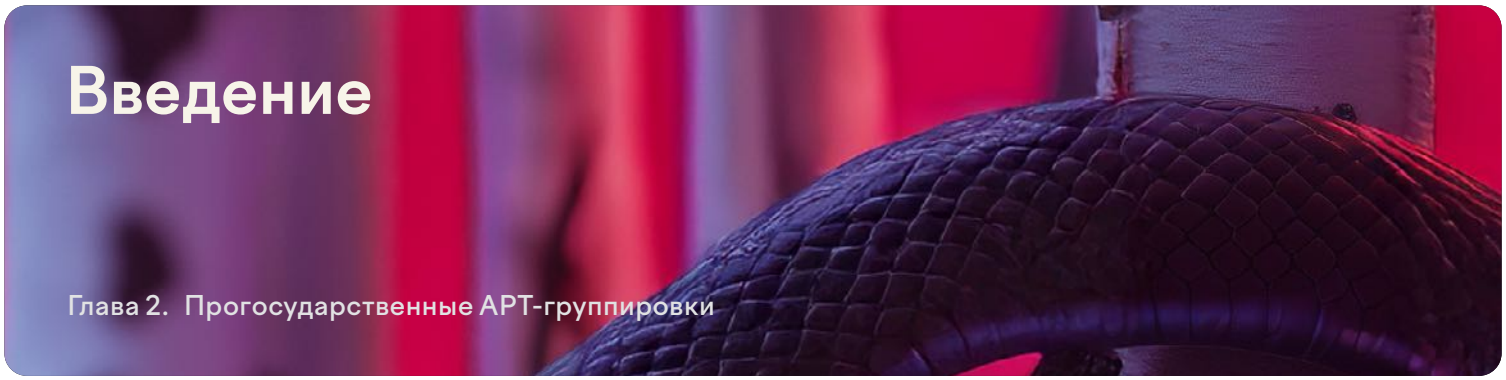
Ukrainian Cyber Alliance активно использует такие методы, как утечка конфиденциальных данных и нанесение ущерба через deface-атаки на веб-ресурсы, что является частью их киберстратегии, направленной на политическое воздействие и мобилизацию общественного мнения.

DC8044

DC8044 — группировка, действующая с января 2019 года. Изначально позиционировалась как сообщество энтузиастов в области информационной безопасности, которое занималось исследованиями и выявлением уязвимостей. После 24 февраля 2022 года группа DC8044 активно участвует в кибератаках на российские цели.

Это сообщество «предположительно» проводило совместные кибератаки с другими хактивистскими группами, такими как **Cyber Anarchy Squad (C.A.S)** и **Ukrainian Cyber Alliance (RUH8)**. Уточним: кибератаки включают, помимо прочего, deface-атаки, утечку данных и распространение вредоносного ПО, направленного на дестабилизацию работы российских ресурсов.

Прогосударственные APT-группировки



Введение

Глава 2. Прогосударственные APT-группировки

С каждым годом исследователям все сложнее классифицировать и разделять группировки на спонсируемые государством, хактивистов и финансово-мотивированных атакующих. Мы предлагаем свой вариант классификации, который актуален на начало 2025 года.

Прогосударственные APT-группировки

Всего в 2024 году **обнаружено 27 прогосударственных групп**, атакующих Россию и СНГ, деятельность нескольких из них выявлена впервые в 2024 году, хотя атаки они проводили в предыдущие годы. Общее число группировок почти вдвое превышает количество групп, деятельность которых раскрыта в 2023 году — тогда мы наблюдали 14 группировок. В 2024 году в исследуемых регионах мы не зафиксировали вредоносной активности со стороны пяти групп, упомянутых в отчете за прошлый год, однако обнаружили 12 новых групп.

Полный список APT-групп, чью вредоносную деятельность мы фиксировали на территории России и стран СНГ в 2024 году, приведен в следующей таблице. Таблица также включает группировки, проводившие атаки в предыдущие годы, о которых стало известно только в отчетном году, например, кампании групп GoldenJackal, NGC2140, NGC2180.

APT-группы, атаковавшие Россию и страны СНГ в 2024 году

f6.ru

Группировка	Страна источника угрозы	Атаки в 2024 году	Атаки до 2024 года, раскрытые только в 2024 году
Sticky Werewolf	Украина	●	
Cloud Atlas	Украина	●	
Core Werewolf	Неизвестно	●	
PhantomCore	Украина	●	
XDSpy	Неизвестно	●	
Tomiris	Казахстан	●	
Dante APT	Неизвестно	●	
ReaverBits	Неизвестно	●	●
Sapphire Cat	Украина	●	
Hellhounds	Неизвестно	●	

APT-группы, атаковавшие Россию и страны СНГ в 2024 году

Группировка/страна	Страна источника угрозы	Атаки в 2024 году	Атаки до 2024 года, раскрытые только в 2024 году
CloudSorcerer	Китай, предположительно	●	●
Mysterious Werewolf	Украина	●	
Unicorn	Неизвестно	●	
Lazy Koala	Неизвестно	●	
Obstinate Mogwai	Страна в Восточной Азии	●	●
TaxOff	Неизвестно	●	●
APT37	Северная Корея	●	●
Lazarus	Северная Корея	●	
Midge APT	Неизвестно	●	
Actor240524	Неизвестно	●	
MuddyWater	Иран	●	
Earth Krahang	Неизвестно	●	●
SugarGh0st Team	Китай	●	●
UAC-0063	Неизвестно	●	
GoldenJackal	Неизвестно		●
NGC2140	Неизвестно		●
NGC2180	Неизвестно		●

Государственные ведомства и военные организации — приоритетная цель для прогосударственных APT-групп. Этот тренд наблюдался все предыдущие годы, не стал исключением и 2024-й. Ещё в 2023 году мы отмечали увеличение количества атак на промышленные предприятия, в 2024-м их число даже немного преобладало над атаками на госсектор. Чаще всего атакующие целились на оборонно-промышленный комплекс. В 2023 году замечено 5 прогосударственных групп, атаковавших промышленность, а в 2024 раскрыто еще 6 новых групп, о деятельности которых ранее было неизвестно. Одна из групп (Mysterious Werewolf), активно атаковавшая ОПК в 2023 году, пропала с радаров исследователей в начале 2024 года. Наиболее активной в 2024 году была группа Sticky Werewolf, она проводила много атак на промышленность, также замечена за единичными атаками в десятке других сфер. Группу Cloud Atlas можно назвать одной из самых стабильных и скрытных групп: она использует один и тот же сценарий атак на протяжении долгого времени, но из-за того, что их вредоносные ссылки действуют ограниченное время или число раз, то чаще всего на момент исследования они уже недоступны, что не позволяет исследовать финальную нагрузку.

ИТ-сектор и телекоммуникации представляют интерес для атакующих как источник данных клиентов и в некоторых случаях используются для атак типа supply-chain или trusted relationship. Этот тренд начал активно использоваться в мире еще несколько лет назад, и злоумышленники, атакующие Россию и СНГ, также стали ему следовать. Например, в середине 2024 года в российской ИТ-компании произошел инцидент, классифицированный специалистами как атака на цепочку поставок. Целью злоумышленников стали организации нефтегазодобывающей отрасли. В случае успеха атака потенциально могла вызвать перебои поставок углеводородного сырья по внутренним и международным контрактам. Прямой ущерб от простоя в компании оценили более чем в 65 млн рублей, а затраты на восстановление внутренних сервисов — в 25 млн рублей. Еще один публичный пример — атака группы Cloud Atlas на государственное учреждение в Азербайджане, в инфраструктуру которого, по выводам проводивших расследование специалистов, злоумышленники попали через организацию, оказывающую техническую поддержку.

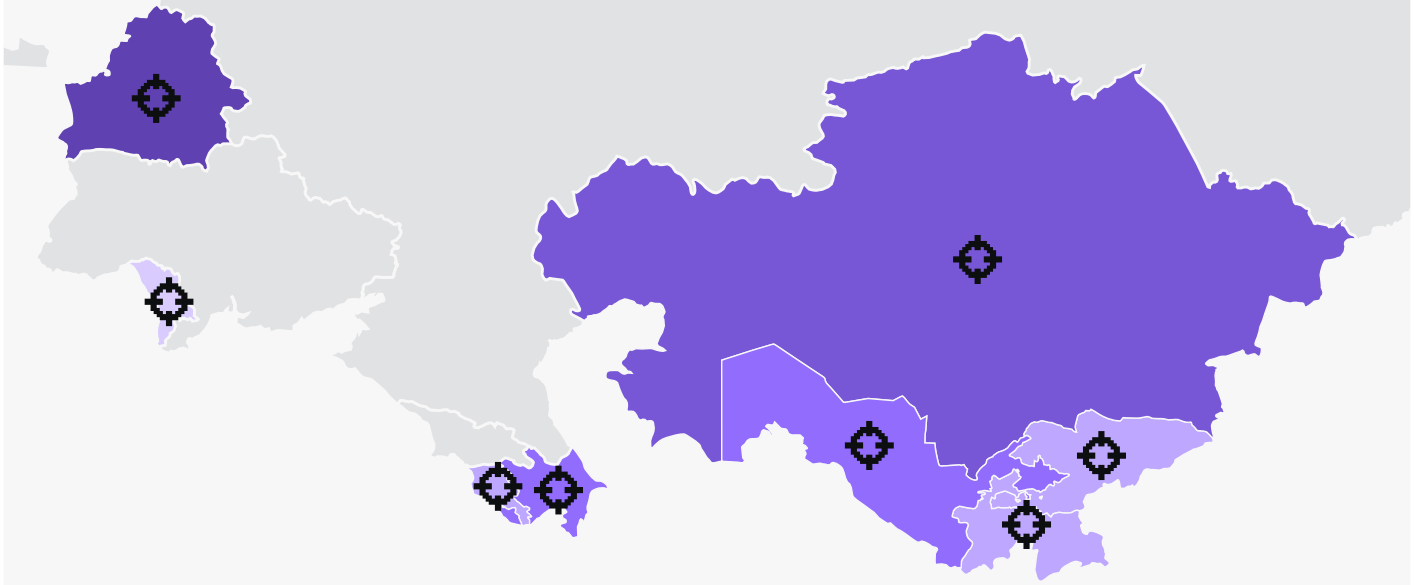
Таблица ниже содержит информацию об отраслях, атакованных прогосударственными группами в 2024 году в России. Важно учитывать, что целевых секторов и атакующих группировок на самом деле больше. В отчете рассматривались атаки, которые попали в наше поле зрения, но не для всей раскрытой вредоносной активности 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 пострадавшим организациям, которые редко открыто освещают факт компрометации.

Атаки на отрасли России в 2024 году, проводимые прогосударственными группами

Группировка/отрасль																		
Sticky werewolf	●	●	●	●	●	●		●				●	●	●	●			●	
Cloud Atlas	●						●	●					●	●					
Core Werewolf	●	●						●						●					
PhantomCore	●	●		●	●	●	●				●	●							
XDSpy	●				●				●		●		●			●			
Tomiris										●			●					●	
Dante APT	●				●		●												
ReaverBits		●					●			●			●				●		
Sapphire Cat	●							●									●		
Hellhounds	●		●		●		●	●	●		●	●	●			●	●	●	●
CloudSorcerer											●		●						
Mysterious Werewolf	●																		
Unicorn	●							●						●	●				
Lazy Koala			●										●				●		●
Obstinate Mogwai													●						
TaxOff													●						
APT37													●						
Lazarus																	●		
Midge APT																			

- Промышленность
- Торговля
- Медицина
- Туризм
- Аэрокосмическая сфера
- Лизинг
- Транспорт и логистика
- Энергетика
- ИБ
- Страхование
- ИТ
- Телекоммуникации
- Государственные учреждения
- Военная
- Религия/ благотворительность
- Строительство
- Финансы
- Горная промышленность
- Образование

Атаки на страны СНГ со стороны прогосударственных APT-групп в 2024 году



Шкала от наименее атакованной к наиболее атакованной стране

Менее — Более

Группировка/страна	AZ	AM	BY	KZ	KG	TJ	UZ	MD
Actor240524	●							
Cloud Atlas	●		●					
Sticky Werewolf			●					
Lazy Koala	●	●	●	●	●	●	●	
XDSpy			●					●
PhantomCore			●					
MuddyWater	●			●				
Core Werewolf		●	●					
Earth Krahang				●	●	●	●	
SugarGh0st Team				●			●	
UAC-0063		●		●	●	●	●	
Midge APT			●					

Ниже приводим описание сценариев атак и инструментов наиболее активных APT-групп, действовавших с целью шпионажа против организаций в России и СНГ в течение 2024 года.

Sticky Werewolf

Начало активности	Используемые инструменты	Основные техники (MITRE)	ID
Апрель 2023	• Darktrack • Sticky.Darktrack • Glory Stealer • Rhadamanthys Stealer • Ozone RAT • Quasar RAT • Sliver implant • MetaStealer • Remcos • DarkTortilla • ScrubCrypt • Ande Loader	Obtain Capabilities: Malware	T1608.001
		Phishing: Spearphishing Attachment	T1566.001
		Phishing: Spearphishing Link	T1566.002
		Command and Scripting Interpreter: Windows Command Shell / PowerShell/ JavaScript/ Visual Basic/ Python/ AutoHotKey & AutoIT	T1059
		Obfuscated Files or Information: Steganography	T1027.003
		Process Injection	T1055
		Masquerading: Double File Extension	T1036.007
		Web Service	T1102
		Non-Standard Port	T1571

f6.ru

Группировка Sticky Werewolf вошла в 2024 год громко и одной из первых — 2 и 3 января наши специалисты зафиксировали около 250 писем, направленных на адреса электронных почт телекоммуникационной компании. Письма содержали вредоносную ссылку, а в качестве финальной нагрузки предполагалась установка Darktrack RAT.

Мы уже отмечали в отчете за 2023 год, что отличительная особенность группы Sticky Werewolf — применение широко распространенного коммерческого вредоносного ПО. В 2024-м злоумышленники добавили в свой арсенал еще несколько таких инструментов, а также стали использовать самописное ПО: например, доработанный вариант DarkTrack, отслеживаемый нами по имени Sticky.Darktrack, или ранее неизвестное ВПО Glory Stealer. Отметим, что на момент обнаружения в стилере присутствовали неиспользуемые участки кода, что косвенно свидетельствует: ВПО находится в стадии доработки или является отредактированным кастомным форком другого проекта. Самый ранний образец загружен на VirusTotal в сентябре 2023 года, предположительно, разработчиком с целью проверить его детектируемость.

Высокая активность злоумышленников привлекла внимание исследователей, это позволило быстрее обнаруживать и блокировать атаки на ранних стадиях. В свою очередь, злоумышленники добавляли в арсенал новые инструменты и изобретали разные сценарии атак. Цифры говорят за себя: за год группа сменила минимум 7 сценариев атак и более 10 инструментов.

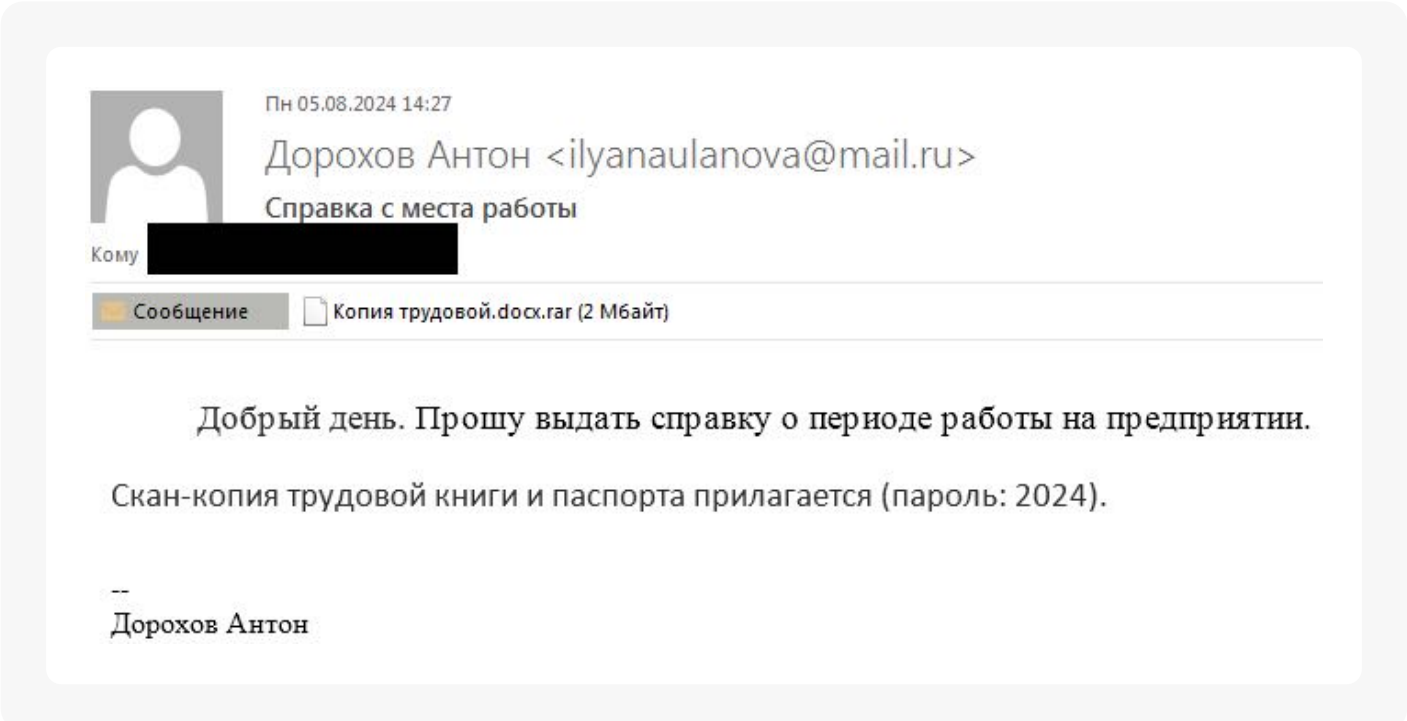
В начале 2024 года группа распространяла самораспаковывающиеся архивы посредством ссылок. Запуск архива приводит к открытию приманки и запуску лоадера, разворачивающего нагрузку на устройстве жертвы. В качестве нагрузки использовались MetaStealer и/или DarkTrack RAT.

Затем группа стала использовать Gophish для проведения рассылок. Вложение — архив, который содержит приманку и самораспаковывающийся архив. В архиве находятся различные файлы, среди которых AutoIt-скрипт и BAT-файл, собирающий из остальных файлов легитимный интерпретатор AutoIt. После запуска AutoIt-скрипта в память процесса внедряется нагрузка. Замечено использование в таком сценарии в качестве нагрузок Sticky.Darktrack, Ozone RAT, Glory Stealer, **Rhadamanthys Stealer**.

В ряде атак злоумышленники использовали DarkTortilla для загрузки полезной нагрузки в виде Darktrack RAT, а с июля 2024-го стали применять Pyinsaller-лоадеры для установки Remcos, QuasarRat.

Летом в очередной раз обновилась цепочка атаки: SFX NSIS → SFX Cabinet → .vbs- или .bat-скрипт→ Powershell → Ande Loader→ Darktrack. Batch содержит PowerShell-скрипт, который загружает с репозитория BitBucket изображение, извлекает из него загрузчик Ande Loader и загружает в память. Загрузчик используется для скачивания по определенному URL конечной нагрузки в виде DarkTrack, которая выполняется в контексте процесса RegAsm.exe. В используемых репозиториях сервиса BitBucket обнаружены десятки образцов другого ВПО, и лишь некоторые из них применялись против российских пользователей. Предполагается, что группа Sticky Werewolf использует для проведения части атак сторонний сервис по распространению ВПО.

Также осенью 2024 года начата кампания Mimistick, в ходе которой использовалась следующая цепочка атаки: 7z → MMC → CERTUTIL → NSIS EXE → BAT → AutoIt script → Quasar RAT. В ряде случаев в качестве финальной нагрузки разворачивался Sliver implant.


Пн 05.08.2024 14:27

Дорохов Антон <ilyanaulanova@mail.ru>

Справка с места работы

Кому [redacted]

Сообщение | Копия трудовой.docx.rar (2 Мбайт)

Добрый день. Прошу выдать справку о периоде работы на предприятии.

Скан-копия трудовой книги и паспорта прилагается (пароль: 2024).

--
Дорохов Антон

Рис. 3. Пример письма группы Sticky Werewolf

Начало активности	Используемые инструменты	Основные техники (MITRE)	ID
2014	• файлы со ссылкой на шаблон в потоке 1Table • CVE-2017-11882 • PowerShower • VBShower • Python-скрипт (v.3) • BloodHound • TOR • Angry IP Scanner v.3.7.6 Advanced Port Scanner v.2.5.3869	Gather Victim Identity Information: Email Addresses	T1589.002
		Phishing: Spearphishing Attachment	T1566.001
		Exploitation for Client Execution	T1203
		Command and Scripting Interpreter: Visual Basic	T1059.005
		Command and Scripting Interpreter: PowerShell	T1059.0011
		Command and Scripting Interpreter: Python	T1059.006
		Indicator Removal: File Deletion	T1070.004
		Hide Artifacts: NTFS File Attributes	T1564.004
		Template Injection	T1221
		System Binary Proxy Execution: Mshta	T1218.005
		Web Service	T1102

Атакующие продолжают использовать сценарий, описанный в конце 2023 года в **нашем блоге**. При открытии пользователем документа из вложения электронного письма происходит загрузка по ссылке удаленного шаблона. Ссылка для загрузки шаблона располагается в потоке 1Table. Загружаемый по ссылке шаблон является RTF-файлом, содержащим эксплойт для уязвимости CVE-2017-11882, в результате эксплуатации которой происходит запуск шелл-кода, предназначенного для загрузки HTA-файла по ссылке и его последующего выполнения. Последний, в свою очередь, создает файл .xml и ряд файлов в альтернативных потоках данных этого файла, в частности:

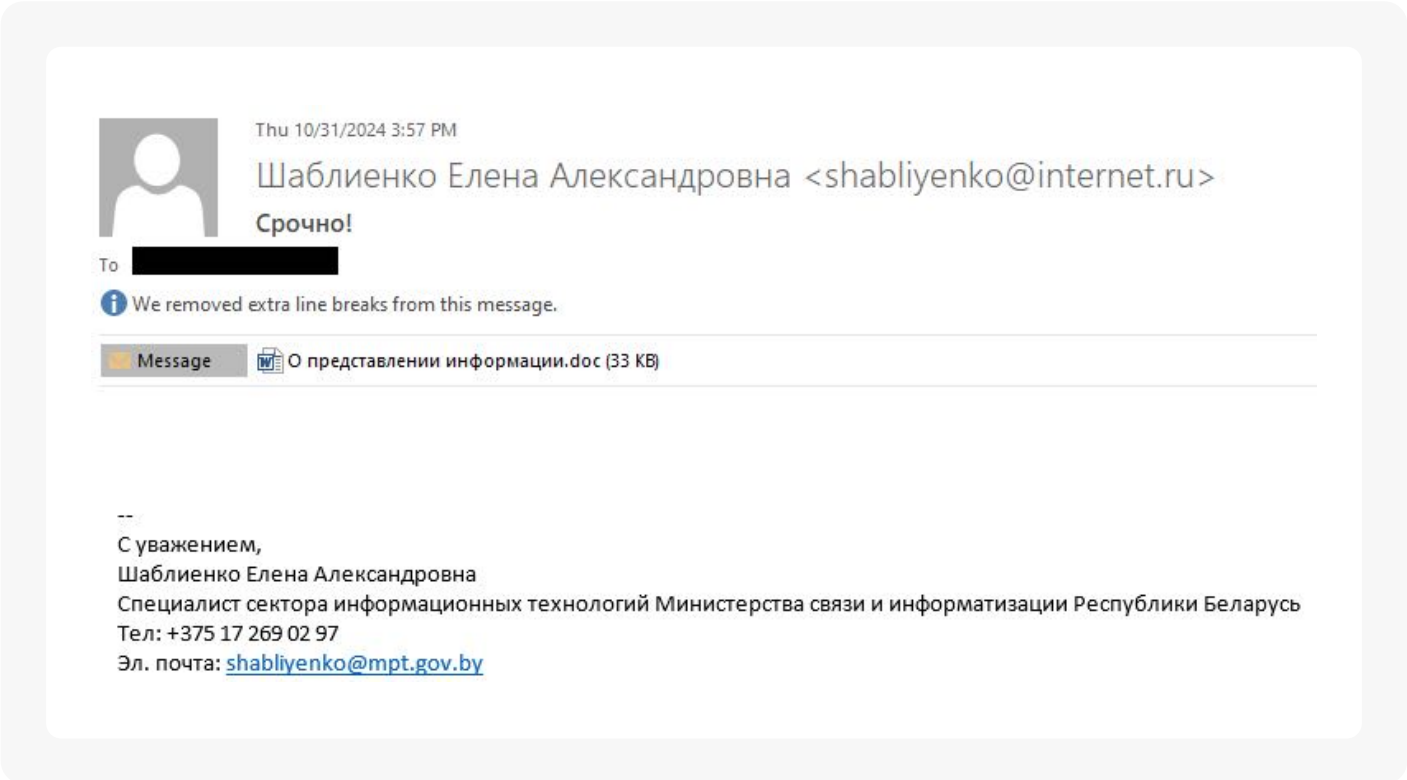
- [rnd]ing.vbs — отвечает за расшифровку и запуск содержащегося в [rnd].hxn VBS-кода;
- [rnd].vbs — идентичен [rnd]ing.vbs;
- [rnd].hxn — отвечает за декодирование содержащейся в нем полезной нагрузки и ее запуск, декодированная полезная нагрузка представляет собой VBS-код, предназначенный для загрузки следующей стадии с сервера атакующих и передачи ей управления;
- [rnd]init.vbs — VBS-скрипт отвечает за очистку содержимого VBS-скриптов и содержимого файлов из определенного каталога.

Вторая возможная цепочка атаки отличается первой частью и состоит из следующих звеньев: ZIP-архив → Batch-файл → PowerShell-скрипт → HTA-файл → VBS-скрипты (в альтернативных потоках NTFS).

На протяжении года обнаружено множество сэмплов и ссылок, однако не всегда удавалось получать дальнейшие нагрузки. Предположительно, злоумышленники используют определенную фильтрацию или ограниченное время жизни ссылок, чтобы минимизировать вероятность анализа их вредоносной деятельности исследователями.

Летом 2024 года опубликована информация об инциденте в одном из государственных учреждений Азербайджана, атрибутированном группе Cloud Atlas. Согласно данным проводивших расследование специалистов, злоумышленники получили доступ к жертве через компанию, предоставляющую ей техническую поддержку. Злоумышленники использовали Tor для обеспечения анонимности, бэкдор PowerShower, Python-скрипт (v.3), SharpHound, Angry IP Scanner версии 3.7.6, Advanced Port Scanner версии 2.5.3869, причем это ПО загружалось на устройство жертвы через Google Chrome. Большинство этих инструментов уже использовалось злоумышленниками как минимум с 2022 года, что подтверждает: группа не спешит менять подход к атакам и успешно действует с таким набором инструментов уже долгое время.

Осенью 2024 группа Cloud Atlas проводила вредоносную рассылку в адрес государственных организаций в России и Беларуси. В ходе расследования инцидента специалисты установили, что в этой кампании злоумышленники использовали «Яндекс Диск» для хранения вредоносных модулей. Cloud Atlas совершенствует и усложняет свои инструменты. Бэкдор PowerShower выполняет зашифрованные команды, спрятанные в файлах формата XML; VBShower использует Google Sheets в качестве C2.


Thu 10/31/2024 3:57 PM

Шаблиенко Елена Александровна <shabliyenko@internet.ru>

Срочно!

To [redacted]

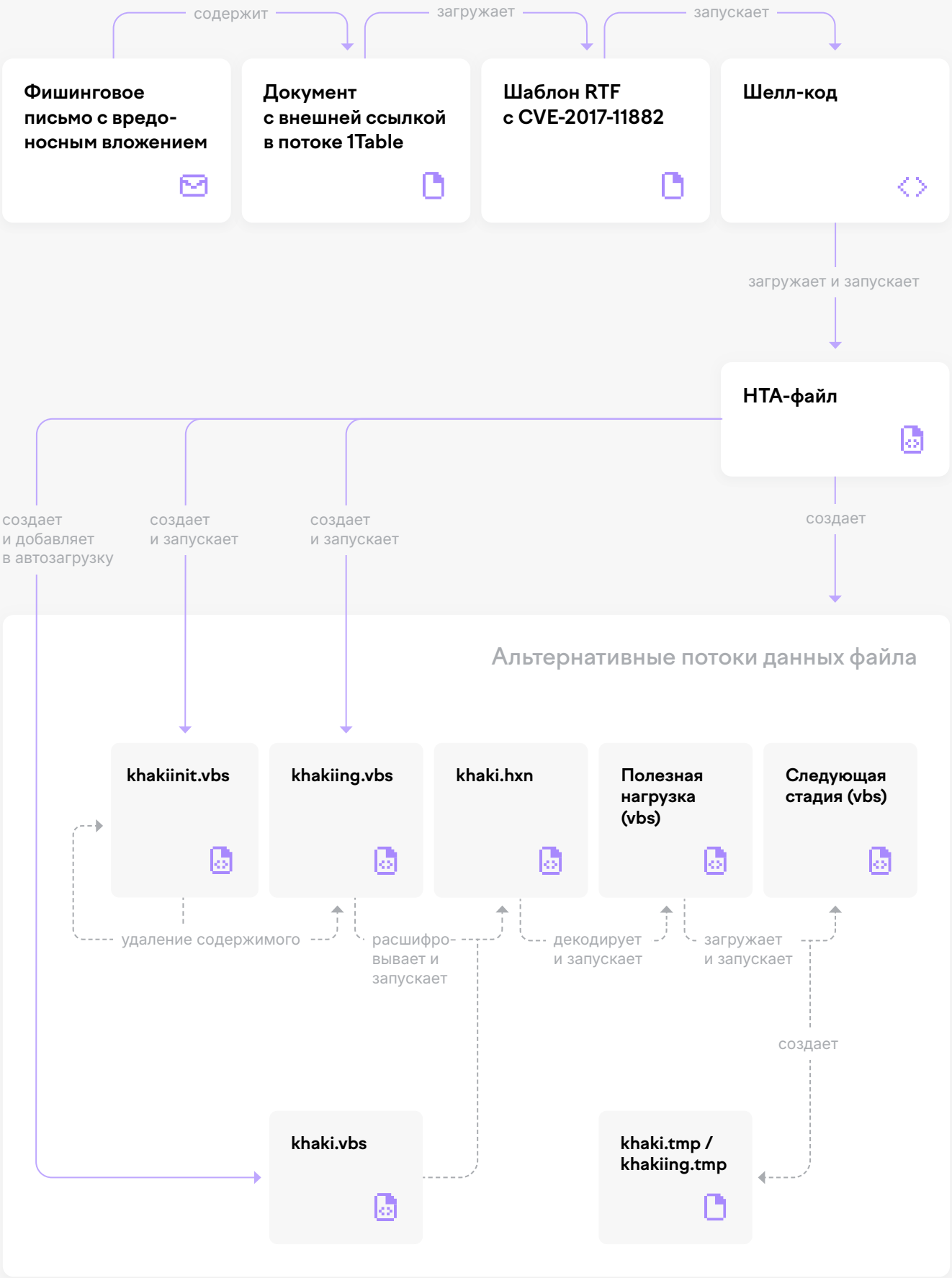
We removed extra line breaks from this message.

Message О представлении информации.doc (33 KB)

--
С уважением,
Шаблиенко Елена Александровна
Специалист сектора информационных технологий Министерства связи и информатизации Республики Беларусь
Тел: +375 17 269 02 97
Эл. почта: shabliyenko@mpt.gov.by

Рис. 4. Пример письма группы Cloud Atlas

Пример базовой цепочки атаки группы Cloud Atlas



Core Werewolf

Начало активности	Используемые инструменты	Основные техники (MITRE)	ID
Август 2021	• UltraVNC • MeshAgent • Go-дроппер • 7zSFX, RarSFX • Batch-, AutoIt-, VBS-скрипты • SSH-backdoor	Acquire Infrastructure: Domains	T1583.001
		Develop Capabilities: Malware	T1587.001
		Obtain Capabilities: Tool	T1588.002
		Phishing: Spearphishing via Service	T1566.003
		Phishing: Spearphishing Link	T1566.002
		Command and Scripting Interpreter: Windows Command Shell	T1059.003
		Command and Scripting Interpreter: AutoHotKey & AutoIT	T1059.010
		Command and Scripting Interpreter: Visual Basic	T1059.005
		Scheduled Task/Job: Scheduled Task	T1053.005
		Remote Services: VNC	T1102

f6.ru

В 2024 группа Core Werewolf продолжила использовать самораспаковывающиеся архивы 7zSFX для установки и запуска UltraVNC.

В марте наши специалисты выявили дроппер, реализованный на языке Go и предназначенный для скрытой установки и запуска легитимной программы удаленного доступа UltraVNC. Дроппер создает каталог, куда извлекает приманку, конфигурацию и исполняемый файл UltraVNC, а также Batch-файл, предназначенный для запуска и закрепления в системе UltraVNC. В мае группа впервые начала использовать AutoIt-скрипты совместно с Batch. А в июле группировка отошла от использования Batch-скипта и перенесла его возможности в AutoIt-скрипты.

Обычно деятельность группировки направлена на военную отрасль и сферу военной промышленности, одна из **атак** была нацелена на военную базу в Армении. Приманки в большинстве случаев выглядят как выписки о расположении военных объектов или списки военнослужащих. Однако летом замечен нестандартный RarSFX, который мог использоваться в атаке на сферу розничной торговли, поскольку в приманке используется логотип одного из ритейлеров, и, по-видимому, приманка предназначена для сотрудников этого ритейлера.

Минимум с июня 2024 года группа Core Werewolf распространяет вредоносные файлы не только через электронную почту, но и через мессенджеры, чаще всего через Telegram.

Летом раскрыта кампания, в ходе которой в качестве финальной нагрузки использовался не UltraVNC, а MeshAgent. Вредоносный файл попадал на машину жертвы посредством вредоносной ссылки, предположительно, полученной в фишинговом письме. Согласно данным исследователей, обнаружено более 120 целей этой кампании в России, также замечены цели в других странах, среди них Индия, Китай, Вьетнам, Тайвань, Турция, Словакия, Филиппины, Австралия, Швейцария и Чехия.

В октябре наши специалисты обнаружили, что **группа Core Werewolf начала использовать цепочку VBS-скриптов для разворачивания UltraVNC**. В общем виде килчейн можно представить так: EXE dropper → serial.vbs (разархивирует пейлоад) → contend.vbs (запускает следующий скрипт) → input.vbs → UltraVNC. Также обнаружен SSH-бэкдор, со средне-высокой уверенностью приписываемый группе Core Werewolf. После запуска бэкдор скрыто запускает SSH-сервер на порту 17241 и ожидает входящих соединений. Сервер удаленно становится доступным злоумышленнику. Файл представляет собой сборку проекта с открытым исходным кодом.

PhantomCore

Начало активности	Используемые инструменты	Основные техники (MITRE)	ID
Июль 2023	• CVE-2023-38831 • CVE-2024-43451 • PhantomCore.Downloader • PhantomRAT • PhantomDL • PhantomCore.KscDL • PhantomCore.KscDL_trim • PhantomCore.TaskRAT • PhantomCore.GreqBackdoor • Metasploit • Chisel • revsocks • WinSW • XenAllPasswordPro • MobaXTerm • Sliver	Compromise Accounts: Email Accounts	T1586.002
		Develop Capabilities: Malware	T1587.001
		Obtain Capabilities: Exploits	T1588.005
		Phishing: Spearphishing Attachment	T1566.001
		Exploitation for Client Execution	T1203
		Command and Scripting Interpreter: Windows Command Shell	T1059.003
		Masquerading	T1036
		Ingress Tool Transfer	T1105
		Multi-Stage Channels	T1104

f6.ru

Первые атаки группы PhantomCore **обнаружены** нами в 2024 году, однако самый ранний домен, используемый группировкой как управляющий сервер для одного из бэкдоров, зарегистрирован в июле 2023 года, то есть группа могла начать свою деятельность еще в прошлом году.

Судя по количеству самописных вредоносных программ PhantomCore, частоте их обновления, а также количеству атак, команда разработчиков этой киберпреступной группы усердно трудилась весь 2024 год. По числу атак PhantomCore сопоставима с группой Sticky Werewolf, но в отличие от последних предпочитает использовать ВПО собственной разработки, а не коммерческое.

В отчетный период злоумышленники проводили фишинговые рассылки с вложением, причем чаще всего отправляли письма с, вероятно, скомпрометированных легитимных адресов.

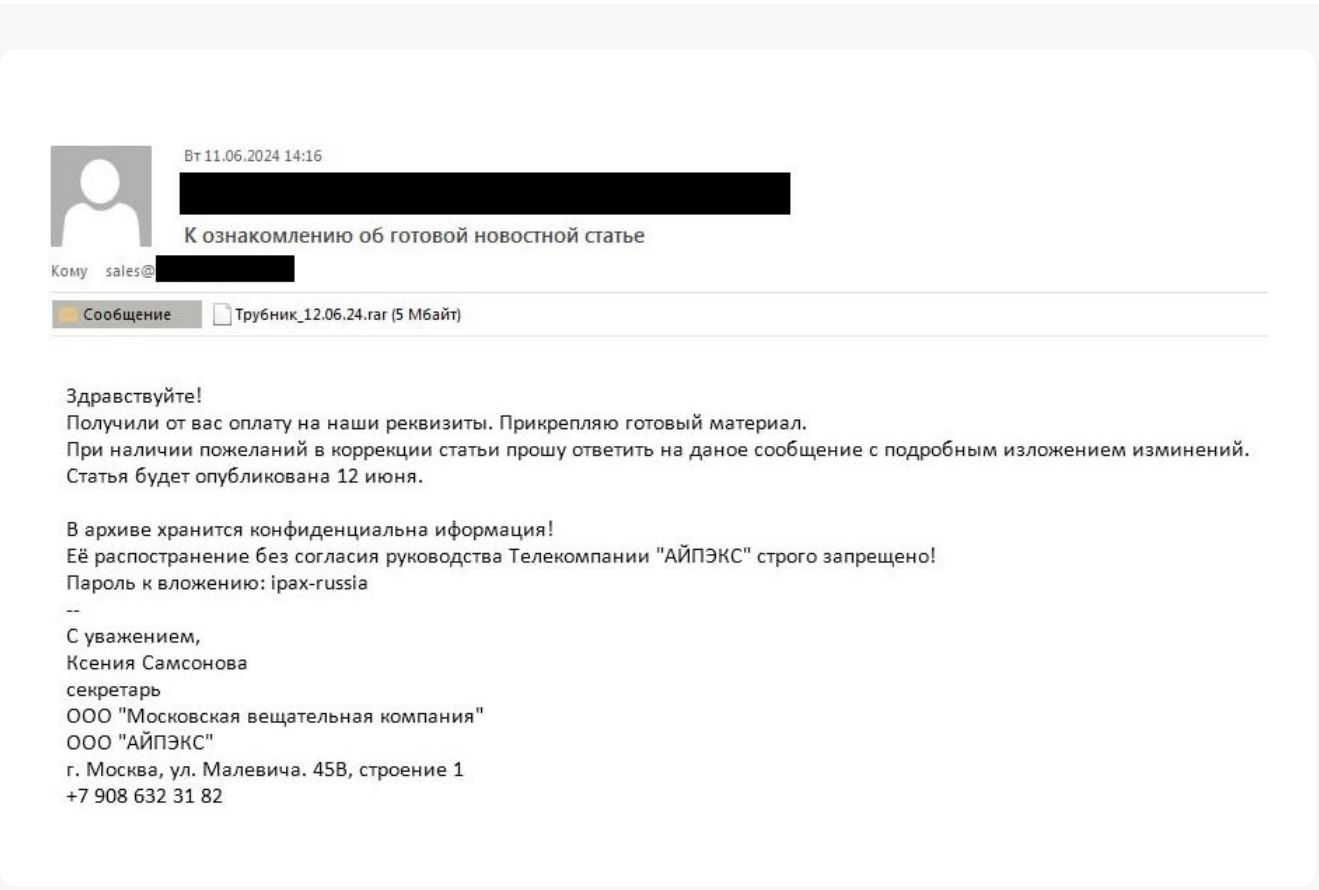
В большинстве первых атак группа распространяет защищенный паролем архив, который содержит PDF-декой и исполняемый файл. Злоумышленники эксплуатируют вариацию уязвимости WinRAR — CVE-2023-38831, в которой вместо ZIP-архивов используются RAR. Таким образом, если пользователь с версией WinRAR меньшей 6.23 запустит PDF-файл, будет запущен исполняемый файл, содержащийся в одноименной директории архива. Исполняемый файл — это загрузчик, получивший имя **PhantomDL**. Сначала он получает имя компьютера/домена жертвы, затем выполняет запрос на сервер, передавая эти данные, в ответ получает команду install для загрузки с определенного адреса следующей нагрузки или команду bay для завершения работы.

Атакующие неоднократно обновляли свой загрузчик, в частности, нами раскрыто 4 разные версии PhantomDL. Позднее злоумышленники перешли от Go-версии загрузчика PhantomDL к версии, написанной на C++, отслеживаемой нами по имени PhantomCore.KscDL. А с конца августа **стали использовать PhantomCore.KscDL_trim** — урезанную версию загрузчика PhantomCore.KscDL.

Кроме загрузчика, постоянные изменения вносились в PhantomRAT. В ходе реагирования на инцидент в предприятии химической промышленности обнаружено несколько инструментов: PhantomRAT v2; PhantomCore.TaskRAT; клиент revsocks; утилита WinSW. Поскольку атака была обнаружена и остановлена на относительно ранних стадиях, то конечную цель атакующих определить не удалось. Специалисты нашей компании установили, что в логах на зараженном сервере фигурирует IP-адрес, который предположительно связан с Metasploit. Также обнаружены логи в виде, вероятно, сгенерированном утилитой chisel. Помимо этого атакующие использовали XenAllPasswordPro (утилита для извлечения учетных данных пользователей) и MobaXTerm (программа, предназначенная для удаленного администрирования компьютеров и серверов). Атакующие также нашли в скомпрометированной сети файл с расширением .kdbx (вероятно, файл из менеджера паролей KeePass), открыли его и, предположительно, сделали экспорт в HTML и XML.

С сентября группа перестала использовать CVE-2023-38831. Злоумышленники рассылали архив, который включает два файла: исполняемый файл с расширением .zip, который содержит архив в оверлее; LNK-файл, который выполняет команду для запуска первого файла как исполняемого. В итоге устанавливается PhantomCore.GreqBackdoor.

В конце ноября группа добавила в арсенал уязвимость CVE-2024-43451, позволяющую получить доступ к NTLMv2-хешу жертвы. Стоит отметить, что об этой уязвимости стало публично известно всего за пару недель до момента использования группировкой, что подчеркивает способность злоумышленников оперативно обновлять инструментарий.



Вт 11.06.2024 14:16 [redacted]

К ознакомлению об готовой новостной статье

Кому sales@[redacted]

Сообщение | Трубник_12.06.24.rar (5 Мбайт)

Здравствуйте!
Получили от вас оплату на наши реквизиты. Прикрепляю готовый материал.
При наличии пожеланий в коррекции статьи прошу ответить на даное сообщение с подробным изложением изминений.
Статья будет опубликована 12 июня.

В архиве хранится конфиденциальна иформация!
Её распространение без согласия руководства Телекомпании "АЙПЭКС" строго запрещено!
Пароль к вложению: ipax-russia
--
С уважением,
Ксения Самсонова
секретарь
ООО "Московская вещательная компания"
ООО "АЙПЭКС"
г. Москва, ул. Малевича. 45В, строение 1
+7 908 632 31 82

Рис. 5. Пример письма группы PhantomCore

XDSpy

Начало активности	Используемые инструменты	Основные техники (MITRE)	ID
2011	• XDSpy.NSISDownloader • XDSpy.GoBackdoor • XDSpy.DSDownloader • XDSpy.CHMDownloader • XDSpy.VBSDownloader	Compromise Accounts: Email Accounts	T1586.002
		Develop Capabilities: Malware	T1587.001
		Phishing: Spearphishing Link	T1566.002
		Command and Scripting Interpreter: Windows Command Shell	T1059.003
		Command and Scripting Interpreter: PowerShell	T1059.001
		Command and Scripting Interpreter: Visual Basic	T1059.005
		Hijack Execution Flow: DLL Side-Loading	T1574.002
		System Binary Proxy Execution: Compiled HTML File	T1218.001
		Ingress Tool Transfer	T1105

В 2024 году группа XDSpy рассылала фишинговые электронные письма, содержащие ссылку на загрузку ARJ-архива с расширением .rar. В архиве находится исполняемый файл с расширением .com — самораспаковывающийся архив (SFX) NSIS, который мы классифицируем как загрузчик XDSpy.NSISDownloader. Предположительно, XDSpy использует во вредоносных рассылках скомпрометированные ранее почтовые адреса, а также спуфинг. В рамках вредоносной кампании злоумышленники атаковали такие российские организации, как НИИ в области авиации, ИТ-компании, страховые компании, ВПК, госучреждения. Кроме того, атакам были подвержены молдавский банк и некоторые белорусские организации. На момент исследования нагрузка недоступна, но на основании анализа предыдущих атак, вероятно, злоумышленники использовали бэкдор XDSpy.GoBackdoor. Это — модульный бэкдор, реализованный на Go. Каждый модуль бэкдора отвечает за определенные функциональные возможности, например: отладка, обнаружение запуска в виртуальной среде, перехват буфера обмена, создание снимков экрана рабочего стола, эксфильтрация данных.

В июле 2024 года бэкдор XDSpy.GoBackdoor обновился. Среди основных изменений можно отметить следующие: удален модуль отладки, модуль эксфильтрации данных и модуль BrowserDump дополнены новыми расширениями файлов и новыми браузерами соответственно.

В том же месяце XDSpy **рассылала** фишинговые электронные письма, содержащие ссылку на загрузку RAR-архива, в котором находятся легитимный исполняемый файл с расширением .exe и вредоносная библиотека msi.dll, запускаемая посредством техники DLL Side-Loading. DLL-файл представляет собой загрузчик, отвечающий за загрузку и запуск файла полезной нагрузки, классифицируемый нами как XDSpy.DSDownloader. В это же время обнаружен еще один загрузчик, получивший название XDSpy.CHMDownloader.

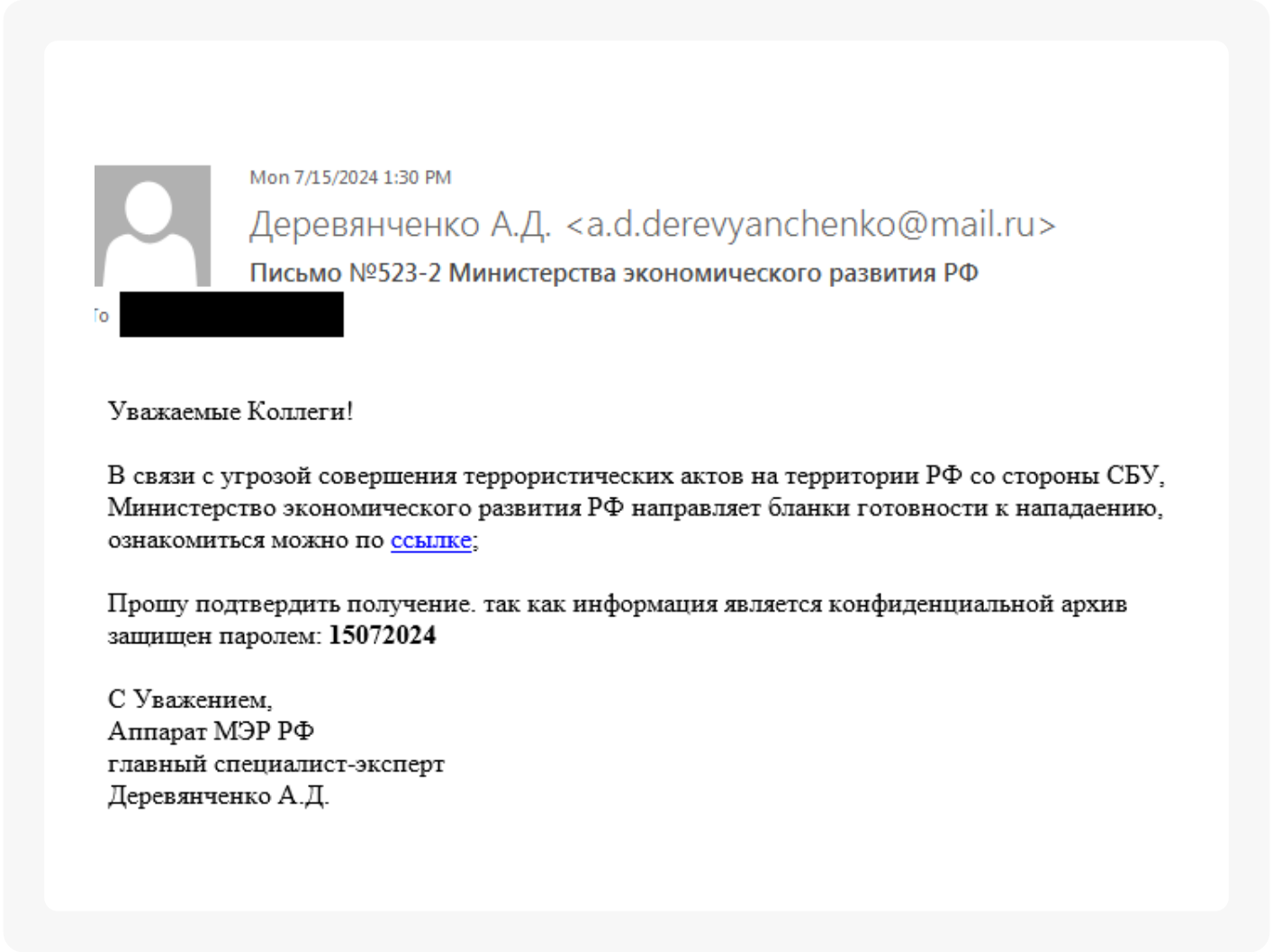
В осенних атаках группа распространяла TAR-архив, в котором содержался закодированный VBE-файл, классифицируемый как загрузчик XDSpy.VBSDownloader.

Tomiris

Начало активности	Используемые инструменты	Основные техники (MITRE)	ID
2020	JLORAT	Phishing: Spearphishing Link	T1566.002
		Command and Scripting Interpreter: Windows Command Shell	T1059.003
		File and Directory Discovery	T1083
		Screen Capture	T1059.003
		Masquerading: Double File Extension	T1036.007
		Ingress Tool Transfer	T1105
		Non-Standard Port	T1571

Группа Tomiris — не очень активная или очень скрытная группировка, атаки которой редко попадают в объектив специалистов. В 2024 году мы выявили две рассылки, направленные в адрес геологоразведочной и государственной организаций.

В июле письма были отправлены на общую почту геологоразведочной организации, второй получатель — предположительно, начальник отдела финансового департамента одного из министерств РФ. Ссылка из письма ведет на загрузку защищенного паролем архива, который содержит приманку и исполняемый файл, замаскированный под .pdf. Исполняемый файл — это загрузчик, скачивающий нагрузку в виде JLORAT с определенного адреса. Бэкдор начинает активность со сбора информации о машине жертвы, после чего отправляет HTTP-запрос POST на C2 через порт 9942. Затем JLORAT ищет определенные ключевые слова в данных, возвращаемых C2, чтобы начать обработку команд. JLORAT — программа для кражи файлов, написанная на Rust, которая собирает системную информацию, выполняет команды, выдаваемые C2-сервером, загружает файлы и делает скриншоты. Бэкдор JLORAT впервые описан в 2023 году и использовался группой Tomiris как минимум с 2022 года. О других группах, использующих эту вредоносную программу, неизвестно. Кроме того, URL C2 соответствует шаблону URL, используемому в предыдущих сэмплах группы Tomiris: http://IP:9942/bot_auth. Поэтому мы, со средней степенью уверенности, приписываем эту активность группе Tomiris.



Mon 7/15/2024 1:30 PM

Деревянченко А.Д. <a.d.derevyanchenko@mail.ru>

Письмо №523-2 Министерства экономического развития РФ

To [redacted]

Уважаемые Коллеги!

В связи с угрозой совершения террористических актов на территории РФ со стороны СБУ, Министерство экономического развития РФ направляет бланки готовности к нападению, ознакомиться можно по ссылке;

Прошу подтвердить получение. так как информация является конфиденциальной архив защищен паролем: 15072024

С Уважением,
Аппарат МЭР РФ
главный специалист-эксперт
Деревянченко А.Д.

Рис. 6. Пример письма группы Tomiris

Dante APT

Начало активности	Используемые инструменты	Основные техники (MITRE)	ID
2024	• Trojan.Siggen 27.11306 • Trojan.Packed2.46324 (a.k.a. Dante.Packer) • Trojan.Siggen28.53599 (a.k.a. Dante.Implant) • CVE-2024-6473	Develop Capabilities: Exploits	T1587.004
		Develop Capabilities: Malware	T1587.001
		Stage Capabilities: Link Target	T1608.005
		Phishing: Spearphishing Attachment	T1566.001
		Phishing: Spearphishing Link	T1566.002
		Masquerading: Double File Extension	T1036.007
		Hijack Execution Flow: DLL Search Order Hijacking	T1574.001
		Indicator Removal: File Deletion	T1070.004
		Ingress Tool Transfer	T1105

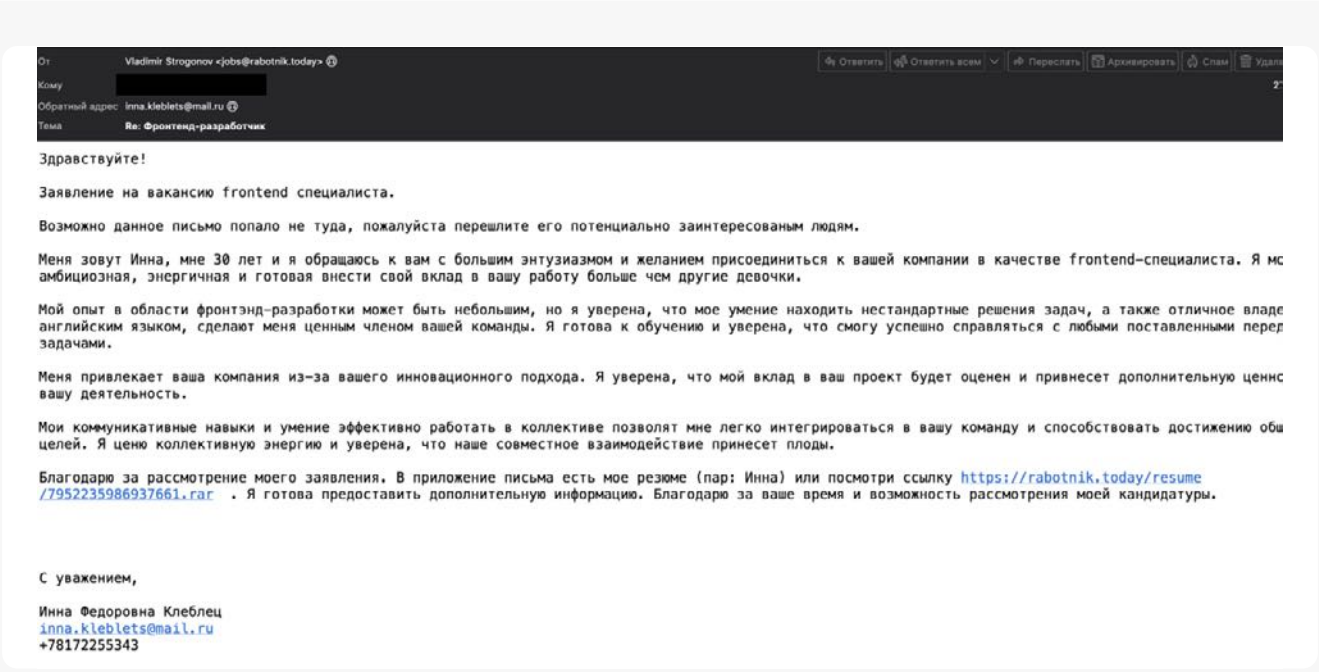
f6.ru

В марте 2024 года группа, отслеживаемая нами по имени Dante APT, попыталась провести атаку на крупного производителя железнодорожного транспорта. Цель атакующих — сбор информации о системе и запуск модульного ВПО на скомпрометированном ПК. Злоумышленники отправили фишинговое письмо, содержащее вредоносное вложение в виде архива и ссылку на вирусный архив. Архив замаскирован под резюме соискателя на вакансию frontend-специалиста. Архив содержит файл, который имеет «двойное» расширение .pdf.lnk, жертва могла видеть первое расширение — .pdf, а расширение .lnk было скрыто. Посредством .lnk скрытно происходил запуск интерпретатора команд PowerShell, скачивавшего с сайта злоумышленников два вредоносных скрипта, каждый из которых запускал свою полезную нагрузку.

Первая из нагрузок представляла собой PDF-приманку и исполняемый файл, маскирующийся под компонент для обновления Яндекс Браузера. Данный файл представляет собой дроппер трояна Trojan.Packed2.46324, который после ряда проверок распаковывал троян Trojan.Siggen28.53599. Последний имеет возможности противодействия отладке, удаленного управления, сбора системной информации и скачивания различных вредоносных модулей.

Вторая нагрузка состояла из PDF-приманки и трояна Trojan.Siggen27.11306, который представляет собой DLL с зашифрованной полезной нагрузкой. Троян эксплуатирует уязвимость Яндекс Браузера к перехвату порядка поиска DLL, получившую номер CVE-2024-6473. Он сохраняется в скрытую папку, куда устанавливается Яндекс Браузер, и там же браузер будет искать необходимые ему библиотеки при запуске. В свою очередь, легитимная библиотека с таким же именем, функция которой заключается в обеспечении безопасности запуска приложений, является системной библиотекой ОС и находится в другой папке. Так как вредоносная библиотека располагается в папке установки Яндекс Браузера, то первой будет загружаться именно она. При этом она получает все разрешения основного приложения. После запуска браузера вредоносная библиотека расшифровывает зашитую в нее полезную нагрузку. Результатом расшифровки является шелл-код, выполнение которого позволяет злоумышленникам запустить .NET-приложение. В свою очередь, этот стейджер загружал из сети вредоносную программу. На момент расследования на сервере, с которым связывался загрузчик, искомый файл не был доступен, однако, учитывая, под каким именем должно было сохраняться данное ПО, можно предположить, что этим трояном являлся Trojan.Packed2.46324.

В апреле было обнаружено письмо, направленное в адрес российского НИИ, специализирующегося на проведении научных исследований, разработке и производстве автоматизированных систем и комплексов связи для кораблей,и береговых объектов России. В качестве вложения злоумышленники рассылали защищенный паролем архив. В архиве содержится LNK-файл, посредством которого скачивается и исполняется Powershell скрипт. В результате скачивается файл, который маскируется под обновление Adobe Reader и представляет собой дроппер трояна Trojan.Packed2.46324. Такая же схема наблюдалась еще в нескольких рассылках в августе и сентябре 2024 года. Системой Managed XDR были заблокированы письма, направленные в адрес промышленной компании и НИИ, занимающегося разработками в авиационной сфере.



От Vladimir Strogonov <jobs@rabotnik.today>
Кому [redacted]
Обратный адрес: inna.kleblets@mail.ru
Тема: Re: Фронтенд-разработчик

Здравствуйте!

Заявление на вакансию frontend специалиста.

Возможно данное письмо попало не туда, пожалуйста перешлите его потенциально заинтересованым людям.

Меня зовут Инна, мне 30 лет и я обращаюсь к вам с большим энтузиазмом и желанием присоединиться к вашей компании в качестве frontend-специалиста. Я мо амбициозная, энергичная и готовая внести свой вклад в вашу работу больше чем другие девочки.

Мой опыт в области фронтэнд-разработки может быть небольшим, но я уверена, что мое умение находить нестандартные решения задач, а также отличное владе английским языком, сделают меня ценным членом вашей команды. Я готова к обучению и уверена, что смогу успешно справляться с любыми поставленными перед задачами.

Меня привлекает ваша компания из-за вашего инновационного подхода. Я уверена, что мой вклад в ваш проект будет оценен и привнесет дополнительную ценно вашу деятельность.

Мои коммуникативные навыки и умение эффективно работать в коллективе позволят мне легко интегрироваться в вашу команду и способствовать достижению общ целей. Я ценю коллективную энергию и уверена, что наше совместное взаимодействие принесет плоды.

Благодарю за рассмотрение моего заявления. В приложение письма есть мое резюме (пар: Инна) или посмотри ссылку https://rabotnik.today/resume /7952235986937661.rar . Я готова предоставить дополнительную информацию. Благодарю за ваше время и возможность рассмотрения моей кандидатуры.

С уважением,

Инна Федоровна Клеблец
inna.kleblets@mail.ru
+78172255343

Рис. 7. Пример письма группы Dante APT

ReaverBits

Начало активности	Используемые инструменты	Основные техники (MITRE)	ID
2023	• MetaStealer • LuckyDownloader	Obtain Capabilities: Malware	T1588.001
		Trusted Relationship	T1199
		Phishing: Spearphishing Attachment	T1566.001
		Phishing: Spearphishing Link	T1566.002
		Process Injection: Portable Executable Injection	T1055.002

В начале 2024 года специалисты Threat Intelligence **обнаружили** новую группу, которой дали имя ReaverBits: «reaver» (в переводе «вор»), поскольку атакующие похищали данные с помощью стилера, а «bits» — из-за использования в URL-адресах «bitbucket» и «bitrix». В большинстве атак группа использовала спуфинг адреса отправителя. Письма содержат ссылки на защищенные паролем архивы, внутри которых расположены исполняемые файлы, классифицируемые как MetaStealer.

Группа активна с декабря 2023 года, до мая 2024-го зафиксировано 5 рассылок в адрес российских компаний из сферы ритейла, телекоммуникаций, процессинговую компанию, агропромышленное объединение и федеральный фонд.

Январские рассылки выбивались из классического килчейна группировки. Злоумышленники применили загрузчик LuckyDownloader, предположительно, воспользовавшись услугой стороннего актора, отслеживаемого по имени LuckyBogdan. Письма содержали ссылки, при переходе по которым мог загрузиться либо архив, либо исполняемый файл. Хеш-суммы файлов в архиве совпадают с хеш-суммой файла, который мог быть загружен по прямой ссылке из письма. Этот файл является загрузчиком вредоносного ПО, получившим название LuckyDownloader. Он выполняет загрузку и расшифровку файла, который будет внедрен в память легитимного процесса и исполнен в контексте этого процесса. В обнаруженном случае нагрузка загружалась с bitbucket.org и представляла собой MetaStealer. В ходе исследования других файлов, расположенных в этом репозитории, было установлено, что они имеют разные классификации и инфраструктуру, а атаки на основе этих инструментов имеют разные региональные цели и методы распространения. На основании имеющихся данных сформирован актор с именем LuckyBogdan, который, предположительно, занимается шифрованием полученного от клиента ВПО, размещает его в зашифрованном виде в репозитории в BitBucket и предоставляет оператору загрузчик LuckyDownloader, который выполнит доставку, расшифровку и запуск ВПО на зараженной системе.

Летом мы не наблюдали активности группы ReaverBits. А осенью замечены рассылки с темами, посвященными необходимости установки цифровых сертификатов. Целями стали два банка, две страховые компании, кредитный брокер, финансовый маркетплейс, транспортно-логистическая группа компаний, а также компания, занимающаяся грузовыми автомобильными перевозками. Отметим, что в большинство организаций злоумышленники повторно разослали письма с другими ссылками с интервалом в несколько дней.

Sapphire Cat

Начало активности	Используемые инструменты	Основные техники (MITRE)	ID
2024	• SapphireStealer (a.k.a. FunnyCat.Stealer) • FunnyCat. Downloader • FunnyCat.Dropper	Develop Capabilities: Malware	T1587.001
		Indicator Removal: File Deletion	T1070.004
		Browser Information Discovery	T1217
		File and Directory Discovery	T1083
		Archive Collected Data	T1560
		Automated Collection	T1119
		Data Staged: Local Data Staging	T1074.001
		Application Layer Protocol: Web Protocols	T1071.001
		Ingress Tool Transfer	T1105
		Fallback Channels	T1008
		Web Service: One-Way Communication	T1102.003

f6.ru

В 2024 году наши специалисты зафиксировали серии атак с использованием вредоносных программ семейства FunnyCat (дроппер, **стилер**, загрузчик). Данные атаки атрибутированы к кластеру активности, названному нами Sapphire Cat.

Первоначальный вектор атаки, предположительно — фишинговое письмо. На основании данных, полученных в ходе исследования, можно выделить два сценария атаки:

1. Пользователь получает фишинговое письмо, содержащее вредоносное вложение или короткую ссылку для загрузки вредоносной программы. Пользователь открывает вредоносное вложение или загружает его по короткой ссылке. Запускается вредоносная программа FunnyCat.Dropper, которая запускает FunnyCat.Stealer и закрепляет в системе FunnyCat.Downloader, используя планировщик задач Windows. Во время работы FunnyCat.Dropper пользователю демонстрируется документ-приманка для отвлечения внимания. Как правило FunnyCat.Dropper имеет иконку PDF-документа и расширение .exe.
2. Пользователь получает фишинговое письмо, содержащее вредоносное вложение или короткую ссылку для загрузки вредоносной программы. Пользователь открывает вложение или загружает его по ссылке. Запускается вредоносная программа FunnyCat.Stealer, которая демонстрирует пользователю документ-приманку для отвлечения внимания и закрепляет в системе FunnyCat.Downloader, используя планировщик задач Windows.

Специалисты нашей компании обнаружили, что стилер доступен для скачивания в Telegram-канале, а его исходный код опубликован в двух постах на андеграундном форуме в 2022 году. SapphireStealer — это C#-стилер, который собирает информацию о хосте, данные из браузеров, файлы. Также он способен делать снимки экрана и отправлять украденные данные в виде ZIP-архивов. Но так как стилер был размещен в публичном доступе, то функциональные возможности экземпляров SapphireStealer могут варьироваться.

Стилер добавляет полученные данные из скомпрометированной системы в ZIP-архив, который посредством бота отправляется в определенный Telegram-чат. Также стилер получает при обращении к определенному Telegram-каналу адрес сервера для отправки ZIP-архива с украденными данными. Стилер получает код веб-страницы с Telegram-каналом, находит в коде веб-страницы строку, закодированную Base64 с помощью регулярных выражений, декодирует строку и получает адрес сервера и отправляет на него ZIP-архив. После передачи подготовленный ZIP-архив с украденными данными удаляется.

Hellhounds

Начало активности	Используемые инструменты	Основные техники (MITRE)	ID
2021	• Decoy Dog • Sliver • 3snake	Develop Capabilities: Malware	T1587.001
		Trusted Relationship	T1199
		Masquerading: Match Legitimate Name or Location	T1036.005
		Input Capture	T1056
		Application Layer Protocol: DNS	T1071.004

В 2023 году сообщалось о 20 жертвах группы Hellhounds, в 2024 специалистам удалось выявить еще 28 жертв среди российских организаций во множестве отраслей. Анализ новых атак показывает, что злоумышленники преимущественно нацелены на IT-компании, большинство из которых являются подрядчиками критически важных организаций. Предположительно, такую активность можно объяснить желанием реализовать атаки через поставщика (trusted relationship). В двух инцидентах группе удалось проникнуть в инфраструктуру жертв через подрядчика. Скомпрометировав учетные данные для входа по протоколу SSH, злоумышленники проникли в инфраструктуру и установили бэкдор Decoy Dog.

Помимо уже известных атак на узлы под управлением ОС Linux, в процессе реагирования на инцидент в транспортной компании специалисты обнаружили успешные атаки с помощью Decoy Dog на Windows, о которых ранее не сообщалось. Также злоумышленники использовали фреймворк Sliver и модифицированную утилиту 3snake для получения учетных записей на узлах под управлением Linux.

CloudSorcerer

Начало активности	Используемые инструменты	Основные техники (MITRE)	ID
2020	• CloudSorcerer • GrewApacha • PlugY • RCSession • GetOutlookInfo • SharpHound • Mimikatz • nbtscan	Acquire Infrastructure: Web Services	T1583.006
		Develop Capabilities: Malware	T1587.001
		Obtain Capabilities: Malware	T1588.001
		Phishing: Spearphishing Attachment	T1566.001
		Inter-Process Communication	T1559
		Hijack Execution Flow: DLL Side-Loading	T1574.002
		Web Service: Bidirectional Communication	T1102.002
		Multi-Stage Channels	T1104
		Exfiltration Over Web Service: Exfiltration to Cloud Storage	T1567.002
		Transfer Data to Cloud Account	T1537

f6.ru

В июле 2024 года исследователи опубликовали информацию о новой группе, нацеленной на российские государственные организации, и присвоили ей имя CloudSorcerer. Одноименная вредоносная программа CloudSorcerer работает как отдельные модули (связи и сбора данных) в зависимости от запущенного процесса. Примечательная особенность — в качестве исходного командного сервера используется страница GitHub. Создается впечатление, что это легитимная и активная страница GitHub, однако в разделе «Автор» на странице GitHub есть интересная строка в шестнадцатеричной кодировке, которая начинается и заканчивается одинаковой последовательностью байтов: CDOY. После ряда преобразований этой строки формируется новый массив байтов. Первый расшифрованный байт — это число, которое указывает вредоносной программе, какую облачную службу использовать. Например, если это байт 1, то вредоносная программа использует облако Microsoft Graph, а если 0 — Yandex Cloud. Следующие байты представляют собой строку токена авторизации, который использует облачный API для аутентификации. После этого вредоносная программа создает два отдельных потока: один отвечает за получение данных из канала Windows, а другой — за отправку данных в этот канал. Эти потоки обеспечивают асинхронный обмен данными между модулями командного сервера и бэкдора. Наконец, модуль командного сервера взаимодействует с облачными службами: считывает данные, получает закодированные команды, декодирует их с помощью таблицы символов и отправляет через именованный канал в модуль бэкдора. И наоборот: получает результаты выполнения команд или эксфильтрованные данные от модуля бэкдора и записывает эти данные в облако.

В конце июля 2024 года выявлена кампания EastWind, нацеленная на российские государственные и IT-организации. Для первоначального заражения злоумышленники отправляли вредоносные письма с RAR-архивами во вложении. В ходе этих атак группа использовала следующее ВПО: троян GrewApacha, обновленный бэкдор CloudSorcerer, ранее неизвестный имлпант PlugY. В новой версии CloudSorcerer в качестве первоначального командного сервера используются страницы профилей в русскоязычной социальной сети «Живой Журнал» и на сайте вопросов и ответов Quora. Специалисты установили, что при помощи CloudSorcerer злоумышленники загружали на зараженные компьютеры ранее неизвестный имплант, и присвоили ему имя PlugY. Набор команд, который PlugY может принимать от сервера, довольно обширен: от работы с файлами и исполнения шелл-команд до наблюдения за действиями на экране, логирования нажатий клавиатуры и слежения за буфером обмена. В ходе разработки импланта, вероятно, использовался код бэкдора DRBControl, ассоциированного с группой APT27.

В 2022 году наши специалисты проводили реагирование на инцидент в российской IT-организации. В ходе реагирования обнаружены следующие вредоносные программы и инструменты:

- программа удаленного администрирования (бэкдор) RCSession;
- программа удаленной загрузки shellcode;
- программа удаленного администрирования (бэкдор) #1;
- программа удаленного администрирования (бэкдор) #2;
- программа удаленного администрирования (бэкдор) #3;
- прокси-сервер;

- скрипты PowerShell удаленной загрузки shellcode #1;
- BAT-файл удаленной загрузки скрипта PowerShell;
- GetOutlookInfo, SharpHound, Mimikatz, nbtscan.

В ходе анализа установлено, что бэкдор RCSession, бэкдор #1, бэкдор #3, программа удаленной загрузки shellcode, прокси-сервер имеют общее авторство и ассоциированы с группой Mustang Panda. В то же время бэкдор #2 можно атрибутировать группе APT31.

Проанализировав исследование о деятельности CloudSorcerer, мы пришли к выводу, что бэкдор CloudSorcerer — это не что иное, как бэкдор #3, который выявлен нами в ходе реагирования на инцидент, а как упоминались выше, этот бэкдор ассоциирован с группой Mustang Panda. Позднее исследователи опубликовали информацию о недавних атаках группы с использованием инструментов CloudSorcerer, GrewApacha, PlugY. Причем, согласно этому исследованию, последние два инструмента также связаны с другими китайскими группами, APT31 и APT27, соответственно. Стоит отметить, что в рамках реагирования на инцидент мы связывали бэкдор #2 с группой APT31, а дополнительное сравнение показало, что бэкдор GrewApacha — это и есть бэкдор #2 из нашего реагирования.

На основе описанных пересечений мы полагаем, что за группой, проводившей атаку на IT-организации в 2022 году, и группой CloudSorcerer стоят одни и те же злоумышленники, которые имеют доступ к инструментам минимум трех китайских группировок.

Mysterious Werewolf

Начало активности	Используемые инструменты	Основные техники (MITRE)	ID
Сентябрь 2023	• Mysterious.TelePy • DotnetCat • Chisel • ngrok.exe • revsocks	Acquire Infrastructure: Web Services	T1583.006
		Develop Capabilities: Malware	T1587.001
		Obtain Capabilities: Tool	T1588.002
		Command and Scripting Interpreter: Windows Command Shell / PowerShell/ Visual Basic/ Python	T1059
		Masquerading: Double File Extension	T1036.007
		Indicator Removal: File Deletion	T1070.004
		Data Staged: Local Data Staging	T1074.001
		Web Service: Bidirectional Communication	T1102.002

f6.ru

Mysterious Werewolf раскрыта в конце 2023 года. Группа атаковала промышленные организации России и Беларуси. Последняя активность замечена в середине января 2024 года.

В начале января обнаружены вредоносные Batch-файлы дропперы, которые создают на компьютере жертвы вредоносные Batch-файлы загрузчики. Атакующие используют облачное хранилище Яндекс.Диск для размещения вредоносных файлов следующих стадий. В качестве итоговой полезной нагрузки на компьютере жертвы разворачивается вредоносный Python-скрипт, классифицируемый нами как троян удаленного доступа. Этот троян мы назвали Mysterious.TelePy ввиду его функциональных особенностей и языка, на котором он написан. RAT выполняет поступающие от атакующих PowerShell-команды, загружает с заданного атакующими сервера определенный файл на компьютер жертвы. Для коммуникации RAT использует Telegram-бот и персональный чат. Применяемые злоумышленниками документы-приманки представляют собой письма российских государственных организаций, таких как Минпромторг России, Ростехнадзор. Приманки, судя по содержимому, предназначены для атак на российские промышленные компании. По ряду признаков эта кампания приписана группе Mysterious Werewolf.

В ходе анализа нашим специалистам удалось установить несколько жертв, которых мы оповестили о вероятной компрометации. Помимо этого, аналитики компании раскрыли часть дополнительных индикаторов и используемых злоумышленниками инструментов. Во время работы Mysterious.TelePy, установленного на устройстве жертвы, бот отправлял команды для загрузки с C2-сервера таких инструментов, как DotnetCat, Chisel, ngrok.exe и, предположительно, revsocks.

APT37

Начало активности	Используемые инструменты	Основные техники (MITRE)	ID
2012	KONNI	Event Triggered Execution: Installer Packages	T1546.016
		Command and Scripting Interpreter: Windows Command Shell	T1059.003
		Masquerading: Masquerade Task or Service	T1036.004
		File and Directory Discovery	T1083
		Archive Collected Data	T1560

В начале 2024 года исследователи обнаружили вредоносный установщик ПО «Статистика КЗУ». Специалистам не удалось найти какие-либо общедоступные ссылки на это ПО, однако на основании путей установки, метаданных файлов и руководств пользователя, включенных в установщик, предполагается, что исходное ПО предназначено для внутреннего использования в МИД России. В составе установщика обнаружены два файла руководства пользователя, в которых подробно описывается установка и использование ПО. Исследователи смогли запустить установщик и использовать инструкции из руководств для доступа к установленному ПО в автономном режиме. Установщик представляет собой MSI-файл с ВПО, интегрированным в процесс установки. Когда пользователь запускает установщик, определяется среда (32/64-разрядную) и выбирается соответствующая нагрузка. В конечном итоге выполняется .bat файл, который отвечает за копирование файлов и настройку службы Windows для закрепления, выполнения, а также копирования включенной конфигурации вместе с файлом полезной нагрузки. Набор возможностей KONNI позволяет операторам выполнять команды, загружать и выгружать файлы, а также указывать интервалы ожидания. Связь осуществляется через HTTP. При передаче файлов KONNI сверяет расширения со списком типов файлов, которые он передает. Файлы других расширений сжимаются в архив .CAB и затем отправляются.

В мае 2024 года обнаружено несколько схожих по логике запуска файлов с именами SpravkiBKsetup_ver._2.5.msi, которые загружены на публичную песочницу в октябре 2023 года. Справки БК — это легитимное ПО, предназначенное для заполнения справок о доходах, расходах, имуществе и обязательствах имущественного характера. При сравнении раскрытых сэмплов с оригинальным ПО с официального сайта исследователи заметили, что злоумышленники добавили несколько вредоносных файлов. При запуске вредоносная программа выполнит .bat файл, который аналогичен рассмотренному выше.

Obstinate Mogwai

Начало активности	Используемые инструменты	Основные техники (MITRE)	ID
Сентябрь 2023	• VIEWSTATE exploitation framework • CVE-2012-0002 • KingOfHearts • Donnect • DimanoRAT • AntSpy • Trochilus • SessionGopher • dns-dump.ps1 • autokerberoast_nomimi_stripped.ps1	Exploit Public-Facing Application	T1190
		Command and Scripting Interpreter: PowerShell/ Unix Shell/ Visual Basic/ Windows Command Shell	T1059
		Valid Accounts	T1078
		Trusted Relationship	T1199
		Use Alternate Authentication Material: Pass the Hash	T1550.002
		Process Injection: Dynamic-link Library Injection	T1055.001

Начало активности	Используемые инструменты	Основные техники (MITRE)	ID
Сентябрь 2023	• VIEWSTATE exploitation framework • Donnect • DimanoRAT • AntSpy • Trochilus • SessionGopher • dns-dump.ps1 • autokerberoast_ nomimi_stripped.ps1	Process Injection: Thread Execution Hijacking	T1055.003
		Steal or Forge Kerberos Tickets: Kerberoasting	T1558.003
		Remote Services: Remote Desktop Protocol/ SMB/Windows Admin Shares/ SSH/ Windows Remote Management	T1021

f6.ru

В конце 2023 года специалисты проводили расследование атаки на российскую телеком-компанию, первые следы присутствия атакующих в сети датировались 2021 годом. Атака была приписана APT-группе, получившей название **Obstinate Mogwai** (или «Упрямый Демон» в переводе с английского). «Упрямый», потому что в ходе работы над инцидентом исследователи наблюдали, как хакеры возвращались в атакованную организацию, пока им окончательно не закрыли все возможности для проникновения. Для входа в сеть хакеры использовали уязвимость десериализации ненадежных данных в параметре ViewState среды ASP.NET. В ходе атаки злоумышленники заразили почти всю инфраструктуру цели: контроллеры доменов, почтовые серверы и ряд других серверов (например, WSUS, системы баз данных, системы разработки, терминальные серверы), системы на периметре и системы ключевых администраторов. Инфраструктура жертвы достаточно разветвленная и имеет множество связанных подсетей других организаций (клиентов и партнеров).

В октябре 2024 года исследователи опубликовали информацию, полученную в ходе расследования трех инцидентов в российских организациях. В исследованных атаках, проведенных группой в 2023 и 2024 годах, атакующие использовали KingOfHearts, TrochilusRAT, а также два новых бэкдора — Donnect и DimanoRAT.

Продолжение активности этой группы специалисты увидели в сентябре 2023 года, когда её целью стала государственная организация. Атаку обнаружили на ранних стадиях. Злоумышленники проникли в инфраструктуру через подключение по VPN без второго фактора, использовав скомпрометированную легитимную учетную запись сотрудника. Основной целью был Exchange. Предположительно, таким образом участники группы хотели закрепиться в инфраструктуре и выполнять дальнейшие действия с использованием десериализации VIEWSTATE. Специалисты выявили следы использования скриптов SessionGopher, dns-dump.ps1, autokerberoast_nomimi_stripped.ps1. Также на Exchange на сетевом периметре имелись следы попыток эксплуатации уязвимости CVE-2012-0002, но на всех системах жертвы эта уязвимость была пропатчена, и потому атака не получила продолжения.

Еще одна атака на другую государственную организацию произошла в январе 2024 года, её обнаружили и пресекли на ранней стадии. Атакующие стремились завладеть Exchange. Предположительно, они планировали закрепиться в инфраструктуре и развивать атаку с помощью десериализации .Net. Другими целями стали различные системы сотрудников, через которые злоумышленники стремились получить доступ к конфиденциальным документам и другой ценной информации. Следы начала атаки обнаружены в событиях IIS, поступающих в SIEM. В них фиксировались GET- и POST-запросы, которые шли с адреса, ранее использовавшегося группировкой. Запросы шли под сертификатом одного пользователя к данным учетной записи другого. В ходе расследования установлено, что сертификаты и учетные записи принадлежат подрядчику организации. Для доступа к серверам, на которых были развернуты системы электронного документооборота, использовались скомпрометированные привилегированные учетные записи подрядчика, предназначенные для администрирования и настройки СЭД и имеющие доступ к конфиденциальным документам. Полное исследование систем подрядчика специалистами не проводилось, потому точки входа в инфраструктуру установить не представилось возможным.

Обзор менее активных прогосударственных APT-группировок

Далее кратко описана деятельность группировок, чьи атаки в 2024 году в России и СНГ были менее заметны, а также активность групп, атаковавших рассматриваемый регион ранее, но раскрытых только в 2024-м.

Lazy Koala

В первом квартале 2024 года специалисты обнаружили серию атак, направленных на Россию и СНГ. Группа, стоящая за атаками, получила название **Lazy Koala**, а их стилер - LazyStealer. Основная задача этого стилера — кража логинов и паролей из Google Chrome и дальнейшая их пересылка Telegram-боту. Точный вектор заражения установить не удалось, однако по всем признакам это был фишинг. Общее количество скомпрометированных учетных записей на момент обнаружения составило 867, из них уникальных — 321.

APT Midge

В апреле специалисты сообщили об атаках группы, отслеживаемой ими как **APT Midge**. Согласно их данным, среди целей группы выявлены организации из России и Беларуси. Атаки начинаются с отправки сообщений с вложенными HTA-файлами. При открытии HTA начинается загрузка и выполнение VBA-скрипта, который, в свою очередь, взаимодействует с C2. Атакующие нацелены на сбор учетных данных, топографии сети и эксфильтрацию чувствительной информации.

Lazarus

В мае 2024 года специалисты обнаружили новый вариант бэкдора Manuscrypt группы **Lazarus** на ПК одного из клиентов в России. Для атак на пользователей по всему миру злоумышленники создали вредоносный сайт танковой DeFi-игры, в которой, якобы, можно получать награды в криптовалюте. Игра не была вредоносной сама по себе, однако сайт содержал скрытый скрипт, который позволял загрузить и выполнить эксплойт для Chrome. Эксплойт содержал код для двух уязвимостей: первая используется для чтения памяти процесса Chrome и записи в нее с помощью JavaScript (CVE-2024-4947), а вторая — для обхода песочницы V8. В течение нескольких месяцев злоумышленники расширяли свое присутствие в социальных сетях, регулярно публикуя посты в X с нескольких учетных записей; используя профессионально разработанные веб-сайты с дополнительным вредоносным ПО, премиум-аккаунты в LinkedIn и фишинговые рассылки; а также устанавливая контакт с инфлюэнсерами из мира криптовалют для рекламы. За основу злоумышленники взяли реальную игру. Хакеры практически полностью повторили ее дизайн: отличия заключались лишь в расположении логотипа и более низком качестве визуального оформления. Вскоре после того, как хакеры запустили кампанию по продвижению своей игры, разработчики исходной версии игры заявили, что из их кошелька похищено 20 000 долларов США в криптовалюте. И хотя разработчики обвинили в произошедшем инсайдера, исследователи полагают, что за атакой могла стоять группа Lazarus, и прежде чем украсть криптовалюту, хакеры похитили исходный код игры.

Unicorn

В сентябре 2024 раскрыта активность группы **Unicorn**, использующей одноименный бэкдор для кражи файлов из системы жертвы. В ходе исследования деятельности группы нашим специалистам удалось обнаружить дополнительную инфраструктуру и связанные файлы. В частности, Unicorn распространяла бэкдор под видом коммерческого предложения о продаже оборудования для СВО со скидкой, а также под видом предложения о безвозмездной передаче техники в фонд для нужд военнослужащих СВО. Группировка рассылает .RAR-архивы в виде почтовых вложений или файлов на Яндекс Диске, на которые ведет ссылка из письма. Внутри архива содержится файл с двойным расширением .pdf.lnk. Вредоносный ярлык содержит команду на запуск приложения mshta, которое скачивает и выполняет файл HTA. При запуске HTA выполняется вредоносный VBS-скрипт, который создаёт на диске два скрипта. В этих скриптах реализована основная функциональность: сбор файлов и их передача на сервер.

TaxOff

В третьем квартале 2024 года специалистами раскрыта серия атак на государственные структуры России. Группа, которой приписана кампания, получила название **TaxOff** из-за использования писем на правовые и финансовые темы в качестве приманок. Начальный вектор заражения — фишинговые письма со ссылкой на Яндекс. Диск, где размещены вредоносные файлы, связанные с «1С», или поддельный установщик, замаскированный под ПО «Справки БК» для заполнения данных о доходах и расходах госслужащих. Интересно, что под это же ПО ранее мимикрировала группа APT37 для распространения бэкдора KONNI. В своих атаках злоумышленники использовали самописный бэкдор Trinper — это C++ многопоточный бэкдор с гибкой конфигурацией. Он собирает системную информацию и запускает в разных потоках три класса: для коммуникации с C2; для мониторинга файловой системы; для перехвата нажатия клавиш.

NGC2140

NGC2140 — группировка, раскрытая в 2024 году, которая использует GoblinRAT и проводит атаки минимум с 2020 года. В результате её действий заражена инфраструктура по меньшей мере четырех российских организаций в ИТ и госсекторе. Операторов GoblinRAT интересует конфиденциальная информация, хранящаяся на серверах государственных органов и их подрядчиков (в том числе в сегментах сети с ограниченным доступом в Интернет).

NGC2180

В конце 2023 года исследователи обнаружили атаку на один из органов исполнительной власти России, в ходе которой использовалось многоступенчатое ВПО, запускавшее на финальной стадии имплант DFKRAT. Группе присвоено имя **NGC2180**. Первичный вектор заражения в случае ранних версий, по всей видимости — фишинговое письмо с загрузчиком во вложении, в последних версиях вектор остался неизвестным. Вредоносная активность запускается полезной нагрузкой, которая доставляется загрузчиками в более ранних версиях и дропперами, эксплуатирующими DLL side-loading — в последних. Ключевой функционал DFKRAT — эксфильтрация файлов, поддержка интерактивного шелла, потенциальная загрузка дополнительного ВПО с сервера управления C2. В качестве C2 для актуальной версии имплантов использовались скомпрометированные серверы центра исследований в Греции и индонезийской компании по оказанию финансовых услуг.

GoldenJackal

В 2024 году обнаружена атака группы **GoldenJackal**, реализованная в 2019 году против посольства одной из стран Южной Азии в Беларуси. Злоумышленники взломали изолированные системы с помощью набора инструментов: GoldenDealer — компонент для передачи вредоносных файлов на изолированные системы через USB-устройства; GoldenHowl — модульный бэкдор, предоставляющий различные возможности для удалённого управления; GoldenRobo — инструмент для сбора и эксфильтрации данных. Схема атаки включала заражение компьютеров с доступом в интернет. После подключения USB-устройства ВПО автоматически переносилось на изолированные системы. Когда это устройство возвращалось к машине с доступом в интернет, собранные данные отправлялись на сервер злоумышленников.

Actor240524

В июле специалисты выявили атаку, направленную на дипломатов Израиля и Азербайджана. Группа, стоящая за этой кампанией, получила название **Actor240524**, а используемые инструменты — ABCloader и ABCsync. Для реализации атак злоумышленники рассылают фишинговые письма с вредоносным вложением в виде файла .DOC с макросом.

MuddyWater

Во втором квартале 2024 года обнаружено более 50 фишинговых писем, направленных на более чем 10 секторов группой **MuddyWater**. Одной из целевых стран стал Азербайджан. Злоумышленники рассылали письма с вложением в виде файла .PDF, которые содержали ссылку на платформу для обмена файлами Egnyte. По ссылке загружается архив .ZIP, содержавший исполняемый файл, классифицируемый как бэкдор BugSleep, который поддерживает возможности закрепления в системе, reverse shell, загрузки/выгрузки файлов на C2 и др. Другие исследователи сообщают об обнаружении имплантов на основе VBS/DLL, которые использовались во вторжениях группой MuddyWater. Импланты обнаружены в нескольких правительственных и телекоммуникационных организациях в Казахстане, Египте, Кувейте, Марокко, Омане, Сирии и ОАЭ.

Earth Krahang

В 2024 году раскрыта кампания группы **Earth Krahang**, нацеленная преимущественно на правительственные учреждения по всему миру, с упором на страны Юго-Восточной Азии, а также на государства Европы, Америки и Африки. В числе атакованных — некоторые страны СНГ: скомпрометированы организации в Узбекистане и Кыргызстане, а организациям из Казахстана и Таджикистана атаки удалось отразить. Злоумышленники использовали фишинговые письма, сканирование серверов. После проникновения в сеть Earth Krahang использовала скомпрометированную инфраструктуру для размещения вредоносных загрузок, перенаправления трафика, а также взломанные почты для отправки фишинговых писем. Earth Krahang применяла Cobalt Strike и бэкдоры RESHELL и DinodasRAT. RESHELL — это простой .NET-бэкдор, обладающий базовыми возможностями сбора информации, удаления файлов и выполнения команд. С 2023 года группа перешла на бэкдор DinodasRAT, который предоставляет более широкие возможности и имеет версии под Windows и Linux. Также в средах жертв группы замечены PlugX и ShadowPad .

SugarGh0st Team

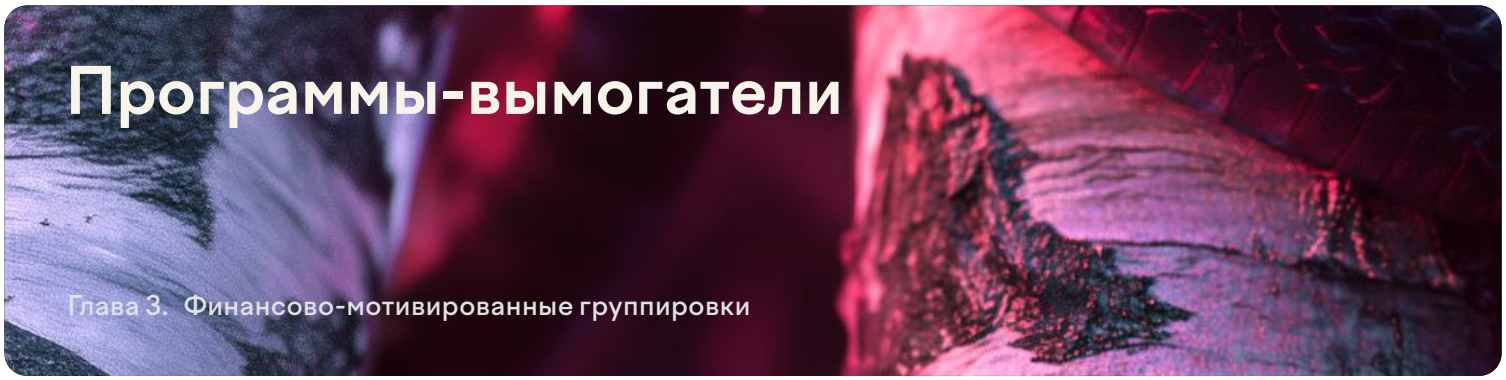
В феврале 2024 года наши специалисты фиксировали вредоносные файлы группы **SugarGh0st Team**, которые использовались в атаках против Узбекистана. Содержимое документа-приманки включает контактную информацию о свободной экономической зоне (СЭЗ) в регионе. Предположительно, атакующие могут быть нацелены на предпринимателей в производственных сферах, желающих реализовать проект в СЭЗ. Злоумышленники по-прежнему разворачивают в качестве финальной нагрузки SugarGh0st RAT.

UAC-0063

С июля 2024 года специалисты отслеживают кампанию группы **UAC-0063**, нацеленную на Азию и Европу. Обнаружено 62 жертвы в ряде стран, включая СНГ: Армению, Казахстан, Кыргызстан, Таджикистан, Узбекистан. Среди целей — организации по защите прав человека, компании по безопасности, правительственные и образовательные учреждения. Среди известных жертв — государственный департамент в Узбекистане; дочерняя компания казахского государственного нефтегазового предприятия; таджикское образовательное и научно-исследовательское учреждение. В ходе кампании группа разворачивает загрузчик HATVIBE и бэкдор CHERRYSPY. Первоначальный доступ, предположительно — через фишинговые письма с вложениями или эксплуатация уязвимости, такой как CVE-2024-23692.

Глава 3

Финансово-мотивированные группировки



Программы-вымогатели

В 2024 году, как и ранее, угроза со стороны шифровальщиков оставалась значительной, ведь практически ежедневно появляется информация о новых крупных инцидентах. Киберпреступные группы направляют усилия преимущественно на крупные компании с большой выручкой, что позволяет злоумышленникам требовать значительный выкуп за расшифровку данных. Все чаще происходят атаки на малый и средний бизнес. На протяжении 2024 года специалистам нашей компании зафиксировали **более 500 атак** с использованием программ-вымогателей в России.

В 2024 году в России и СНГ была отмечена низкая активность группировок HardBit и BlackShadow, атаковавших российских пользователей в предыдущие годы. Также не зафиксированы атаки со стороны группировки **Werewolves**. Зато продолжали действовать **Shadow** (под новым именем DarkStar), **HsHarada**, **DCHelp**, **RCRU64**, **GazpromLocker**. Отметим, что многие атаки шифровальщиков в России имеют явные связи с проукраинскими хактивистскими группировками.

Как и в предыдущие годы, злоумышленники не используют новые уникальные программы и обходятся шифровальщиками на основе Lockbit 3.0 Black (чаще всего), Conti, Babuk, а иногда шифруют данные легитимными инструментами (DiskCryptor, OpenSSL, WinRar). По-прежнему группировки не используют технику создания DLS-ресурсов: если злоумышленники хотят опубликовать доказательства совершенных атака, они делают это в Telegram/X-каналах. Выявлены факты публикации скомпрометированных данных в каналах известных хактивистских групп, что подтверждает связи между шифровальщиками и хактивистами.

2024 год отметился появлением ряда новых группировок, использующих для своих атак вредоносные программы-шифровальщики:

- **Masque,**
- **TeslaRVNG (Secles),**
- **ToxUnit,**
- **Sauron,**
- **Muliaka,**
- **Head Mare** (сама группа появилась в 2023 году, но атаки с использованием шифровальщиков замечены только в 2024-м).

Стоит отметить, что большинство программ-вымогателей, используемых атакующими в 2024 году, по-прежнему основаны на утекшем инструментарии программы-вымогателя **LockBit**, а также злоумышленники активно эксплуатируют легитимные утилиты удаленного доступа для первоначального проникновения в инфраструктуру жертвы.

Все больше хактивистских группировок стали прибегать к шифрованию данных жертвы. Так, например в июле 2024 года группировка **Cyber Anarchy Squad** заявила об атаке на крупную российскую IT-компанию, зашифровав часть ее инфраструктуры, в октябре она совершила совместную атаку с **Ukrainian Cyber Alliance**, использовав ВПО типа Wiper, а уже в ноябре зашифровала Linux-системы компании из сферы спорта. В это же время об атаке на крупную строительную компанию заявил злоумышленник **BadB** в своем Telegram-канале **CyberSec's**, для получения выкупа была зашифрована инфраструктура компании.

В 2024 году наиболее активными группировками, атаковавшими российские компании, стали:

- **Shadow** — 20 атак на крупные компании,
- **MorLock** — 15 атак,
- **Proton/Shinra** — более 25 атак,
- **Head Mare** — 20 атак (большая часть — на государственные компании),
- **Mimic** — более 110 атак на физических лиц и небольшие компании,
- **Enmity/Mammon** — более 25 атак,
- **BlackJack** — 10 атак на государственные компании,
- **DCHelp** — около 15 атак,
- **LokiLocker/BlackBit** — более 25 атак,
- **HsHarada** — более 10 атак.

В 2024 году после временного затишья вновь активизировались такие группировки, как **OldGremlin**, **Gazprom Locker**, **RCRU64**. В свою очередь, RaaS сервис **Phobos**, активный до сентября 2024 года, прекратил деятельность. Его разработчик был задержан и экстрадирован в США в ноябре. Этот арест не стал единичным случаем, так, например, в июле 2024 года по запросу Интерпола в Москве был задержан 37-летний Федор Андреев, более известный под псевдонимами «Azot» и «Angelo» и подозреваемый в связях с хакерской группировкой **TrickBot**. Чуть позднее, в августе, в США был задержан гражданин России Павел Кублицкий, по предварительной информации являвшийся модератором известного хакерского форума WWH-club. А уже в конце ноября стало известно о задержании в Калининграде Михаила Матвеева (более известного под псевдонимом Wazawaka), связанного с такими программами-вымогателями, как **LockBit**, **Hive** и **Babuk**.

Жертвами вымогателей чаще всего становились российские производственные, строительные, фармацевтические и ИТ-компании, предприятия добывающей промышленности, ВПК, организации из сферы услуг.

Все группировки, атаковавшие Россию в 2024 году, можно условно поделить на три группы:

1. **Проукраинские группировки** — в ходе исследования атак установлено, что такие группировки так или иначе связаны между собой, зачастую используют одинаковые инструменты, а порой совершают совместные атаки, в которых принимают участие сразу несколько групп. Основное отличие между ними — конфигурационные файлы программ-вымогателей и контакты для связи.
2. **Персидские группировки** — эти атакующие практически идентичны по тактикам, техникам и процедурам, а также используют похожие инструменты. Различаются только используемой программой-вымогателем. Вероятно, атакующие имеют отношение к странам, население которых говорит на персидском языке.
3. **Другие** — группировки не имеют между собой общих унифицирующих признаков, тем не менее, можно выделить тактики, техники и процедуры, наиболее часто используемые всеми группировками.

Shadow

Начало активности	Используемые инструменты	Цель	Основные техники (MITRE)	ID
Март 2023	• Lockbit 3 Black • Babuk • GodzillaWebshell • DarkGate • FaceFish • SystemBC • Cobint • Netscan • PingCastle • AnyDesk • Mimikatz • PowerSploit • CobaltStrike • Sysinternals • PsExec • ProcDump • Ngrok • Meterpreter	Шифрование данных и требование выкупа	Exploit Public-Facing Application	T1190
			Valid Accounts: Domain Accounts	T1078.002
			Command and Scripting Interpreter: PowerShell	T1059.001
			Command and Scripting Interpreter: Windows Command Shell	T1059.003
			Remote Services: Remote Desktop Protocol	T1021.001
			Data Encrypted for Impact	T1486

f6.ru

Группировка Shadow, которая в январе 2024 года сменила имя на DarkStar, атаковала российские компании на протяжении всего 2024 года. Запрашиваемый выкуп составил от 4,5 до 320 млн рублей (в криптовалюте BTC или XMR). Однако злоумышленники не ограничиваются лишь требованием выкупа: замечены случаи кражи криптовалюты из личных кошельков сотрудников атакованных компаний, а также похищение файлов типа session от Telegram-аккаунтов жертв. Тактики, техники и процедуры группировки остались прежними. Более подробно о группировке Shadow можно прочитать в исследовании компании — **«Тени не скроются. Расследование атак группировки Shadow»**.

Вероятна связь данного атакующего с хактивистскими группировками. Так, отмечено, что некоторые компании были зашифрованы группировкой Shadow, а скомпрометированные данные впоследствии опубликованы в источниках, связанных с группировкой Cybersec's. Кроме того, по информации исследователей, группировка Shadow совершала совместные атаки с Cyber Anarcy Squad (C.A.S). Вероятно, в рамках совместной работы участники групп делятся доступами к сетям жертв, инфраструктурой и инструментами.

MorLock

Начало активности	Используемые инструменты	Цель	Основные техники (MITRE)	ID
Январь 2024	• LockBit 3 Black • Babuk (ESXi, NAS) • Sliver • Facefish • Godzilla web-shell • SoftPerfect Network Scanner • PingCastle • resocks • pretender • AnyDesk • XenAllPasswordPro • nssm • PsExec • PetitPotato • Putty • Localtonet • chisel • Bulldog Backdoor (GoRed)	Шифрование данных и требование выкупа/ Шифрование и удаление данных	Valid Accounts: Domain Accounts	T1078.002
			Hide Artifacts	T1564
			Remote Services: Remote Desktop Protocol	T1021.001
			Data Encrypted for Impact	T1486

Появившись в начале января 2024 года, группировка MorLock начала вести активную вымогательскую деятельность, и уже в конце месяца на форуме BreachForums выставила на продажу базу данных охранной компании за 100 BTC. Данные компании были зашифрованы, для этого использовался LockBit 3 Black. Отличительные черты группировки — использование таких инструментов, как **Sliver**, имплант собственной разработки **BulldogBackdoor (GoRed)** и мессенджер Session для связи с жертвой. Также в некоторых атаках выявлены случаи использования майнера и Metasploit. Стоит отметить, что в некоторых атаках группировка использовала специальное ВПО типа Wiper для уничтожения зашифрованных данных. По имеющейся информации, в одной из майских атак злоумышленники запросили более 2 млн долларов в BTC.

Head Mare

Начало активности	Используемые инструменты	Цель	Основные техники (MITRE)	ID
Декабрь 2023	• LockBit 3 Black • Cobalt Strike • Meterpreter • Mimikatz • Sliver • Ngrok • Wiper • XenAllPasswordPro • PhantomDL • PhantomRAT	Шифрование и удаление данных/ Шифрование данных и требование выкупа	Valid Accounts	T1078
			Data Destruction	T1485
			Service Stop	T1489
			Defacement	T1491

f6.ru

Группировка Head Mare впервые заявила о себе в конце 2023 года. Изначально злоумышленники атаковали российские предприятия в сферах ВПК, ТЭК, IT, телекоммуникаций, машиностроения, организуя утечки внутренней документации и публикуя их в социальной сети X. Однако в третьем квартале 2024 года также обнаружены атаки на российские коммерческие предприятия без публикации внутренних документов и с требованиями выкупа за расшифровку. Атаки группировки приводили к простою компаний на протяжении нескольких суток.

Также злоумышленники проводили deface-атаки на сайты жертв. Большой всплеск активности пришелся на октябрь 2024 года, тогда в течение пяти дней злоумышленники атаковали пять компаний. Head Mare в основном применяет в атаках общедоступное программное обеспечение. Для первоначального доступа и эксплуатации злоумышленники начали использовать фишинговые письма, содержащие архивы с вредоносным ПО PhantomDL и PhantomRAT, а для связи с жертвами — аккаунты в мессенджере Telegram. Стоит отметить, что в арсенале злоумышленников также есть инструмент, получивший название Persey и позволяющий атакующим создавать задачи в планировщике Windows для запуска целевого файла.

BlackJack

Начало активности	Используемые инструменты	Цель	Основные техники (MITRE)	ID
2023	• LockBit 3 Black • Mimikatz • AnyDesk • Fuxnet • Radmin • CloudEyE • Shamoon	Шифрование и удаление данных/ компрометация данных	Valid Accounts	T1078
			Scheduled Task/Job	T1053
			Indicator Removal	T1070
			Data Destruction	T1485
			Service Stop	T1489
			Defacement	T1491

f6.ru

BlackJack — хактивистская группировка, предположительно аффилированная со Службой безопасности Украины, активная на протяжении всего 2024 года и нацеленная на компании, расположенные на территории России. Злоумышленники шифруют данные жертв с помощью программы-вымогателя, основанной на утекшем инструментарии LockBit 3 Black, и используют ВПО типа Wiper для удаления данных в системе жертвы, а также проводят deface-атаки на сайты жертв. У группировки есть Telegram-канал, в котором злоумышленники публикуют сообщения об успешных атаках, а также всевозможные данные из инфраструктуры жертв. По одной из версий, BlackJack не является самостоятельной группировкой, а представляет собой новостной агрегатор различных атакующих — в частности, Twelve и Mordor.

Детализированная таблица по техникам и процедурам, характерным для данной категории атакующих

f6.ru

Тактика	Техника	Описание
TA0001 Initial Access	**T1190** Exploit Public-Facing Application	Проукраинские группировки эксплуатируют уязвимости публично-доступных сервисов, таких как Atlassian Confluence, Zimbra, MS Exchange, JetBrains TeamCity
	T1078.002 Valid Accounts: Domain Accounts	Проукраинские группировки используют действительные учетные записи жертв, купленные на теневых рынках
	T1133 External Remote Service	Для доступа к периметру используют публично-доступные сервисы жертв, такие как VPN и RDP

Детализированная таблица по техникам и процедурам, характерным для данной категории атакующих

Тактика	Техника	Описание
TA0001 Initial Access	**T1199** Trusted Relationship	Для доступа к периметру используют публично-доступные сервисы жертв, такие как VPN и RDP
	T1566.001 Phishing: Spearphishing Attachment	Проукраинские группировки проводили фишинговые рассылки с вредоносными вложениями, которые загружали вирусную программу DarkGate
TA0002 Execution	**T1047** Windows Management Instrumentation	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
	T1204.002 User Execution: Malicious File	Атакующие используют методы социальной инженерии, чтобы вынудить пользователя запустить вредоносный файл из вложения фишингового сообщения
	T1106 Native API	В используемых атакующими программах используются функции Native API
	T1053.002 Scheduled Task/Job:	Для удалённого запуска проукраинские группировки используют модуль atexec фреймворка CrackMapExec
	T1053.005 Scheduled Task /Job: Scheduled Task	Для запуска программ и выполнения команд проукраинские группировки создают задания планировщика Windows
	T1059.001 Command and Scripting Interpreter: PowerShell	Для выполнения различных действий проукраинские группировки используют командный интерпретатор Windows (cmd.exe) и PowerShell на системах под управлением Windows, и оболочку bash на системах под управлением Unix-подобных ОС
	T1059.003 Command and Scripting Interpreter: Windows Command Shell	Для выполнения различных действий проукраинские группировки используют командный интерпретатор Windows (cmd.exe) и PowerShell на системах под управлением Windows, и оболочку bash на системах под управлением Unix-подобных ОС
	T1059.004 Command and Scripting Interpreter: Unix Shell	Для выполнения различных действий проукраинские группировки используют командный интерпретатор Windows (cmd.exe) и PowerShell на системах под управлением Windows, и оболочку bash на системах под управлением Unix-подобных ОС

Детализированная таблица по техникам и процедурам, характерным для данной категории атакующих

Тактика	Техника	Описание
TA0002 Execution	**T1569.002** System Services: Service Execution	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	**T1053.005** Scheduled Task/Job: Scheduled Task	Для сохранения доступа к внутреннему периметру жертв проукраинские группировки создают задания планировщика Windows для запуска утилиты ngrok
	T1078.002 Valid Accounts: Domain Accounts	Для сохранения доступа к внутреннему периметру жертв проукраинские группировки используют скомпрометированные легитимные доменные учетные записи
	T1133 External Remote Service	Для сохранения доступа к внутреннему периметру жертв проукраинские группировки используют RDP-, VPN- и почтовые сервисы
	T1136.001 Create Account: Local Account	Для сохранения доступа к внутреннему периметру жертв проукраинские группировки создают локальные и доменные учетные записи
	T1136.002 Create Account: Domain Account	Для сохранения доступа к внутреннему периметру жертв проукраинские группировки создают локальные и доменные учетные записи
	T1543.003 Create or Modify System Process: Windows Service	Для сохранения доступа к внутреннему периметру жертв проукраинские группировки инсталлируют программу удаленного доступа AnyDesk в качестве службы, а также создают службы для закрепления Cobint
	T1574.006 Hijack Execution Flow: Dynamic Linker Hijacking	В системах под управлением ОС Linux атакующие используют руткит Facefish, который загружается посредством LD_PRELOAD (/etc/ld.so.preload)
	T1505.003 Server Software Component: Web Shell	Для сохранения доступа к внутреннему периметру жертв проукраинские группировки используют веб-шелл Godzilla, размещаемый на публично-доступных веб-серверах
	T1547.001 Boot or Logon Autostart Execution: Registry Run Keys	Для сохранения доступа к внутреннему периметру жертв проукраинские группировки используют ключи автозапуска реестра для запуска бэкдоров

Детализированная таблица по техникам и процедурам, характерным для данной категории атакующих

Тактика	Техника	Описание
TA0004 Privilege Escalation	**T1068** Exploitation for Privilege Escalation	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
	T1053.005 Scheduled Task /Job: Scheduled Task	Для запуска некоторых загруженных инструментов и программы-вымогателя с привилегиями NT SYSTEM используются задания планировщика Windows
	T1543.003 Create or Modify System Process: Windows Service	Для повышения привилегий и выполнения команд с привилегиями NT SYSTEM проукраинские группировки создают службы одноразового выполнения
	T1078.002 Valid Accounts: Domain Accounts	Для повышения привилегий проукраинские группировки используют скомпрометированные легитимные доменные и локальные учетные записи с высоким уровнем привилегий
	T1078.003 Valid Accounts: Domain Accounts	Для повышения привилегий проукраинские группировки используют скомпрометированные легитимные доменные и локальные учетные записи с высоким уровнем привилегий
TA0005 Defense Evasion	**T1036.004** Masquerading: Masquerade Task or Service	Проукраинские группировки очищают журналы событий Windows
	T1036.005 Masquerading: Match Legitimate Name or Location	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.
	T1070.001 Indicator Removal: Clear Windows Event Logs	Проукраинские группировки очищают журналы событий Windows
	T1070.004 Indicator Removal on Host: File Deletion	Проукраинские группировки удаляют свои утилиты, скрипты, а также результаты их работы из каталогов `%PUBLIC%`, `%PUBLIC%\Temp`, `%PROGRAMDATA%`, `%USERPROFILE%\Desktop` и т.д.

Детализированная таблица по техникам и процедурам, характерным для данной категории атакующих

Тактика	Техника	Описание
TA0005 Defense Evasion	**T1078.002** Valid Accounts: Domain Accounts	Проукраинские группировки используют легитимные доменные учетные записи пользователей
	T1484.001 Domain Policy Modification: Group Policy Modification	Проукраинские группировки используют PowerShell-скрипт gpo.ps1 для внесения изменений в групповые политики с целью нейтрализации средств защиты
	T1112 Modify Registry	Созданная с помощью PowerShell-скрипта gpo.ps1 групповая политика модифицирует на системах в домене параметры системного реестра, связанные с WinRM, Windows Defender, Windows Firewall и др.
	T1550.002 Use Alternate Authentication Material: Pass the Hash	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
	T1562.001 Impair Defenses: Disable or Modify Tools	Проукраинские группировки отключают встроенные средства защиты, а также антивирусные средства сторонних разработчиков, изменяют их настройки, в том числе и списки исключений
	T1562.004 Impair Defenses: Disable or Modify System Firewall	Атакующие отключают брандмауэр Windows
	T1620 Reflective Code Loading	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	**T1555.002** Credentials from Password Stores: Credentials from Web Browsers	Проукраинские группировки используют утилиты `XenAllPasswordPro` и `ff_grab`, позволяющие извлекать пароли пользователей из множества программ, таких как: почтовые клиенты, браузеры, FTP-клиенты и другие
	T1555.004 Credentials from Password Stores: Windows Credential Manager	Проукраинские группировки используют утилиты XenAllPasswordPro и mimikatz для извлечения аутентификационных данных из диспетчера учетных данных Windows
	T1555.005 Credentials from Password Stores: Password Managers	Атакующие экспортируют данные, хранимые в парольных менеджерах KeePass, Passwork и др.

Детализированная таблица по техникам и процедурам, характерным для данной категории атакующих

Тактика	Техника	Описание
TA0006 Credential Access	**T1003.001** OS Credential Dumping: LSASS Memory	Проукраинские группировки используют утилиту ProcDump для получения дампа процесса lsass.exe и извлекают данные из lsass.exe программой mimikatz
	T1003.003 OS Credential Dumping: NTDS	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`
	T1003.006 OS Credential Dumping: DCSync	Проукраинские группировки проводят атаки DCSync при помощи mimikatz
	T1552.001 Unsecured Credentials: Credentials in Files	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
	T1552.001 Unsecured Credentials: Bash History	Проукраинские группировки ищут и извлекают аутентификационные данные из истории выполненных ко-манд оболочек Unix-подобных систем
TA0007 Discovery	**T1046** Network Service Discovery	Для разведки сетевой инфраструктуры жертвы атакующие используют сетевые сканеры Slitheris Net-work Discovery, PingCastle, fscan, NetScan
	T1087.001 Account Discovery: Local Account	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
	T1087.002 Account Discovery: Domain Account	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

Детализированная таблица по техникам и процедурам, характерным для данной категории атакующих

Тактика	Техника	Описание
TA0007 Discovery	**T1069.001** Permission Groups Discovery: Local Groups	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
	T1069.002 Permission Groups Discovery: Domain Groups	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
	T1482 Domain Trust Discovery	Для сбора и изучения сведений о доверительных отношениях между доменами проукраинские группировки используют утилиту Windows nltest.exe, а также скрипт ADRecon
	T1018 Remote System Discovery	Для получения информации об удаленных системах атакующие используют сетевые сканеры Slitheris Network Discovery, Advanced IP Scanner, fscan. Для сбора и изучения сведений о системах, инсталлированных программах и запущенных процессах атакующие используют скрипт PowerShell SA.ps1 и инструмент PowerView
	T1057 Process Discovery	Для получения информации об удаленных системах атакующие используют сетевые сканеры Slitheris Network Discovery, Advanced IP Scanner, fscan. Для сбора и изучения сведений о системах, инсталлированных программах и запущенных процессах атакующие используют скрипт PowerShell SA.ps1 и инструмент PowerView
	T1082 System Information Discovery	Для получения информации об удаленных системах атакующие используют сетевые сканеры Slitheris Network Discovery, Advanced IP Scanner, fscan. Для сбора и изучения сведений о системах, инсталли-рованных программах и запущенных процессах атакующие используют скрипт PowerShell SA.ps1 и инструмент PowerView
	T1518 Software Discovery	Для получения информации об удаленных системах атакующие используют сетевые сканеры Slitheris Network Discovery, Advanced IP Scanner, fscan. Для сбора и изучения сведений о системах, инсталлированных программах и запущенных процессах атаку-ющие используют скрипт PowerShell SA.ps1 и инструмент PowerView

Детализированная таблица по техникам и процедурам, характерным для данной категории атакующих

Тактика	Техника	Описание
TA0007 Discovery	**T1033** System Owner/User Discovery	Проукраинские группировки собирают и изучают сведения о владельцах систем, а также о вошедших пользователях на целевую систему. Проукраинские группировки собирают и изучают сведения о сетевых подключениях целевых систем, о наличии смежных подсетей, а также проверяют доступность целевых систем к сети Интернет
	T1016.001 System Network Configuration Discovery: Internet Connection Discovery	Проукраинские группировки собирают и изучают сведения о владельцах систем, а также о вошедших пользователях на целевую систему. Проукраинские группировки собирают и изучают сведения о сетевых подключениях целевых систем, о наличии смежных подсетей, а также проверяют доступность целевых систем к сети Интернет
	T1049 System Network Connections Discovery	Для сбора и изучения сведений о сетевых подключениях проукраинские группировки используют команду net use
	T1083 File and Directory Discovery	Проукраинские группировки изучают содержимое ка-талогов локальных, смонтированных сетевых дисков, а также различных каталогов удаленных систем, как правило, с помощью Проводника Windows, а также командами оболочек bash и cmd
	T1135 Network Share Discovery	Проукраинские группировки изучают содержимое каталогов локальных, смонтированных сетевых дисков, а также различных каталогов удаленных систем, как правило, с помощью Проводника Windows, а также командами оболочек bash и cmd
	T1654 Log Enumeration	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	**T1021.001** Remote Services: Remote Desktop Protocol	Атакующие используют RDP для продвижения по сети
	T1021.002 Remote Services: SMB/Windows Admin Shares	Для перемещений по SMB проукраинские группировки используют утилиты Sysinternals Psexec, Impacket SMBExec

Детализированная таблица по техникам и процедурам, характерным для данной категории атакующих

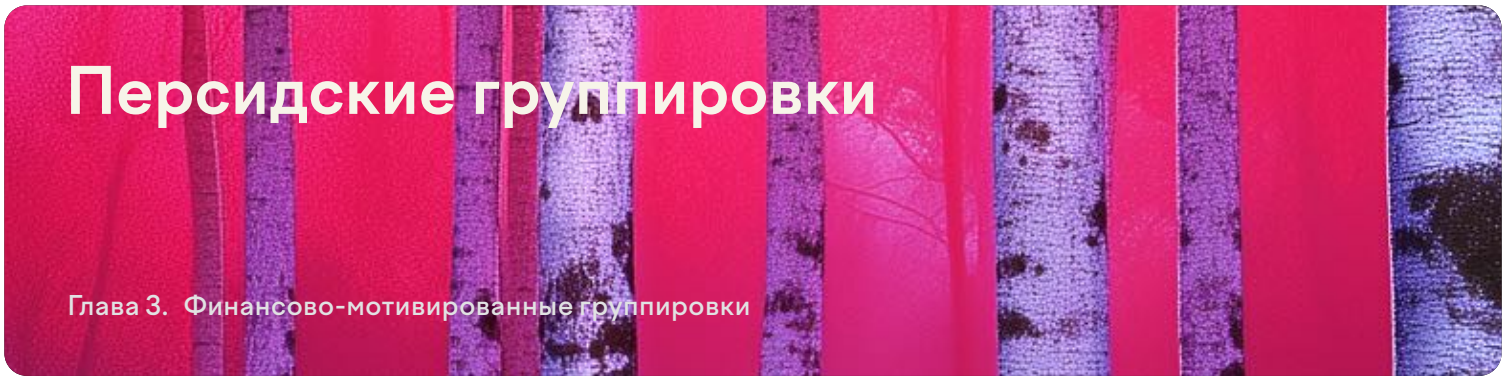
Тактика	Техника	Описание
TA0008 Lateral Movement	**T1021.004** Remote Services: SSH	Для перемещений с использованием SSH проукраинские группировки используют SSH-клиенты PuTTY и ssh
	T1021.006 Remote Services: Windows Remote Management	Для перемещений по протоколу WinRM атакующие используют командлет Enter-PSSession и Invoke-Comman
	T1210 Exploitation of Remote Services	Проукраинские группировки эксплуатируют уязвимости Zerologon (CVE-2020-1472) и EternalBlue (CVE-2017-0144) для перемещения на уязвимые системы
	T1550.002 Use Alternate Authentication Material: Pass the Hash	Проукраинские группировки перемещаются в инфраструктуре с использованием скомпрометированных NTLM-хешей паролей легитимных пользователей
	T1570 Lateral Tool Transfer	При перемещениях по узлам инфраструктуры проукраинские группировки копируют необходимый инструментарий в каталоги `%Public%`, `%Pub-lic%\Temp`, `%systemroot%\Logs`, `%ProgramData%` и реже `%userprofile%\Desktop`, `%userprofile%\Downloads`
TA0009 Collection	**T1005** Data from Local System	Проукраинские группировки ищут и собирают интересующие их данные с локальных и сетевых хранилищ, а также из баз данных
	T1039 Data from Network Shared Drive	Проукраинские группировки ищут и собирают интересующие их данные с локальных и сетевых хранилищ, а также из баз данных
	T1213 Data from Information Repositories	Проукраинские группировки ищут и собирают интересующие их данные, хранимые в различных инфор-мационных системах, таких как Confluence, wiki и т.п.
	T1560.001 Archive Collected Data: Archive via Utility	Для сжатия собранных конфиденциальных данных проукраинские группировки используют как встроенные архиваторы Windows, так и имеющиеся на систе-мах сторонние
	? (новая техника) 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

Детализированная таблица по техникам и процедурам, характерным для данной категории атакующих

Тактика	Техника	Описание
TA0011 Command And Control	**T1071.001** Application Layer Protocol: Web Protocols	Применяемый атакующими фреймворк пост-эксплуатации Cobint использует для взаимодей-ствия с C2 про-токолы HTTP, HTTPS
	T1132.001 Data Encoding:	Фреймворк постэксплуатации Cobint использует кодирование Base64
	T1132.002 Data Encoding: Non-Standard Encoding	ВПО DarkGate использует Base64 с нестан-дартной таблицей символов
	T1573 Encrypted Channel	Проукраинские группировки используют для удаленного доступа к скомпрометированным системам Cobint, Facefish, AnyDesk, которые осуществляют асимметричное/симметричное шифрование канала связи с C2
	T1105 Ingress Tool Transfer	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`, `%Sys-temroot%` и `%Systemroot%\System32`
	T1219 Remote Access Software	Для удаленного доступа к скомпрометированной инфраструктуре проукраинские группировки используют программу удаленного доступа (RAT) AnyDesk
	T1572 Protocol Tunneling	Для доступа к скомпрометированной системе атакующие используют туннели, построенные с использованием ngrok и revsocks
	T1090 Proxy	Для доступа к скомпрометированной системе атакующие используют туннели, построенные с использованием ngrok и revsocks
TA0010 Exfiltration	**T1567.002** Exfiltration Over Web Service: Exfiltration to Cloud Storage	Атакующие загружают похищенные данные на облачные хранилища данных (Mega[.]io, gofile[.]io, drop-mefiles[.]net и др.). В зависимости от объема данных злоумышлен-ники осуществляют эксфильтрацию с помощью веб-браузеров либо программы Rclone
	T1041 Exfiltration Over C2 Channel	Некоторые похищенные данные направлялись по каналам взаимодействия с управляющим сервером Co-bint. Эксфильтрацию информации малого объема проукраинские группировки проводят через буфер обмена во время активных RDP-сессий

Детализированная таблица по техникам и процедурам, характерным для данной категории атакующих

Тактика	Техника	Описание
TA0010 Exfiltration	**T1048.002** Exfiltration Over Al-ternative Protocol: Exfiltration Over Asymmetric Non-C2 Protocol	Эксфильтрация больших объемов информации проводится проукраинскими группировками с помощью утилиты Rclone. Данные передаются по протоколу SFTP на подконтрольные атакующим ресурсы
TA0040 Impact	**T1490** Inhibit System Recovery	Атакующие осуществляли удаление теневых копий томов, отключали возможности восстановления систем Windows, а также удаляли резервные копии систем
	T1531 Account Access Removal	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
	T1529 System Shut-down/Reboot	Атакующие могут отключать системы администраторов скриптами PowerShell
	T1485 Data Destruction	Атакующие создают задачи на удаление бэкапов при помощи систем управления резервного копирования. В некоторых атаках Twelve для уничтожения данных использовалась программа-вайпер Endurance-Wiper
	T1561.001 Disk Wipe: Disk Content Wipe	Проукраинские группировки используют утилиту BOOTICE для очистки содержимого дискового пространства методом принудительной перезаписи случайными данными хранилищ резервных копий
	T1491.001 Defacement: Internal Defacement	В некоторых атаках атакующие меняют обои рабочего стола хостов и выводят текст с требованием выкупа на принтеры
	T1486 Data Encrypted for Impact	Для шифрования данных в Windows-системах злоумышленники используют программу-вымогатель LockBit 3 Black, для шифрования данных в Linux-системах — программу-вымогатель Babuk



Персидские группировки

LokiLocker/BlackBit

Начало активности	Используемые инструменты	Цель	Основные техники (MITRE)	ID
Август 2021	• BlackBit • AccountCrack • Mimikatz • NirSoft • Advanced Port Scanner Process Hacker 2 • Revo Uninstaller	Шифрование данных и требование выкупа	Scheduled Task/Job: Scheduled Task	T1053.005
			Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1547.001
			Remote Services: Remote Desktop Protocol	T1021.001
			Data Encrypted for Impact	T1486

f6.ru

LokiLocker/BlackBit — группа шифровальщиков, которая обнаружена в августе 2021 года. LokiLocker/BlackBit шифрует данные с помощью AES-256 в режиме GCM (счётчик с аутентификацией Галуа), а ключ затем шифруется с помощью открытого RSA ключа жертвы. Стоит отметить, что к концу 2024 года замечен небольшой спад активности группировки. Вполне вероятно, что это связано с появлением конкурента в виде Proton и его вариаций. Контакты злоумышленников, тактики и техники остались прежними.

Proton/Shinra

Начало активности	Используемые инструменты	Цель	Основные техники (MITRE)	ID
Март 2023	• Proton • Mimikatz • Process Hacker • Sysinternals	Шифрование данных и требование выкупа	Data Encrypted for Impact	T1486

f6.ru

Proton — написанный на C++ аналог шифровальщика LockiLocker/Blackbit. Аналогично LokiLocker/BlackBit, при запуске Proton проверяет наличие установленной раскладки клавиатуры fa-IR (персидская клавиатура). Судя по всему, Proton практически полностью заменил Lokilocker/Blackbit. Атаки данного шифровальщика наблюдались на протяжении всего 2024 года, преимущественно жертвами стали компании малого бизнеса. В феврале 2024 года обнаружен новый образец программы-вымогателя Zenex, изучив который наши эксперты пришли к выводу, что это разновидность Proton. В начале апреля также обнаружена программа-вымогатель Shinra, которая является другой ветвью развития Proton. Стоит отметить, что обе ветви (Proton и Shinra) активны на конец 2024 года и используются параллельно.

Mimic Ransom

Начало активности	Используемые инструменты	Цель	Основные техники (MITRE)	ID
Июнь 2022	Mimic	Шифрование данных и требование выкупа	Exploit Public-Facing Application	T1190
			User Execution: Malicious File	T1204.002
			Data from Local System	T1005
			Data Encrypted for Impact	T1486

Mimic — программа-вымогатель, появившаяся в июне 2022 года. В третьем квартале 2024 года злоумышленники поменяли используемые контакты (ICQ/Skype) на более актуальные и привычные пользователям (Email/Telegram), а также отошли от использования набора креативных расширений («.PANIN», «.PODSTAVLIAIPOPKU», «.ANI_LOARAK», «.PHILIP_KIRKOROV»). Самым частым используемым расширением стало «.elpaco-team». С большой долей вероятности Mimic используют для атак несколько групп.

Все атакованные Mimic цели по-прежнему — либо физические лица, либо небольшие коммерческие организации. Стоит также отметить, что в четвертом квартале 2024 года замечены атаки Mimic, в которых злоумышленники использовали мессенджеры Tox и Session для связи с жертвами. В июле была совершена атака Mimic Ransomware (Elpaco-team) на российского пользователя. В результате анализа записки, оставленной злоумышленниками, эксперты нашей компании выявили полное ее сходство с записками Phobos RaaS. Это может свидетельствовать о том, что атакующие состоят сразу в нескольких партнерских сервисах. **Средняя сумма выкупов злоумышленников, как правило, составляет до 100 тысяч рублей за один хост и до 300 тысяч рублей за сервер**.

Enmity/Mammon

Начало активности	Используемые инструменты	Цель	Основные техники (MITRE)	ID
Апрель 2023	Enmity	Шифрование данных и требование выкупа	External Remote Services	T1133
			Remote Services: Remote Desktop Protocol	T1021.001
			Data Encrypted for Impact	T1486

f6.ru

Enmity — это программа-вымогатель, впервые обнаруженная в апреле 2023 года и активная на протяжении всего 2024 года. В середине августа 2024 года экспертами нашей компании была обнаружена атака шифровальщика Mammon на российскую компанию. После анализа было установлено, что данная программа-вымогатель является новой версией Enmity. По имеющимся данным, злоумышленники запрашивают от 3000 до 10 000 долларов США за расшифровку одного сервера и от 20 000 долларов США до 2 BTC за расшифровку всех компьютеров внутри компании. Одним из векторов первоначального доступа злоумышленников является подключение через RDP.

HsHarada

Начало активности	Используемые инструменты	Цель	Основные техники (MITRE)	ID
Декабрь 2022	• HsHarada • CobaltStrike • Godzilla Webshell • Meterpreter	Шифрование данных и требование выкупа	Active Scanning: Vulnerability Scanning	T1595.002
			Exploit Public-Facing Application	T1190
			Command and Scripting Interpreter: PowerShell	T1059.001
			Data Encrypted for Impact	T1486

f6.ru

HsHarada/Rapture — это семейство программ-вымогателей, впервые обнаруженное 31 декабря 2022 года. 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. На протяжении 2024 года HsHarada проявляла умеренную активность по отношению к жертвам в России.

RCRU64

Начало активности	Используемые инструменты	Цель	Основные техники (MITRE)	ID
2021	RCRU64	Шифрование данных и требование выкупа	Command and Scripting Interpreter: Windows Command Shell	T1059.003
			Scheduled Task/Job: Scheduled Task	T1053.005
			Indicator Removal: File Deletion	T1070.004
			Data Encrypted for Impact	T1486

RCRU64 — это программа-вымогатель, первая активность которой пришлась на конец марта и начало апреля 2021 года. Для шифрования используются алгоритмы AES и RSA. После отсутствия атак на российские компании с февраля 2024 года в середине августа был обнаружен сэмпл, который представляет собой шифровальщик RCRU64. Судя по всему, жертвой стал пользователь из Индии, а уже в конце ноября были замечены атаки на российских пользователей.

Sauron

Начало активности	Используемые инструменты	Цель	Основные техники (MITRE)	ID
Октябрь 2024	Sauron	Шифрование данных и требование выкупа	Inhibit System Recovery	T1490
			Data Encrypted for Impact	T1486

Sauron — программа-вымогатель, впервые обнаруженная в октябре 2024 года, разработанная на основе исходного кода Conti 3 и имеющая схожие концептуальные черты с семейством Proxima. Вредоносная программа шифрует файлы и добавляет к их именам уникальный идентификатор, присваиваемый жертве, адрес электронной почты киберпреступников и расширение «.Sauron». Как только процесс шифрования завершен, Sauron меняет обои на рабочем столе и отправляет сообщение с требованием выкупа. Стоит отметить, что первые атаки с использованием данной программы-вымогателя на российских пользователей были обнаружены в октябре 2024 года.

Детализированная таблица по техникам и процедурам, характерным для данной категории атакующих

f6.ru

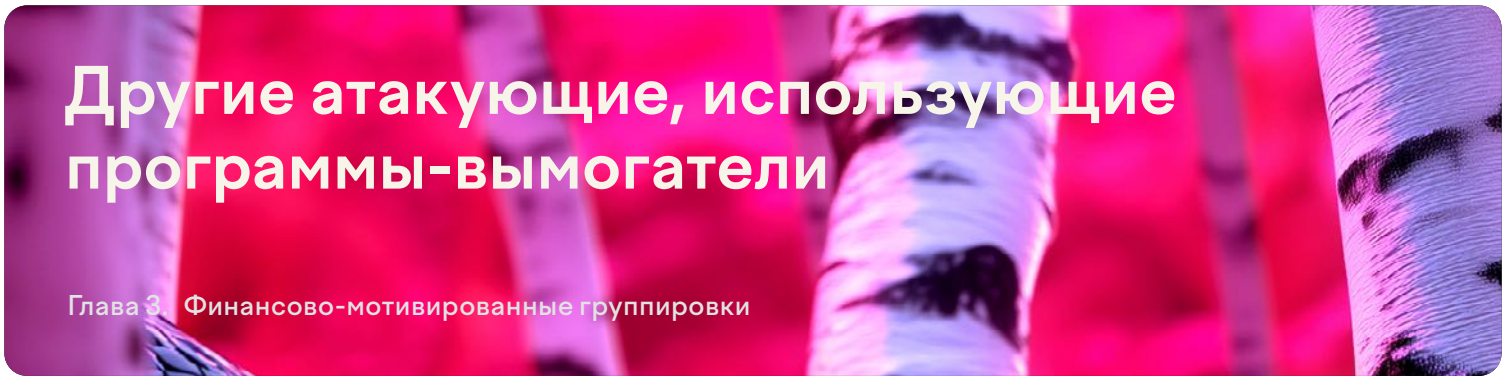
Тактика	Техника	Описание
TA0001 Initial Access	**T1133** External Remote Services	В качестве первоначального доступа атакующие преимущественно используют публично доступный RDP
	T1078 Valid Accounts	Злоумышленники использовали для получения доступа скомпрометированные учетные данные
TA0002 Execution	**T1059.003** Command and Scripting Interpreter: Windows Command Shell	Атакующие используют Windows Command Shell для выполнения различных действий
TA0003 Persistence	**T1078** Valid Accounts	Полученные атакующими легитимные учетные записи используются для закрепления в скомпрометированной инфраструктуре
	T1136 Create Account	Некоторые партнеры для закрепления в системе создавали привилегированные учетные записи
TA0004 Privilege Escalation	**T1078** Valid Accounts	Атакующими для повышения привилегий используются легитимные учетные данные с правами администратора. Существующие учетные данные администратора домена использовались злоумышленниками для продвижения по сети
TA0005 Defense Evasion	**T1562.001** Impair Defenses: Disable or Modify Tools	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)

Детализированная таблица по техникам и процедурам, характерным для данной категории атакующих

Тактика	Техника	Описание
TA0005 Defense Evasion	**T1070.001** Indicator Removal on Host: Clear Windows Event Logs	Атакующие очищают журналы событий Windows (Event Logs) на скомпрометированном хосте
	T1070.004 Indicator Removal: File Deletion	Атакующие удаляют после использования свои ранее загруженные на хост инструменты
TA0006 Credential Access	**T1003** OS Credential Dumping	Для получения привилегированных учетных данных атакующие используют популярную легитимную утилиту mimikatz
	T1552 Unsecured Credentials	Некоторые партнеры использовали для извлечения паролей утилиты NirSoft RouterPassView, PstPassword, VNCPassView. Также некоторые атакующие использовали утилиту Everything для поиска аутентификационных данных в текстовых файлах
	T1555.003 Credentials from Password Stores: Credentials from Web Browsers	Некоторые партнеры использовали для извлечения паролей утилиты NirSoft OperaPassView, WebBrowserPassView
	T1555.003 Credentials from Password Stores: Windows Credential Manager	Некоторые партнеры использовали для извлечения паролей утилиту NirSoft CredentialsFileView
	T1110 Brute Force	Злоумышленники используют подбор паролей для получения доступа
TA0007 Discovery	**T1018** Remote System Discovery	Для получения информации об удаленных системах атакующие используют сетевые сканеры Advanced Port Scanner, SoftPerfect Network Scanner
	T1046 Network Service Scanning	Для сканирования открытых портов в сети атакующие используют сетевые сканеры Advanced Port Scanner, SoftPerfect Network Scanner
	T1087 Account Discovery	Для получения списка пользователей в Active Directory некоторые партнеры пользовались утилитой LoginParser
	T1135 Network Share Discovery	Атакующие используют различные версии консольной утилиты NS для сканирования общих ресурсов сети

Детализированная таблица по техникам и процедурам, характерным для данной категории атакующих

Тактика	Техника	Описание
TA0007 Discovery	**T1083** File and Directory Discovery	Для получения информации о файлах и каталогах некоторые партнеры использовали утилиту Everything
TA0008 Lateral Movement	**T1021.001** Remote Services: Remote Desktop Protocol	Атакующие использовали RDP для дальнейшего продвижения по сети
	T1570 Lateral Tool Transfer	При продвижении внутри сети жертвы и развертывании программы-вымогателя атакующие осуществляют копирование на хост необходимого набора инструментов
TA0011 Command and Control	**T1105** Ingress Tool Transfer	После получения первоначального доступа атакующие копируют на скомпрометированный хост набор необходимых инструментов
TA0040 Impact	**T1485** Data Destruction	Атакующие с помощью программы-вымогателя после истечения 30-дневного срока выплаты выкупа могут уничтожить все данные на скомпрометированных хостах
	T1486 Data Encrypted for Impact	Атакующие используют программы-вымогатели для шифрования файлов на скомпрометированных хостах с целью получения выкупа



Другие атакующие, использующие программы-вымогатели

Masque

Начало активности	Используемые инструменты	Цель	Основные техники (MITRE)	ID
Январь 2024	• LockBit 3 Black • Babuk • AnyDesk • Mimikatz • ProcDump • PsExec • SMBexec • Chisel • MystiqueLoader • XenAllPasswordPro	Шифрование данных и требование выкупа	Valid Accounts	T1078
			Remote Services: SMB/ Windows Admin Shares	T1021.002
			Data Encrypted for Impact	T1486

Masque — группировка, использующая для атак программу-вымогатель LockBit 3 Black, появившаяся в январе 2024 года. Записка с требованием выкупа составлена только на русском языке, что говорит о том, что группировка нацелена исключительно на российские компании. В самой записке нет никаких деталей, кроме контактов злоумышленников в мессенджере qTox. В большинстве случаев начальным вектором атаки Masque является компрометация публично доступных сервисов, таких как VMware Horizon, через эксплуатацию уязвимости CVE-2021-44228 (log4shell) в библиотеке log4j, несмотря на то, что с момента её обнаружения прошло значительное время. В одной из атак для продвижения внутри инфраструктуры жертвы использовались скомпрометированные учетные данные в режиме самораспространения PsExec. По имеющейся информации, в одной из атак осенью 2024 года запрошенная **сумма выкупа составила 75 000$**. Также стоит отметить, что группировка использовала собственный лоадер MystiqueLoader, по команде с управляющего сервера (C2) он может производить загрузку из сети интернет программного модуля PE и его запуск непосредственно в памяти текущего процесса. Агент осуществляет взаимодействие с C2 с помощью протокола DNS.

Muliaka

Начало активности	Используемые инструменты	Цель	Основные техники (MITRE)	ID
Январь 2024	• Conti 3 • WinRM	Шифрование данных и требование выкупа	Valid Accounts	T1078
			Command and Scripting Interpreter: PowerShell	T1059.001
			Remote Services: Windows Remote Management	T1021.006
			Data Encrypted for Impact	T1486

f6.ru

Злоумышленник использует шифровальщик — модификацию Conti 3 (под Windows) и под ESXi предположительно самописную на языке Rust вредоносную программу-шифровальщик. Злоумышленник, получивший название Muliaka, атаковал российские компании минимум с декабря 2023 года.

Период с момента получения доступа к ИТ-инфраструктуре жертвы до начала шифрования данных составляет примерно 2 недели. В ходе исследования активности группы специалисты нашей компании выяснили, что для удаленного доступа к ИТ-инфраструктуре жертвы атакующие использовали VPN-сервис компании, а для перемещения по узлам инфраструктуры — службу удаленного управления WinRM (Windows Remote Management).

Для распространения программы-вымогателя в сети жертвы и её запуска на хостах Windows злоумышленники использовали установленное корпоративное антивирусное программное обеспечение. Для удаленного запуска шифровальщика злоумышленники создали инсталляционный пакет и соответствующую задачу. Отметим, что при наличии установленного антивируса в ИТ-инфраструктуре жертвы продвинутые атакующие все чаще предпочитают использовать этот продукт для скрытного и эффективного продвижения по сети.

После первого квартала 2024 года активности со стороны данной группировки выявлено не было.

OldGremlin

Начало активности	Используемые инструменты	Цель	Основные техники (MITRE)	ID
2020	• TinyFluff • TinyCrypt • TinyIsolator • TinyLink • TinyNode • TinyHTA • OldGremlin. JsDownloader	Шифрование данных и требование выкупа	Phising: Spearphishing Link	T1566.002
			Command and Scripting Interpreter: JavaScript	T1021.002
			Obfuscated Files or Information	T1027

OldGremlin — это русскоязычная хакерская группировка, впервые обнаруженная в марте 2020 года и атакующая исключительно российские компании. Всего за свой первый период активности (с марта 2020 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 рублей за восстановление доступа к данным, а в 2022 году ценник поднялся до 1 млрд рублей. После отсутствия активности с сентября 2022 по август 2024 года нашими экспертами были обнаружены фишинговые электронные письма, при анализе которых были обнаружены индикаторы, указывающие на то, что данные письма являлись частью рассылки OldGremlin. Внутри писем также был обнаружен JavaScript-сценарий, классифицированный как загрузчик и названный OldGremlin.JsDownloader, в задачи которого входит загрузка и выполнение произвольных JavaScript-сценариев.

DCHelp

Начало активности	Используемые инструменты	Цель	Основные техники (MITRE)	ID
2021	• DiskCryptor • Mimikatz • Account Restore • MeshAgent • Advanced Port Scanner	Шифрование данных и требование выкупа	Valid Accounts	T1078
			External Remote Services	T1133
			System Information Discovery	T1082
			Remote Services: Remote Desktop Protocol	T1021.001
			Data Encrypted for Impact	T1486

Атакующий, получивший название DCHelp, использует для шифрования легитимную программу DiskCryptor и совершает атаки исключительно на российские коммерческие компании. DCHelp первые был обнаружен в январе 2023 года. Предположительно, DCHelp не является группировкой, вероятнее всего, за атаками стоит один человек, прибегающий к сотрудничеству с другими злоумышленниками. Для первоначального доступа в сеть жертвы атакующий использует RDP-доступ в доменные сети, предоставленный, как правило, аффилированным лицом (партнером). Сумма выкупа при атаке формируется из следующих факторов: оборот клиента, количество серверов рабочих станций, важность информации, сумма приблизительных потерь компании при восстановлении с нуля. По полученным данным, **максимальная сумма выкупа, полученная организатором DCHelp, составила 248 000 долларов** (хотя ранее считалось, что данная сумма не превышает 15 000 долларов). Также стоит отметить, что DCHelp отошел от привычного использования DLS для публикации данных жертвы, вместо этого сайт стал больше походить на интернет-магазин, на нем публикуются названия компаний с суммами выкупа за расшифровку, а спустя время данные удаляются.

GazpromLocker

Начало активности	Используемые инструменты	Цель	Основные техники (MITRE)	ID
Март 2023	• Conti • Cobalt Strike • AnyDesk	Шифрование данных и требование выкупа	Exploit Public-Facing Application	T1190
			File and Directory Discovery	T1083
			Remote Services	T1021
			Data Encrypted for Impact	T1486

f6.ru

GazpromLocker — это программа-вымогатель, основанная на коде шифровальщика Conti. Впервые была замечена в середине марта 2023 года. Она добавляет расширение «.GAZPROM» в конце имени зашифрованного файла. Почти год, начиная с июля 2023 года, группировка не проявляла никакой активности. Однако, по имеющимся данным, в июне 2024 года произошло минимум две атаки с использованием данного ВПО, контакты злоумышленников при этом остались прежними.

TeslaRVNG (Secles)

Начало активности	Используемые инструменты	Цель	Основные техники (MITRE)	ID
Декабрь 2023	• TeslaRVNG • Mimikatz • NLBrute • NirSoft • SDelete • Advanced Port Scanner • SoftPerfect Network Scanner	Шифрование данных и требование выкупа	Remote Services: Remote Desktop Protocol	T1021.001
			Data Encrypted for Impact	T1486

f6.ru

Secles — это 4-я версия программы-вымогателя TeslaRVNG, впервые обнаруженная в декабре 2023 года. После шифрования данных злоумышленники требуют выкуп. Преимущественно атакует физических лиц, однако зафиксированы были замечены единичные случаи атак на российские компании. При атаке на компании злоумышленники требуют выкуп в размере 5000–10 000 долларов. Программа-вымогатель шифрует файлы и изменяет их названия, добавляя к ним уникальный идентификатор, присвоенный жертве, имя пользователя Telegram-бота злоумышленников и расширение — «.secles»/«.secles2».

ToxUnit

Начало активности	Используемые инструменты	Цель	Основные техники (MITRE)	ID
Сентябрь 2024	• LockBit 3 Black • Babuk	Шифрование данных и требование выкупа	Valid Accounts	T1078
			Group Policy Discovery	T1615
			Data Destruction	T1485
			Data Encrypted for Impact	T1486

f6.ru

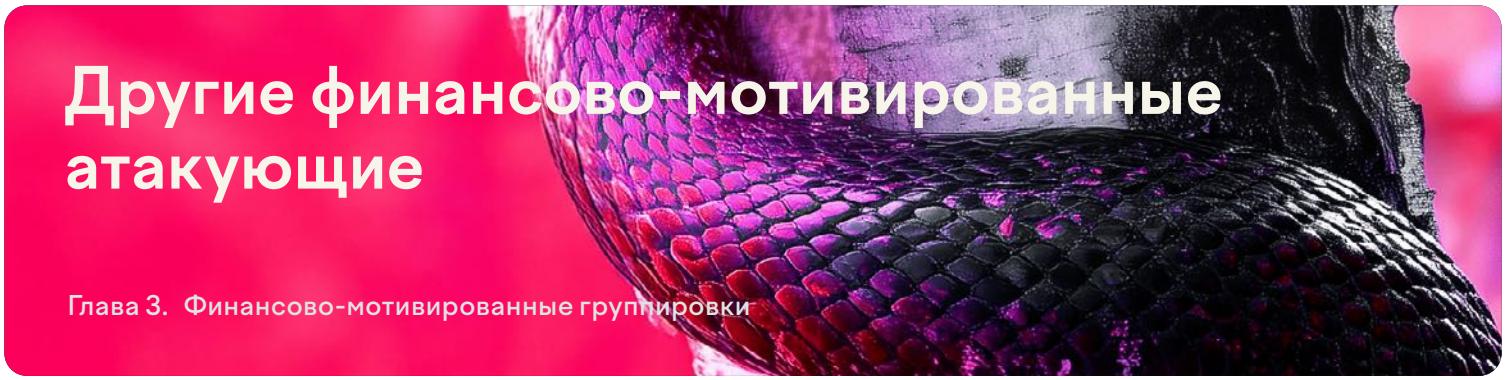
ToxUnit — группировка, использующая для своих атак шифровальщик, основанный на утекших билдерах LockBit 3 Black и Babuk (для Windows), впервые обнаруженная в сентябре 2024 года. Группа, вероятно, не ограничивается географическим расположением своих жертв. Файлы с контактами для связи и выкупа — полностью на английском языке, группировка ориентирована на жертв в разных странах. На конец года было обнаружено две атаки на компании из России.

Детализированная таблица по техникам и процедурам, характерным для данной категории атакующих

Тактика	Техника	Описание
TA0001 Initial Access	**T1133** External Remote Services	В качестве первоначального доступа атакующие преимущественно используют публично доступный RDP
	T1078 Valid Accounts	Злоумышленники использовали для получения доступа скомпрометированные учетные данные
TA0002 Execution	**T1059.003** Command and Scripting Interpreter: Windows Command Shell	Атакующие используют Windows Command Shell для выполнения различных действий
	T1569.002 System Services: Service Execution	Злоумышленники могут воспользоваться диспетчером управления службами Windows (SCM) для выполнения вредоносных команд или полезных нагрузок. Также используются утилиты PsExec, SBMexec, SDelete
	T1053.005 Scheduled Task/Job: Scheduled Task	Атакующие создают задание в планировщике
TA0003 Persistence	**T1136** Create Account	Некоторые злоумышленники для закрепления в системе создавали привилегированные учетные записи
TA0004 Privilege Escalation	**T1078** Valid Accounts	Атакующими для повышения привилегий используются легитимные учетные данные с правами администратора
TA0005 Defense Evasion	**T1562.004** Impair Defenses: Disable or Modify System Fire-wall	Атакующие отключают либо добавляют новые правила для антивирусных решений на хостах
	T1070.001 Indicator Removal on Host: Clear Windows Event Logs	Атакующие очищают журналы событий Windows (Event Logs) на скомпрометированном хосте
	T1070.004 Indicator Removal: File Deletion	Атакующие удаляют после использования свои ранее загруженные на хост инструменты
TA0006 Credential Access	**T1003** OS Credential Dumping	Для получения привилегированных учетных данных атакующие используют популярную легитимную утилиту mimikatz
	T1552 Unsecured Credentials	Злоумышленники используют утилиту xenallpasswordspro для извлечения паролей из различных программ и приложений.

Детализированная таблица по техникам и процедурам, характерным для данной категории атакующих

Тактика	Техника	Описание
TA0006 Credential Access	**T1110** Brute Force	Некоторые злоумышленники используют подбор паролей для получения доступа
TA0007 Discovery	**T1018** Remote System Discovery	Для получения информации об удаленных системах атакующие используют сетевые сканеры Advanced Port Scanner, SoftPerfect Network Scanner
	T1046 Network Service Scanning	Для сканирования открытых портов в сети атакующие используют сетевые сканеры Advanced Port Scanner, SoftPerfect Network Scanner
	T1083 File and Directory Discovery	Атакующие изучают пользовательские каталоги на разных хостах
TA0008 Lateral Movement	**T1021.001** Remote Services: Remote Desktop Protocol	Атакующие используют RDP для перемещения внутри инфраструктуры
	T1570 Lateral Tool Transfer	При продвижении внутри сети жертвы и развертывании программы-вымогателя атакующие осуществляют копирование на хост необходимого набора инструментов
TA0011 Command and Control	**T1105** Ingress Tool Transfer	После получения первоначального доступа атакующие копируют на скомпрометированный хост набор необходимых инструментов
TA0040 Impact	**T1486** Data Encrypted for Impact	Атакующие используют программы-вымогатели для шифрования файлов на скомпрометированных хостах с целью получения выкупа



Другие финансово-мотивированные атакующие

Buhtrap

Buhtrap — вредоносное ПО и одноименная финансово-мотивированная киберпреступная русскоговорящая группа, действующая с октября 2014 года. Первые атаки на финансовые учреждения были зафиксированы в августе 2015 года, до этого группа атаковала только клиентов банков. Фокус атак группы приходится на банки России и Украины. Основным вектором проникновения в корпоративные сети были фишинговые письма от имени Банка России или его представителей, часть атак проводилась с помощью наборов эксплойтов и дистрибутивов легального программного обеспечения.

В 2016 году исходные коды Buhtrap были опубликованы в открытом доступе, что привело к увеличению количества атак через систему клиент-банк уже различными атакующими.

Ущерб от атак с использованием ВПО Buhtrap в 2020–2022 годах оценивается как минимум в 2 млрд рублей.

В 2023 году фиксировалось появление ресурсов, замаскированных под сайты бухгалтерской тематики, на которых жертва могла скачать вредоносные файлы, полезной нагрузкой которых являлся загрузчик ВПО Buhtrap, при этом наблюдалась высокая степень сходства с обнаруженными ранее образцами 2018-2020 годов. Атаки в 2023 году не были массовыми.

В сентябре 2024 года специалисты Центра кибербезопасности обнаружили новую кампанию по доставке ВПО Buhtrap. Злоумышленники использовали подход с продвижением своих приманок в поисковой выдаче с помощью рекламы Яндекса.

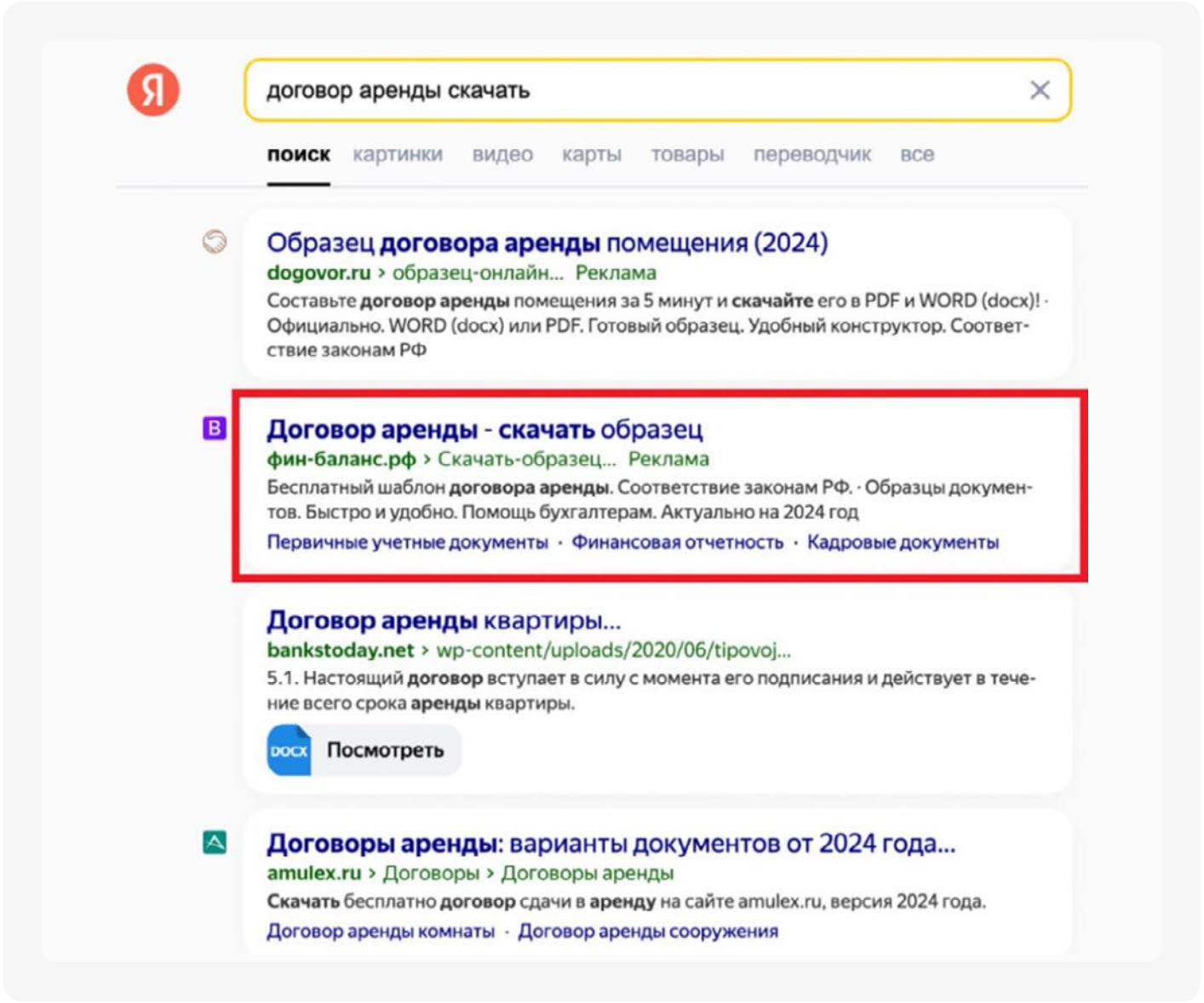


Рис. 8. Распространение ВПО Buhtrap с помощью рекламы Яндекса

В итоге жертва попадает на страницу, где можно скачать документы:

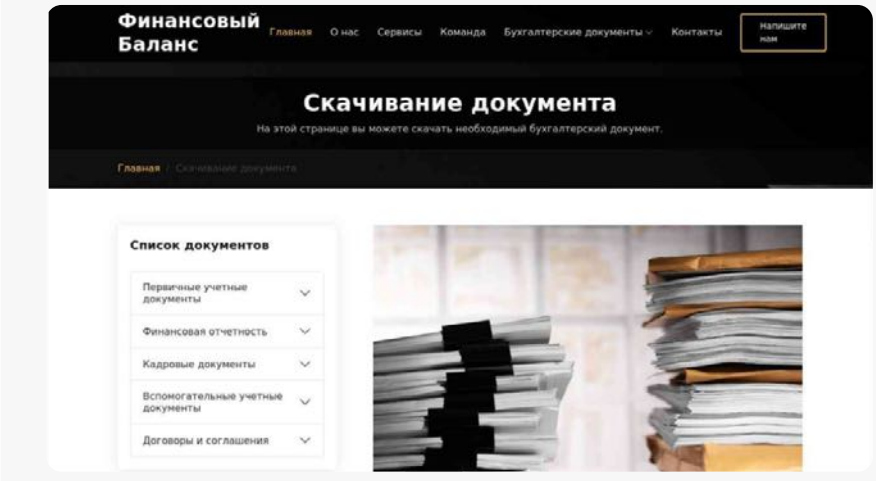


Рис. 9. Страница скачивания вредоносных документов

Скачиваемый архив содержит исполняемый файл, который сбрасывает на устройство Buhtrap RAT. Buhtrap RAT сохраняется на диск и прописывается в автозагрузку.

В ходе дальнейшего анализа была обнаружена дополнительная инфраструктура злоумышленников, которая включала лендинги для распространения ВПО, мимикрирующие под бухгалтерские сайты для скачивания документов, ряд серверов и доменов злоумышленников, а также ВПО для Android, вероятно, связанное с данными атакующими.

Вредоносное ПО с помощью веб-инжекта отображало на экране жертвы баннер, побуждающий установить «мобильный цифровой отпечаток»:

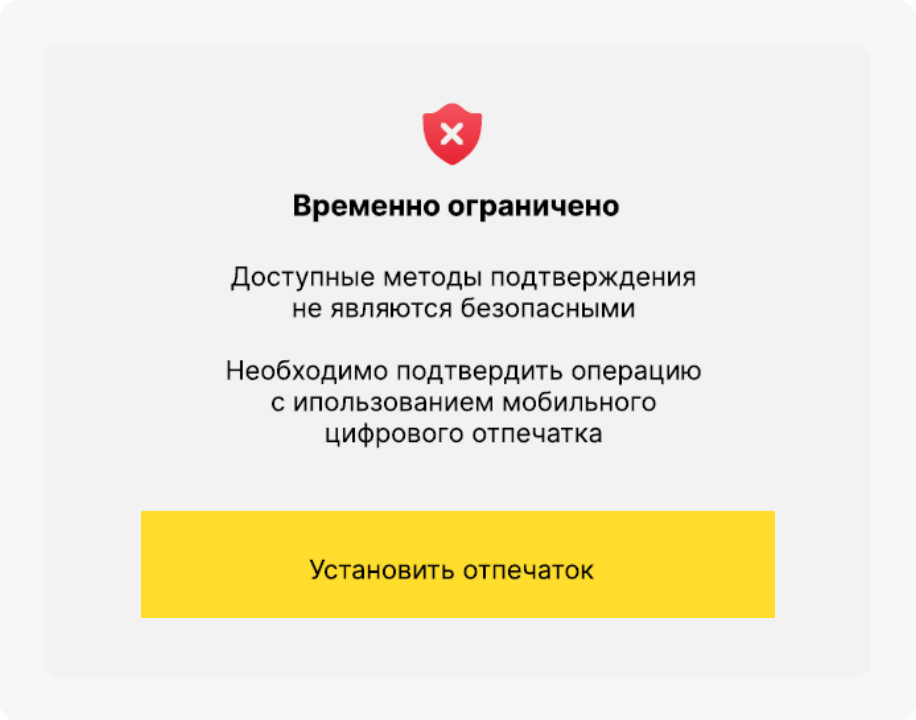


Рис. 10. Веб-инжект, отображаемый вредоносным ПО

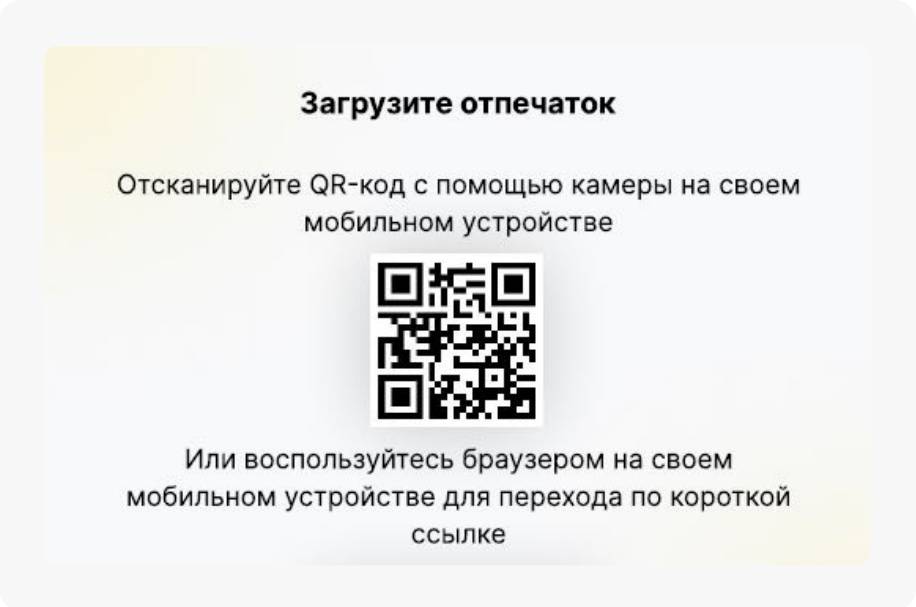


Рис. 11. QR-код, демонстрируемый с помощью веб-инжекта

Указанный QR-код содержал ссылку на скачивание APK-файла. Семейство было названо Buhtrap.Identifier Trojan. Данное ВПО предназначено для перехвата SMS-сообщений, сбора данных об устройстве и отправки полученной информации на C2.

На протяжении четвертого квартала 2024 года активность данного атакующего оставалась высокой, наблюдалось как появление новых лендинговых страниц бухгалтерской тематики, так и новых сэмплов ВПО для Android.

GOFFEE (aka Paper Werewolf)

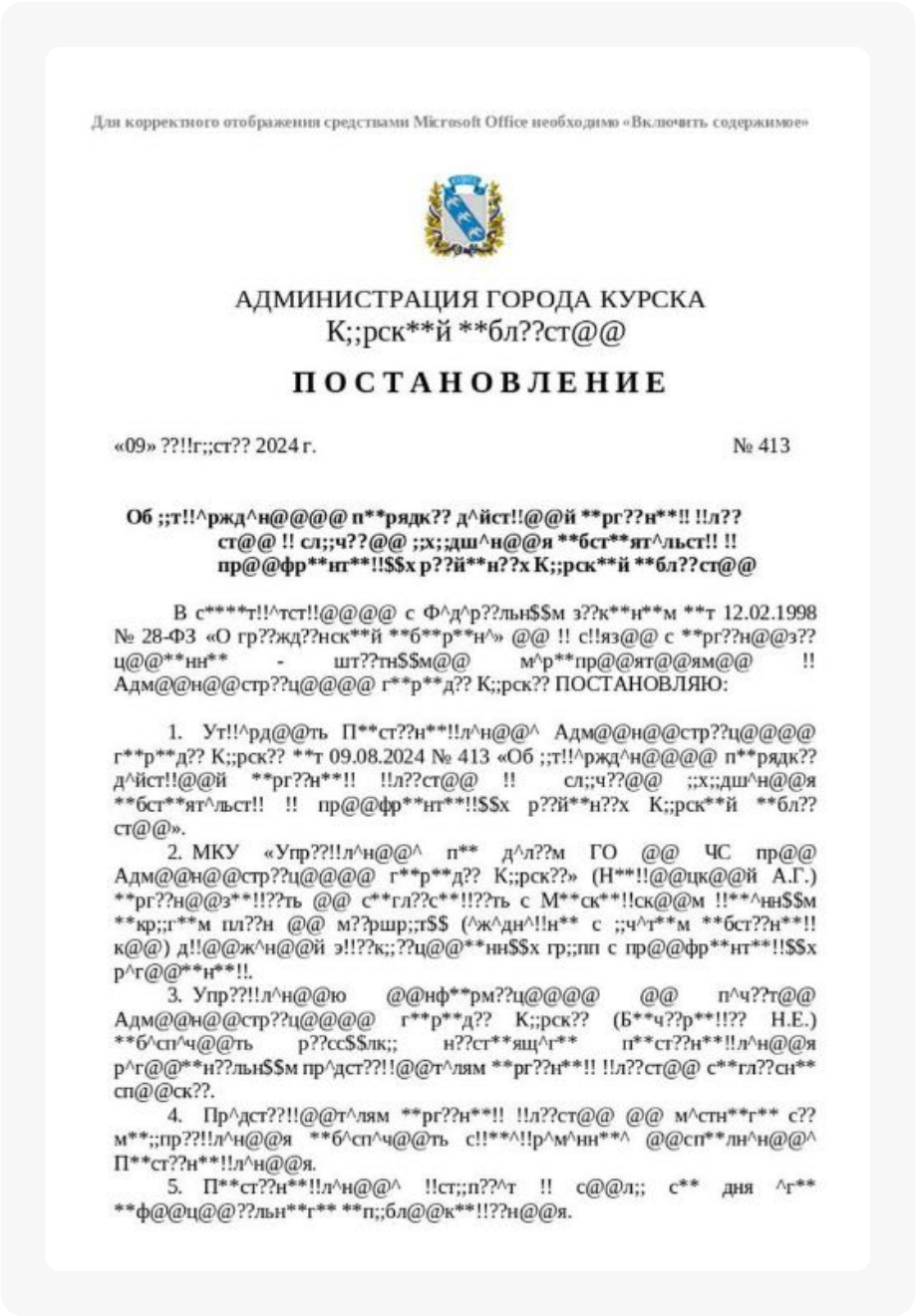
Начало активности	Используемые инструменты	Цель	Основные техники (MITRE)	ID
2020 год	• Owowa • PowerRAT • QwakMyAgent	Кража информации, шпионаж	Command and Scripting Interpreter: PowerShell	T1059.001
			Command and Scripting Interpreter: Visual Basic	T1059.005
			Command and Scripting Interpreter: JavaScript	T1059.007
			Deobfuscate/Decode Files or Information	T1140
			Application Layer Protocol: Web Protocols	T1071.001

f6.ru

Группировка GOFFEE, также известная как Paper Werewolf, начала свою деятельность в 2020 году, сосредоточившись на кибершпионаже. На ранних этапах своей активности она использовала разнообразные методы для компрометации систем, включая разработку специализированных инструментов. Одним из таких инструментов стал Owowa, предназначенный для атак на серверы Microsoft Exchange. Его использование в России было зафиксировано с мая 2022 года.

С начала осени 2024 года группировка значительно усилила свою активность, сконцентрировавшись на атаках на государственные учреждения, а также технологические, телекоммуникационные и производственные компании России. В арсенале появились новые инструменты, такие как модульный агент QwakMyAgent. Этот инструмент предоставлял возможность выполнять сложные команды и загружать дополнительные модули на скомпрометированные системы, повышая эффективность атак.

На первоначальном этапе атак GOFFEE в этот период осуществлялась массовая рассылка фишинговых писем с вредоносными документами Microsoft Office, содержащими зашифрованные макросы.



Для корректного отображения средствами Microsoft Office необходимо «Включить содержимое»

АДМИНИСТРАЦИЯ ГОРОДА КУРСКА
К;;рск**й **бл??ст@@

ПОСТАНОВЛЕНИЕ

«09» ??!!г;;ст?? 2024 г. № 413

Об ;;т!!^ржд^н@@@@ прядк?? д^йст!!@@й **рг??н**!! !!л?? ст@@ !! сл;;ч??@@ ;;х;;дш^н@@я **бст**ят^льст!! !! пр@@фр**нт**!!$$х р??й**н??х К;;рск**й **бл??ст@@**

В с****т!!^тст!!@@@@ с Ф^д^р??льн$$м з??к**н**м **т 12.02.1998 № 28-ФЗ «О гр??жд??нск**й **б**р**н^» @@ !! с!!яз@@ с **рг??н@@з?? ц@@**нн** - шт??тн$$м@@ м^р**пр@@ят@@ям@@ !! Адм@@н@@стр??ц@@@@ г**р**д?? К;;рск?? ПОСТАНОВЛЯЮ:

1. Ут!!^рд@@ть П**ст??н**!!л^н@@^ Адм@@н@@стр??ц@@@@ г**р**д?? К;;рск?? **т 09.08.2024 № 413 «Об ;;т!!^ржд^н@@@@ п**рядк?? д^йст!!@@й **рг??н**!! !!л??ст@@ !! сл;;ч??@@ ;;х;;дш^н@@я **бст**ят^льст!! !! пр@@фр**нт**!!$$х р??й**н??х К;;рск**й **бл?? ст@@».
2. МКУ «Упр??!!л^н@@^ п** д^л??м ГО @@ ЧС пр@@ Адм@@н@@стр??ц@@@@ г**р**д?? К;;рск??» (Н**!!@@цк@@й А.Г.) **рг??н@@з**!!??ть @@ с**гл??с**!!??ть с М**ск**!!ск@@м !!**^нн$$м **кр;;г**м гл??н @@ м??ршр;;г$$ (^ж^дн^!!н** с ;;ч^т**м **бст??н**!! к@@) д!!@@ж^н@@й э!!??к;;??ц@@**нн$$х гр;;пп с пр@@фр**нт**!!$$х р^г@@**н**!!.
3. Упр??!!л^н@@ю @@нф**рм??ц@@@@ @@ п^ч??т@@ Адм@@н@@стр??ц@@@@ г**р**д?? К;;рск?? (Б**ч??р**!!?? Н.Е.) **б^сп^ч@@ть р??сс$$лк;; н??ст**ящ^г** п**ст??н**!!л^н@@я р^г@@**н??льн$$м пр^дст??!!@@т^лям **рг??н**!! !!л??ст@@ с**гл??сн** сп@@ск??.
4. Пр^дст??!!@@т^лям **рг??н**!! !!л??ст@@ @@ м^стн**г** с?? м**;;пр??!!л^н@@я **б^сп^ч@@ть с!!**^!!р^м^нн**^ @@сп**лн^н@@^ П**ст??н**!!л^н@@я.
5. П**ст??н**!!л^н@@^ !!ст;;п??^т !! с@@л;; с** дня ^г** **ф@@ц@@??льн**г** **п;;бл@@к**!!??н@@я.

Рис. 12. Вредоносный документ группировки GOFFEE

При открытии таких документов вредоносный код активировался, что позволяло злоумышленникам загружать дополнительные программы для дальнейшего сбора данных, выполнения команд или обеспечения доступа к инфицированным системам. Среди этих программ были не только вышеуказанные, но и такие инструменты, как PowerRAT. Этот инструмент предоставляет атакующим возможность осуществлять удаленное выполнение команд на зараженном устройстве, устанавливать дополнительное вредоносное ПО и собирать конфиденциальные данные из скомпрометированного устройства.

Confman

Начало активности	Используемые инструменты	Цель	Основные техники (MITRE)	ID
2024	• DCRat • Gophish	Кража информации, шпионаж	Phishing: Spearphishing Link	T1566.002
			User Execution	T1204
			Scheduled Task/Job	T1053
			Impair Defenses: Disable or Modify Tools	T1562:001
			Masquerading: Match Legitimate Name or Location	T1036.005
			Obfuscated Files or Information: Compile After Delivery	T1027.004

В августе 2024 года специалисты Threat Intelligence зафиксировали кибератаку, направленную на крупные российские компании. Для реализации атаки использовались модифицированная версия вредоносной программы DarkCrystal RAT (DCRat), и платформа Gophish, предназначенная для проведения фишинговых кампаний, а также сетевая инфраструктура, подготовка которой началась в мае 2024 года. Целью атакующих было проникновение в инфраструктуру предприятий, получение доступа к данным и управление зараженными системами.

Для распространения вредоносного ПО применялись фишинговые письма, стилизованные под официальные сообщения Министерства энергетики РФ. В этих письмах содержались ссылки на поддельные ресурсы, внешне напоминающие облачные хранилища или приложения для видеоконференций. Кроме того, злоумышленники использовали технику HTML Smuggling, позволяющую скрытно загружать вредоносные файлы через JavaScript, встроенный в HTML-документы, что в свою очередь повышало успешность заражения.

Рис. 13. Веб-ресурс «24видеоконференцсвязь.рф», при доступе к которому осуществляется скачивание архива ivauc.7z, содержащего ВПО DCRat

Атаки также отличались использованием C2-серверов и поддельных доменов, которые создавали иллюзию легитимности для жертв. Злоумышленники стремились получить доступ к конфиденциальной информации из различных секторов, включая энергетику и финансы, что создавало угрозу для значимых инфраструктурных объектов.

Кроме того, часть инфраструктуры, связанной со злоумышленниками и мимикрировавшей под инфраструктуру государственных органов, не использовалась в зафиксированных атаках. Это может свидетельствовать о том, что эти ресурсы готовятся для проведения атак в будущем. Такой подход может указывать на стратегическое планирование злоумышленников, предполагающее создание резервных данных или запуск более сложных и масштабных операций на последующих этапах.

Дополнительно было выявлено, что часть инфраструктуры, через которую осуществлялось распространение вредоносного программного обеспечения, **пересекается с элементами инфраструктуры**, **атрибутированной к группировке GOFFEE** (aka Paper Werewolf). Это пересечение может свидетельствовать как об использовании обеими группировками одного и того же сервиса или платформы, предоставляющей услуги по распространению ВПО в рамках модели Malware-as-a-Service (MaaS), так и о том, что обнаруженные пересечения могут указывать на более тесное сотрудничество между группировками, включая возможное объединение ресурсов, обмен техническими данными или совместное проведение атак.

Hive0117 (aka Watch Wolf)

Начало активности	Используемые инструменты	Цель	Основные техники (MITRE)	ID
2022	DarkWatchman RAT	Хищение денежных средств	Phishing: Spearphishing Attachment	T1566.001
			Scheduled Task/Job: Scheduled Task	T1053.005
			Modify Registry	T1112
			Input Capture: Keylogging	T1056.001
			System Information Discovery	T1082

Злоумышленники из Hive0117, также известной как Watch Wolf, впервые попали на радары исследователей в феврале 2022 года. Отличительной чертой данной группы является использование вредоносного ПО для удаленного доступа DarkWatchman RAT.

Список функциональных возможностей трояна DarkWatchman на момент 2022 года включал:

- сбор информации о системе с использованием WMI;
- выполнение произвольного JS-кода через порождение процесса wscript.exe или без создания нового процесса через вызов функции eval();
- загрузка и запуск произвольного EXE-файла;
- загрузка и запуск произвольного DLL-файла с вызовом указанной функции;
- выполнение PowerShell-скриптов;
- выполнение WMI-команд;
- выполнение команд Windows Shell;
- удаленное обновление кейлогера;
- запись произвольного JS-кода, запускаемого при каждом старте RAT, в реестр;
- очистка Event Logs;
- очистка истории браузеров;
- удаление теневых копий с помощью vssadmin.exe;
- загрузка файлов с зараженной машины на C2-сервер;
- создание отложенных задач;
- DGA.

В 2024 активность преступной группы наблюдалась с апреля по декабрь — злоумышленники создавали фишинговые страницы для загрузки ВПО, которые имели тематику, связанную с налогами для юридических лиц и законодательными актами для закупок, производили рассылки, а также вносили следующие изменения в DarkWatchman RAT:

- был изменен XOR-ключ для расшифровки основного кода DarkWatchman RAT;
- удалена команда для загрузки и выполнения DLL;
- добавлена очистка истории веб-браузера Internet Explorer;
- добавлена функция запуска созданной запланированной задачи в планировщике задач Windows;
- добавлена функция сбора файлов истории веб-браузеров: Internet Explorer, Firefox, Chrome, YandexBrowser.

В декабре 2024 была произведена массовая рассылка от имени «Pony Express». Интересно, что мимикрия под данный бренд уже использовалась атакующими в ноябре 2023 года. В случае с email-рассылками цепочка атак группировки следущая: письмо содержит ZIP-архив, внутри которого находятся несколько файлов, в том числе исполняемый файл. Данный исполняемый файл представляет собой самораспаковывающийся архив (RarSFX) и содержит команду в комментариях. В результате выполнения указанной команды содержимое самораспаковывающегося архива RarSFX распакуется, и запустится DarkWatchman RAT.

VasyGrek (aka Fluffy Wolf)

Начало активности	Используемые инструменты	Цель	Основные техники (MITRE)	ID
2016	• RMS • AveMaria (WarzoneRAT) • BurnsRAT • META Stealer • RedLine Stealer • PureHVNC • PureCrypter • PureLogs	Удаленный доступ к скомпрометированным устройствам, кража информации и хищение денежных средств	User Execution: Malicious File	T1204.002
			Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1547.001
			Phishing: Spearphishing Link	T1566.002
			Remote Access Software	T1219
			Hijack Execution Flow: DLL Side-Loading	T1574.002

f6.ru

Начиная с 2020 года специалисты нашей компании отслеживают атаки злоумышленника VasyGrek, нацеленного на российские компании как минимум с 2016 года. В качестве первоначального вектора атак VasyGrek использует электронные письма, отправляемые якобы от имени бухгалтерии на финансовые темы с запросами на подпись актов сверки, платежных поручений и т. д. Ниже представлен пример фишингового письма злоумышленника.

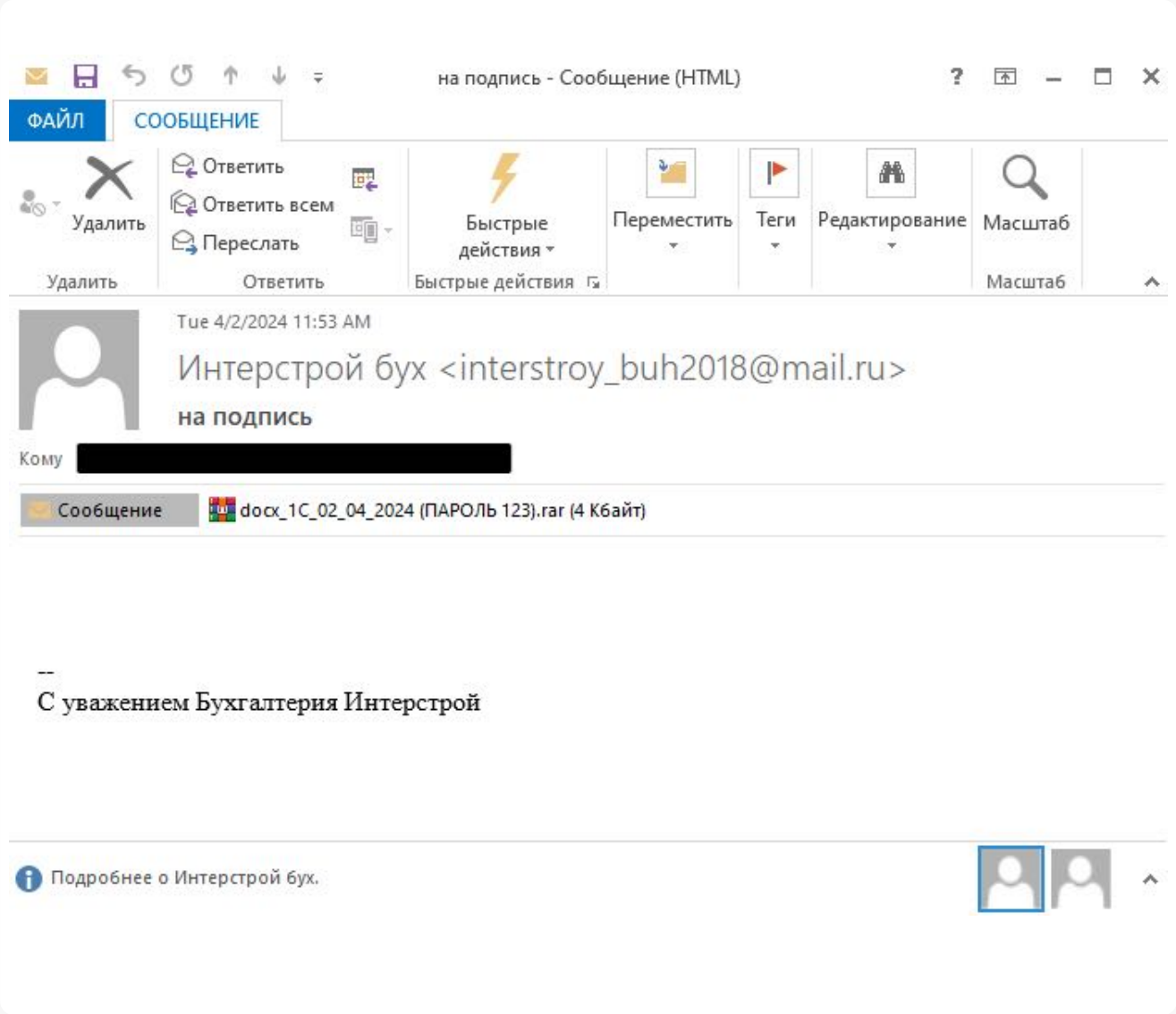
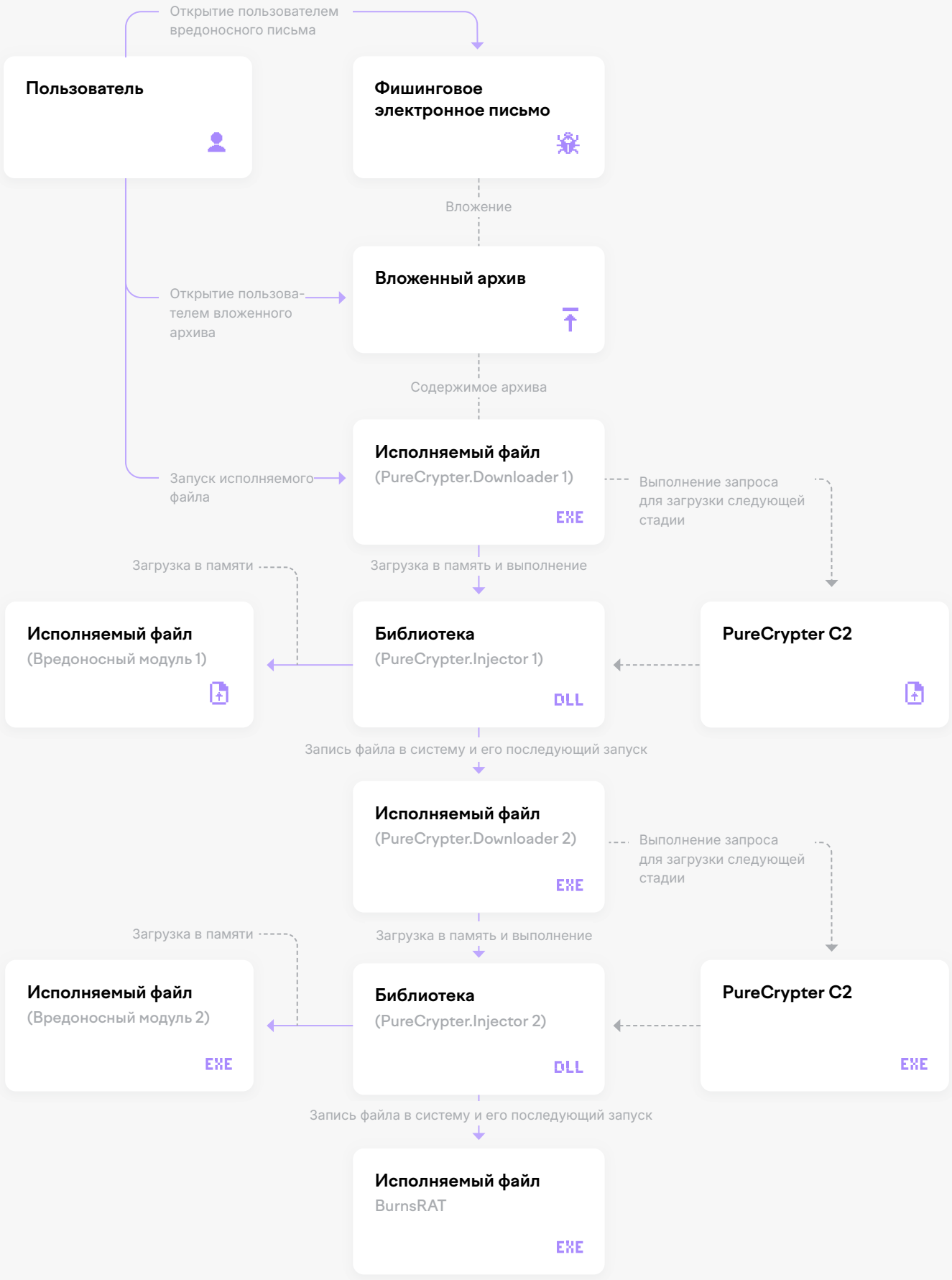


Рис. 14. Пример письма, отправляемого злоумышленником VasyGrek

В своих многочисленных атаках VasyGrek использовал инфицированные модификации легитимных инструментов удаленного управления системой — RMS (Remote Utilities), вредоносное ПО разработчика PureCoder (PureCrypter, PureLogs, PureHVNC), а также другое доступное для покупки в публичном пространстве ВПО, такое как META Stealer, WarzoneRAT (AveMaria), RedLine Stealer.

На рисунке ниже представлена цепочка заражения VasyGrek в 2024 году. Цепочка заражения может иметь отличия в конкретных атаках. Например, в некоторых атаках вместо вложенного архива используется URL-адрес, при переходе по которому загружается архив. Также VasyGrek может использовать разное количество PureCrypter. Downloader, таким образом изменяя количество вредоносных инструментов, загружаемых на зараженную систему. Кроме того, ближе к концу 2024 года в его цепочку заражения добавились VBS-сценарии, которые используются для обфускации инициализации атаки, а также для закрепления в системе.

Пример актуальной цепочки заражения злоумышленника VasyGrek



По нашим данным, после того как на зараженную систему устанавливался BurnsRAT, VasyGrek отправлял команды следующего вида: cmdv start {URL}. Данные команды использовались для отображения веб-страницы с указанным злоумышленником URL в браузере на зараженной системе. В исследуемых случаях ссылки содержали лендинг-страницы с фейковыми формами авторизациии в бизнес-аккаунты банковских сервисов. VasyGrek использовал веб-страницы, содержащие фейковые формы, как минимум, с 2022 года.

В абсолютном большинстве атак обнаруженной нами финальной стадией цепочки заражения являлась инфицированная модификация ПО удаленного управления системой Remote Utilities (RMS). Данное вредоносное ПО классифицируется специалистами нашей компании как BurnsRAT. Однако после публикации **нашего блога** о сотрудничестве VasyGrek с продавцом ВПО Mr.Burns он перестал использовать BurnsRAT. В атаках, выявленных в июле-ноябре 2024 года, он применял META Stealer и инструменты разработчика PureCoder (PureLogs, PureHVNC). Как и в атаках ранее, полезные нагрузки доставлялись с помощью ВПО-загрузчика PureCrypter.

Установить связь VasyGrek со злоумышленником Mr.Burns специалистам удалось следующим образом: при анализе сэмпла ВПО, используемого в атаках VasyGrek в 2020 году, была обнаружена ссылка на командный сервер. При обращении к домену из этой ссылки открывалась корневая директория, в которой находился конфигурационный файл, содержащий токен бота Telegram и команды для работы бота с базой данных. Свободный доступ к корневой директории, вероятно, осуществлялся вследствие технических ошибок в конфигурации сервера. В ходе дальнейшего исследования были получены сообщения, отправленные и полученные этим ботом и было выяснено, что он использовался для получения данных с зараженных устройств. Взаимодействие с Telegram-ботом осуществляли только два пользователя, которые в результате дальнейших исследований на хак-форумах и в мессенджерах были атрибутированы к злоумышленникам VasyGrek и Mr.Burns. Второй из них является истинным долгожителем дарквеба: первые его сообщения на теневых форумах датируются 2010 годом. Созданные Mr.Burns программы в большинстве своем основываются на легитимных средствах удаленного управления, таких как TeamViewer, RMS (Remote Utilities), LiteManager и др. Таким образом, ошибка, допущенная при настройке командного сервера, привела специалистов к связи двух злоумышленников, взаимодействие которых длилось более пяти лет.

Kirill KSV

Начало активности	Используемые инструменты	Цель	Основные техники (MITRE)	ID
2023	• RADX RAT • DCRat • PureLogs	Хищение денежных средств	Phishing: Spearphishing Link	T1566.002
			User Execution	T1204
			Scheduled Task/Job	T1053
			System Binary Proxy Execution	T1218
			Account Discovery	T1087

С конца 2023 года специалисты нашей компании фиксируют атаки, проводимые атакующим **Kirill KSV**, нацеленные на сотрудников российских компаний. Злоумышленники распространяют вредоносные программы DarkCrystal RAT (DCRat) и RADX RAT через фишинговые письма. Название группировки произошло от домена kirill.ksv.example.com, найденного в заголовках этих писем. В тексте писем содержались ссылки на поддельные домены, маскирующиеся под легитимные ресурсы, что способствовало повышению доверия к этим сообщениям и увеличению вероятности заражения.

До конца сентября 2024 года Kirill KSV активно атаковал компании, представляющие финансовый, информационно-технологический, энергетический, транспортный, производственный и биотехнологический сектора. В это время он значительно расширил свою инфраструктуру, добавив новые домены, хосты и вредоносное программное обеспечение.

В августе 2024 года Kirill KSV начал активно использовать новый инструмент — PureLogs. Этот инструмент относится к классу вредоносного программного обеспечения типа стилер и позволяет злоумышленнику похищать данные с устройства жертвы. PureLogs извлекает пользовательскую информацию из браузеров, включая куки, пароли и данные автозаполнения, а также данные из криптовалютных кошельков и приложений. Кроме того, он сканирует и похищает файлы, обнаруженные на зараженном устройстве, по заданной атакующим маске.

С октября 2024 года атаки со стороны Kirill KSV не фиксировались. Эти обстоятельства могут свидетельствовать как о смене тактики, предполагающей переход на более скрытые методы работы, так и о полном прекращении деятельности.

Rezet (aka Rare Wolf)

Начало активности	Используемые инструменты	Цель	Основные техники (MITRE)	ID
2018	• AnyDesk • Mipko Employee Monitor	Хищение денежных средств	Phishing: Spearphishing Link	T1566.002
			Command and Scripting Interpreter: Windows Command Shell	T1059.003
			User Execution: Malicious File	T1204.002
			Credentials from Password Stores: Credentials from Web Browsers	T1555.003
			File and Directory Discovery	T1083
			Application Layer Protocol: Mail Protocols	T1071.003
			Remote Access Software	T1219

Группировка Rezet, также известная как Rare Wolf, начала свою деятельность в конце 2018 года. В своей работе она использует разнообразные методы заражения, включая фишинговые атаки, посредством которых они распространяют вредоносное программное обеспечение. С начала 2019 года группа применяла WebBrowserPassView (wbpv.exe) для сбора паролей из браузеров, а также использовала Mipko Employee Monitor для мониторинга активности пользователей, перехвата нажатий клавиш и записи с экрана. Кроме того, в период с 2018 по 2021 год Rezet активно распространяла майнеры.

С 2021 года группировка начала использовать файл rezet.cmd, который стал ключевым элементом её атак. Этот файл применялся для создания скрытых каталогов на заражённых устройствах, таких как %SYSTEMDRIVE%\Intel, где размещались вредоносные программы и файлы для дальнейшей эксплуатации. Вредоносные программы также использовали методы обфускации, такие как модификация реестра, чтобы гарантировать их запуск при старте системы.

В 2024 году активность Rezet значительно возросла. В их атаках стали использоваться более сложные методы. Одним из них стало расширенное использование фишинговых писем с вложениями и декой-документами, которые часто связаны с политической тематикой или важными социальными событиями, что помогает злоумышленникам повышать доверие жертв и увеличивать вовлеченность. Конечной полезной нагрузкой этих атак обычно становятся Mipko Employee Monitor или AnyDesk — программы, которые позволяют злоумышленникам дистанционно контролировать устройства жертв, записывать с экрана и перехватывать нажатия клавиш.

В 2024 году группировка также значительно расширила свою инфраструктуру, добавив новые домены в зоне .ru, однако многие из этих доменов ещё не использовались в атаках. В будущем они, скорее всего, будут активно использовать эти домены, имена которых часто ассоциируются с офисными сервисами, верификацией и облачными технологиями. Это свидетельствует о том, что Rezet планирует продолжить использование фишинговых рассылок с текстами писем или вложениями, которые будут связаны с этими темами, чтобы повысить свою эффективность и маскировку атак.

Таким образом, Rezet продолжает развивать свою стратегию, повышая степень скрытности и точности своих атак. Активность группировки растет, и с каждым месяцем она находит новые способы обхода защитных механизмов, используя более разнообразные и гибкие методы воздействия.

Stone Wolf

Начало активности	Используемые инструменты	Цель	Основные техники (MITRE)	ID
2024	• DarkGate • LummaC2 • Remcos • Pure HVNC • BrockenDoor • Tuoni	Кража информации	User Execution: Malicious File	T1204.002
			Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1547.001
			Phishing: Spearphishing Link	T1566.002
			Remote Access Software	T1219
			Hijack Execution Flow: DLL Side-Loading	T1574.002

Группировка Stone Wolf, впервые обнаруженная в мае 2024 года, атакует в основном органы госвласти и организации из сферы ИТ, рассылая фишинговые письма для распространения Meduza Stealer. Во многих известных случаях атака начиналась с рассылки фишинговых писем, замаскированных под существующие компании, занимающиеся автоматизацией технологических процессов. В письме просят ознакомиться с техническим заданием, которое якобы находится в приложенном архиве.

В осенних атаках (октябрь-ноябрь 2024) атакующий распространял такие бэкдоры, как Remcos, DarkGate и ранее неизвестное семейство BrockenDoor, позволяющее опрашивать командные центры, передавать с них файлы и запускать их, а также выполнять команды.

Также в атаках группы встречался инструмент для постэксплуатации Tuoni, предназначенный для пентестеров и обучающих целей. Ранее данный фреймворк не использовался злоумышленниками.

FakeTicketer

Начало активности	Используемые инструменты	Цель	Основные техники (MITRE)	ID
Июнь 2024	• Zagrebator.RAT • Zagrebator.Stealer	Компрометация данных	Phishing: Spearphishing Link	T1566.002
			User Execution	T1204
			Scheduled Task/Job	T1053
			System Binary Proxy Execution	T1218
			Account Discovery	T1087

f6.ru

FakeTicketer — злоумышленник, активный как минимум с июня 2024 года и занимающийся рассылкой ВПО типа stealer и RAT. В первых выявленных атаках ВПО было замаскировано под билеты на спортивное мероприятие, поэтому было сделано предположение, что злоумышленнк имеет финансово-мотивированные цели.

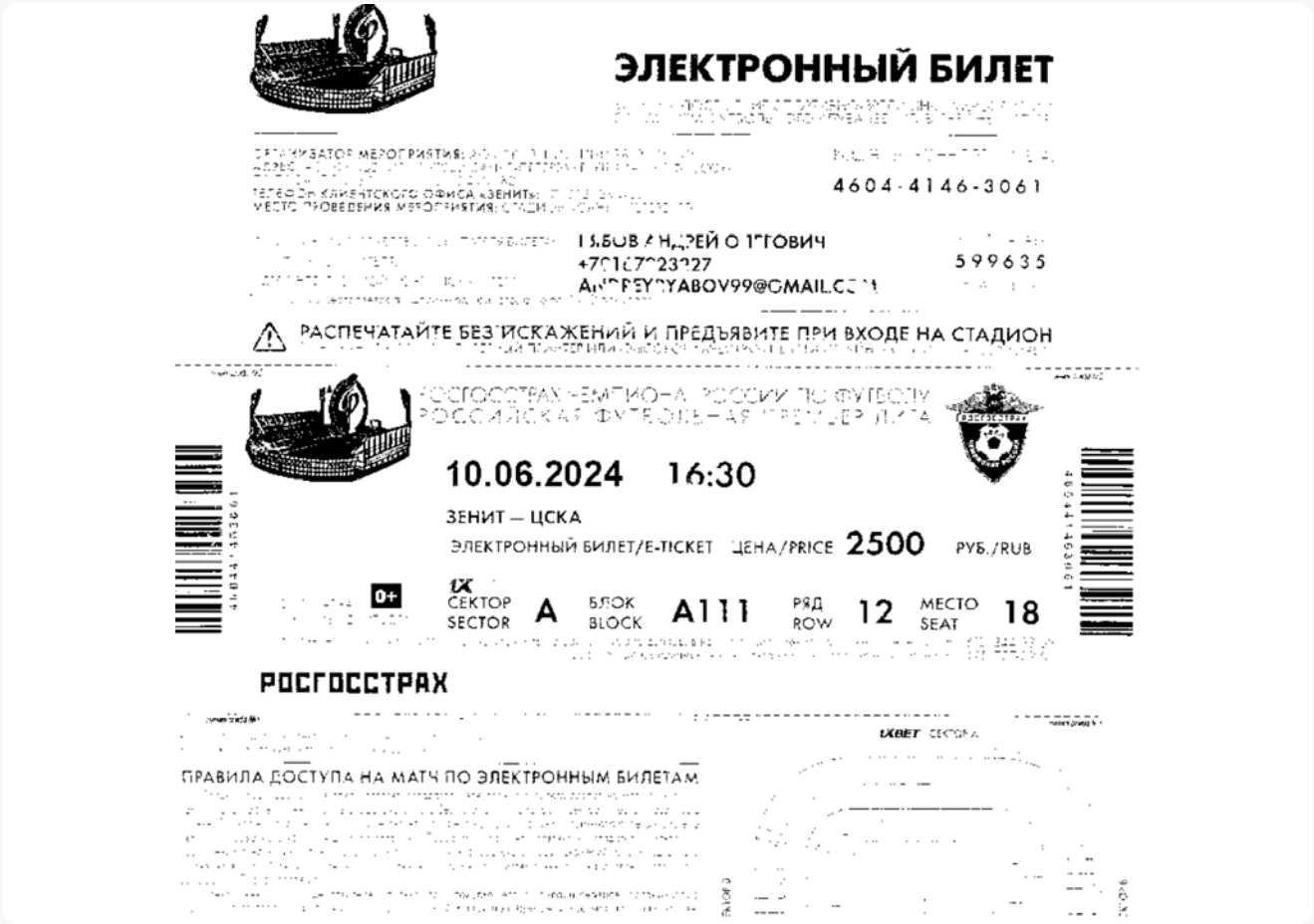


Рис. 15. Пример файла-декоя

В октябре в качестве документа-приманки злоумышленники использовали школьный аттестат. В декабре же приманка была замаскирована под нормативный акт, выпущенный администрацией города Симферополя Республики Крым. Этот факт дает аналитикам повод усомниться, что атакующие — финансово-мотивированные, а не политически.

Помимо декоя на компьютер жертвы попадает исполняемый .NET файл, сбрасывающий полезную нагрузку в виде **Zagrebator.RAT**. Это ВПО типа RAT, поддерживающее следующие команды:

- сохранить в указанный файл указанный контент;
- найти и отправить на C2 все файлы с рабочего стола и рекурсивно всех подкаталогов;
- найти и отправить на C2 все файлы из указанного каталога, без рекурсии;
- перечислить все файлы всех дисков ПК (в корне, без рекурсии), отправить на C2;
- перечислить все файлы указанного диска или папки (в корне, без рекурсии), отправить на C2;
- удалить указанный файл.

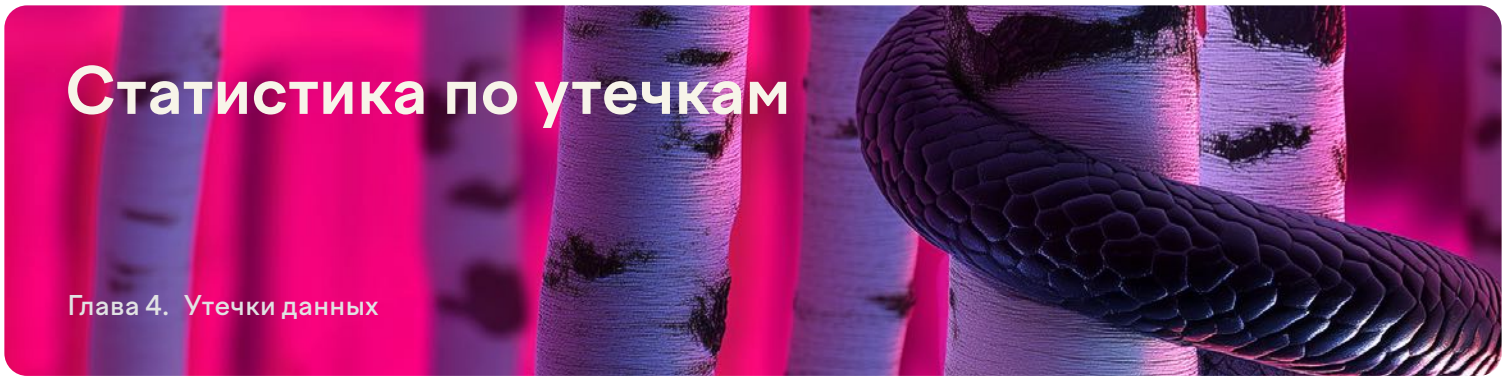
Zagrebator.Stealer позволяет собирать данные авторизации из браузеров Mozilla, Opera, Microsoft Edge, Chrome, которые записываются в DataTable и передаются в XML-формате в PUT-запросе на C2.

Утечки данных

Утечки данных

В 2024 году аналитики Threat Intelligence компании F6 зафиксировали на андеграундных форумах и в тематических Telegram-каналах **455 новых случаев публичных утечек** баз данных по компаний из России и СНГ. Для сравнения: в 2023 было выявлено 246 случаев утечек.

Суммарно утечки 2024 года содержали **более 457 млн строк** с данными 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

Часть утечек злоумышленники не публиковали в открытом доступе — продавали или использовали в последующих каскадных атаках на крупных игроков коммерческого и государственного секторов. Также в 2024 году были зафиксированы случаи, когда злоумышленники выдавали старые «слитые» данные за новые крупные утечки для привлечения повышенного внимания.

Сравнение кол-ва утекших строк с данными пользователей

f6.ru

Год	Кол-во
2024	457 577 054
2023	296 000 000

Электронные почтовые адреса, телефонные номера и пароли пользователей, оказавшиеся в открытом доступе, представляют наибольшую угрозу, поскольку они могут быть использованы злоумышленниками для различных атак. Из общего количества утекших данных 236 919 480 записей содержали электронные адреса, причем только 154 541 847 из них были уникальными. Также было зафиксировано, что 153 228 995 записей содержат пароли пользователей, среди которых 102 836 067 уникальных. Записей с телефонными номерами насчитывается 459 497 755, из которых 220 496 247 уникальные.

Количество утекших баз данных

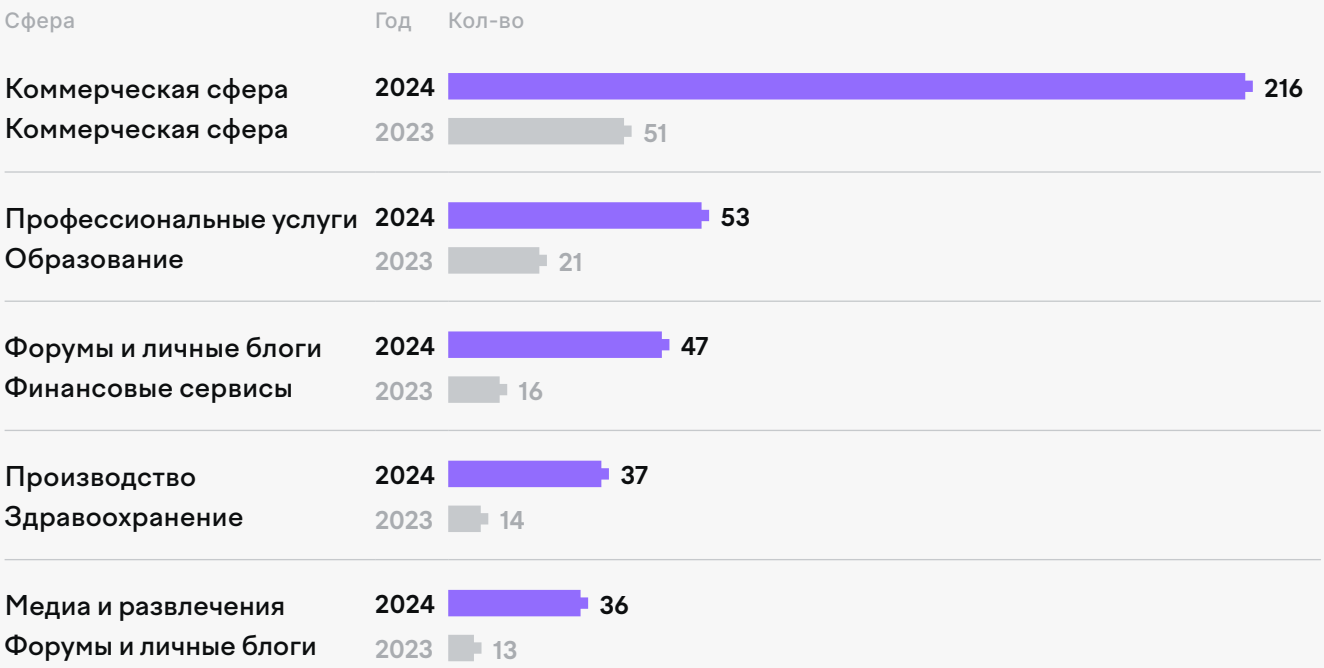
f6.ru

Год	Кол-во
2024	455
2023	246

За рассматриваемый период можно отметить, что на первом месте по скомпрометированным отраслям остается коммерческая сфера. К ней можно отнести все сайты интернет-магазинов (одежда, электроника, спорттовары, мебельные магазины и так далее). В 2024 году сайты компаний в сфере оказания профессиональных услуг заняли второе место по количеству опубликованных баз данных, относящихся к ним. Третью позицию по количеству опубликованных баз данных занимают тематические сайты форумов и личных блогов.

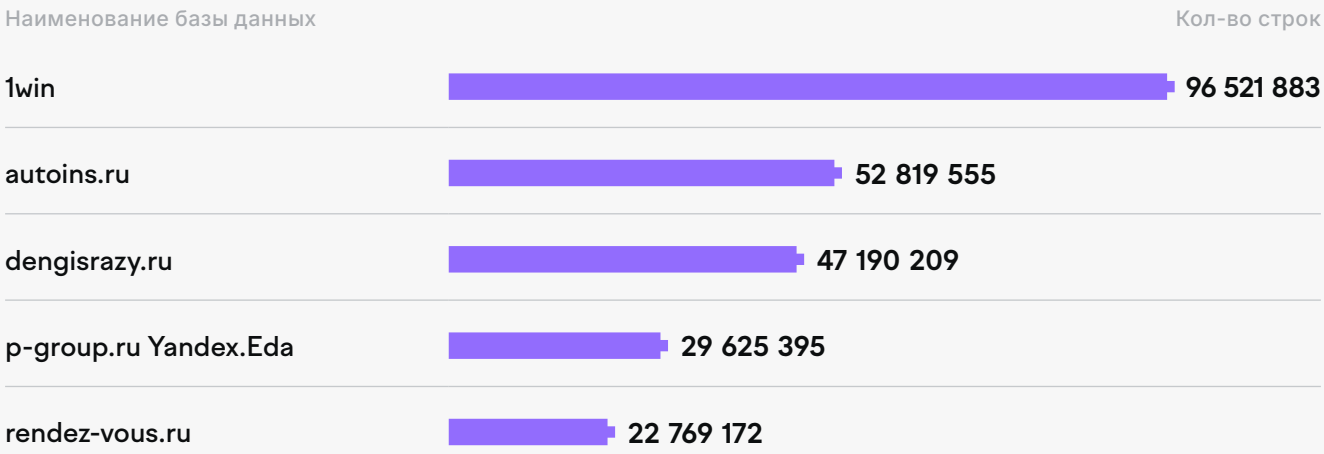
Сравнение по индустриям

f6.ru



Топ 5 самых объемных утечек по количеству строк

f6.ru



В таблице выше представлены наименования баз данных по доменам скомпрометированных сайтов компаний, указанных злоумышленником.

1. Утечка букмекерской компании «1Win»;
2. Публикация данных крупной страховой компании;
3. Данные сайта онлайн-займов «Деньги сразу»;
4. Публикация обогащенной версии утечки ЯндексЕда от 2022 года, найденной в опубликованных данных компании «Performance Group»;
5. Публикация данных магазина обуви и одежды «Rendez-Vous».

Тренды, связаные с утечками данных

В ходе анализа были выявлены определенные тренды, которые будут описаны ниже.

Злоумышленники продолжают активно публиковать базы данных в Telegram

За рассматриваемый период специалистами Threat Intelligence было зафиксировано практически в 2 раза больше публикаций баз данных российских компаний в Telegram, чем на тематических форумах. В 2023 году 68,70% всех публикаций приходилось на Telegram.

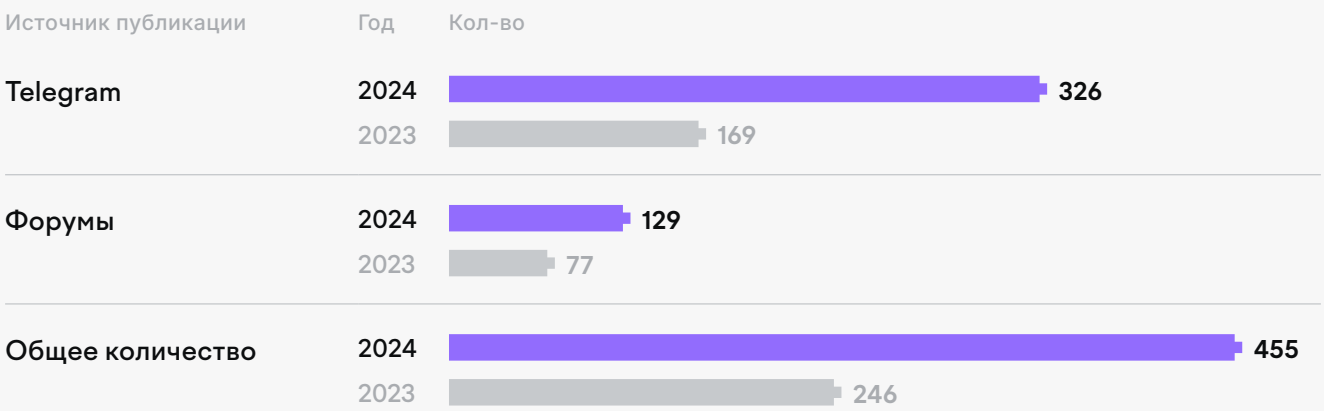
В отличие от андеграундных форумов, где необходимо набирать очки репутации, оплачивать регистрацию, следовать правилам форума, в Telegram любой пользователь может создать свой тематический канал.

Кроме того, на андеграундных форумах существуют правила, согласно которым нельзя публиковать поддельные данные, продавать старые базы данных и так далее. При нарушении правил происходит блокировка аккаунта либо удаление поста о продаже/публикации. В Telegram злоумышленники не ограничены и зачастую публикуют как старые случаи утечек, так и приватные базы данных. Также они обмениваются ими в приватных чатах. Обманывают клиентов, продавая старые базы данных под видом свежей утечки.

Безусловно, андеграундные форумы продолжат свое существование как площадка для публикации и продажи баз данных ввиду того, что множество злоумышленников предпочитают не рисковать своими финансами, использовать гарант-сервисы форумов и связываться только с проверенными продавцами. Однако нельзя отрицать факт того, что Telegram удобен и некоторые злоумышленники используют его как основную площадку для публикации скомпрометированных ими баз.

Сравнительная статистика по кол-ву публикаций в Telegram и на форумах

f6.ru



Больше Telegram-каналов, публикующих приватные базы данных

В 2023 году появились Telegram-каналы, в которых злоумышленники начали публиковать приватные базы данных. В большинстве случаев администраторы подобных каналов не являются первоисточниками компрометации. Они приобретают приватные базы данных у других злоумышленников либо обмениваются базами с целью дальнейшей публикации.

В 2024 году данный способ распространения получил развитие. Появилось множество подобных каналов, которые занимаются одним и тем же — публикацией баз данных, которые находятся в распоряжении ограниченного круга лиц. Актуальность баз данных может варьироваться: в открытом доступе оказываются как относительно свежие данные, так и базы, скомпрометированные за несколько лет до того, как стать общедоступными. Нередко публикуют и поддельные базы данных, приобретенные у других злоумышленников. Немногие каналы проверяют качество публикуемых данных.

Публикация баз с искаженным набором данных

Специалистами Threat Intelligence также были зафиксированы случаи публикации искаженных баз данных. В подобных наборах часть цифр в номерах телефонов или электронных почтовых адресах искажена заменой цифр (например, цифры «6» могут быть поменяны на «9» и т.д.). Важно отметить, что искажена лишь часть данных и в любом случае в открытом доступе оказывается ряд настоящих данных.

Цель, которую преследуют злоумышленники, продавая поддельные данные, остается неизвестной. Можно лишь предположить, что таким образом они пытаются набить цену настоящему набору данных. После того как оказывается, что опубликованная приватная база данных была частично искажена, сразу находятся продавцы, которые могут продать оригинальные данные за крупную сумму.

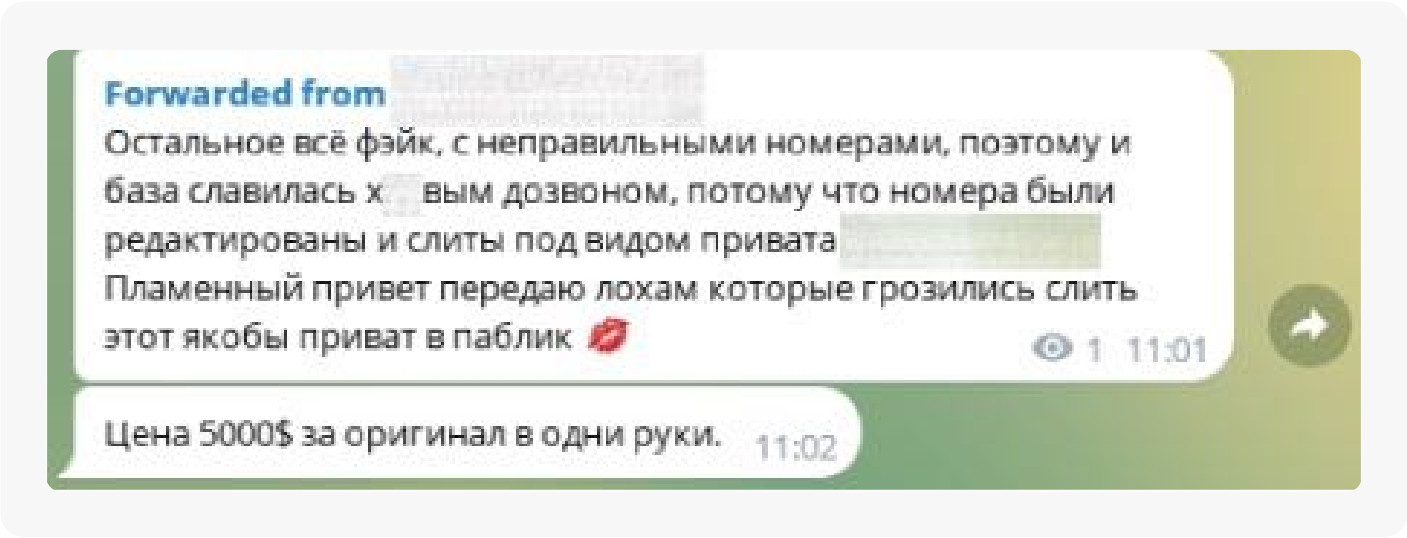


Рис. 16. Пример сообщения злоумышленника, продающего базы

Компрометации данных белорусских компаний

Основной анализ посвящен утечкам российских компаний, однако в 2024 году специалистами Threat Intelligence были также зафиксированы публикации скомпрометированных данных компаний из Беларуси.

31 июля 2024 года в Telegram-канале «Cyber.Anarchy.Squad» от имени администратора канала опубликовано сообщение о распространении базы компании «Belbazar24» (belbazar24[.]by) на интернет-ресурсе «Mega».

Опубликованный SQL-файл содержит несколько таблиц с персональными данными пользователей:

- таблица «it_email_list», содержит 102 483 строк: имена пользователей, адреса электронных почт.
- таблица «it_orders», содержит 154 440 строк: телефонные номера, IP-адреса, адреса электронных почт, имена.

13 сентября 2024 года «Cyber.Anarchy.Squad» опубликовали часть данных, похищенных в ходе атаки на Белорусскую торгово-промышленную палату. Злоумышленниками не были опубликованы базы данных, содержащие электронные почтовые адреса. В результате компрометации был опубликован архив «Дані_працівників+підприємства.rar», включающий в себя PDF-документы, телефонные справочники БелТПП, табели учета рабочего времени, резюме, отсканированные копии паспортов работников и иные внутренние документы.

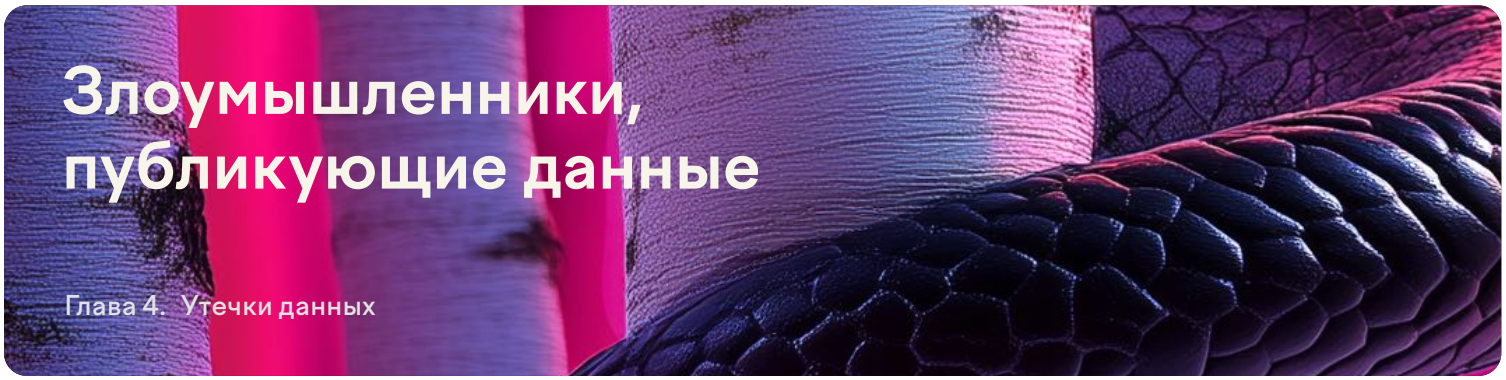
Вместе с Белорусской торгово-промышленной палатой группировкой «Cyber.Anarchy.Squad» были скомпрометрированы данные следующих белорусских организаций:

- «Белпатентсервис»
- «Белинтерэкспо»
- «Международный арбитражный суд при БелТПП»
- «Центр делового образования Белорусской торгово-промышленной палаты» и ряд других сопутствующих ресурсов.

10 ноября 2024 года «DumpForums» опубликовали заявление об атаке и полном уничтожении инфраструктуры белорусского государственного ресурса «Электронные счета-фактуры» (vat[.]gov[.]by). Также злоумышленники заявили о выгрузке баз данных, содержащих порядка 478 тысяч строк личной информации граждан: хэшированные пароли, имена, адреса электронной почты, системные данные.

14 ноября 2024 года группировка «DumpForums» заявила о компрометации данных «Национального банка Республики Беларусь» (nbrb[.]by). «DumpForums» заявили, что планируют опубликовать базы данных на своем форуме. Однако в 2024 году в открытом доступе база данных так и не появилась. Ряд источников сообщают, что база содержит порядка 759 тысяч строк, среди которых находятся такие персональные данные как: ФИО, телефонные номера, адреса электронных почт, названия организаций, системные данные. Информация не оглашалась злоумышленниками публично, а значит, требует дополнительного подтверждения.

В 2024 году появилось большое количество новых злоумышленников, которые публиковали базы данных в личных Telegram-каналах (как публичных, так и приватных) и на андеграундных форумах.



Злоумышленники, публикующие данные

Sh4dow

Sh4dow — злоумышленник, публикующий базы данных преимущественно российских компаний. Его первая активность была зафиксирована на известном андеграундном форуме BreachForums. Скриншот профиля, зарегистрированного 28 декабря 2023 года, представлен ниже:

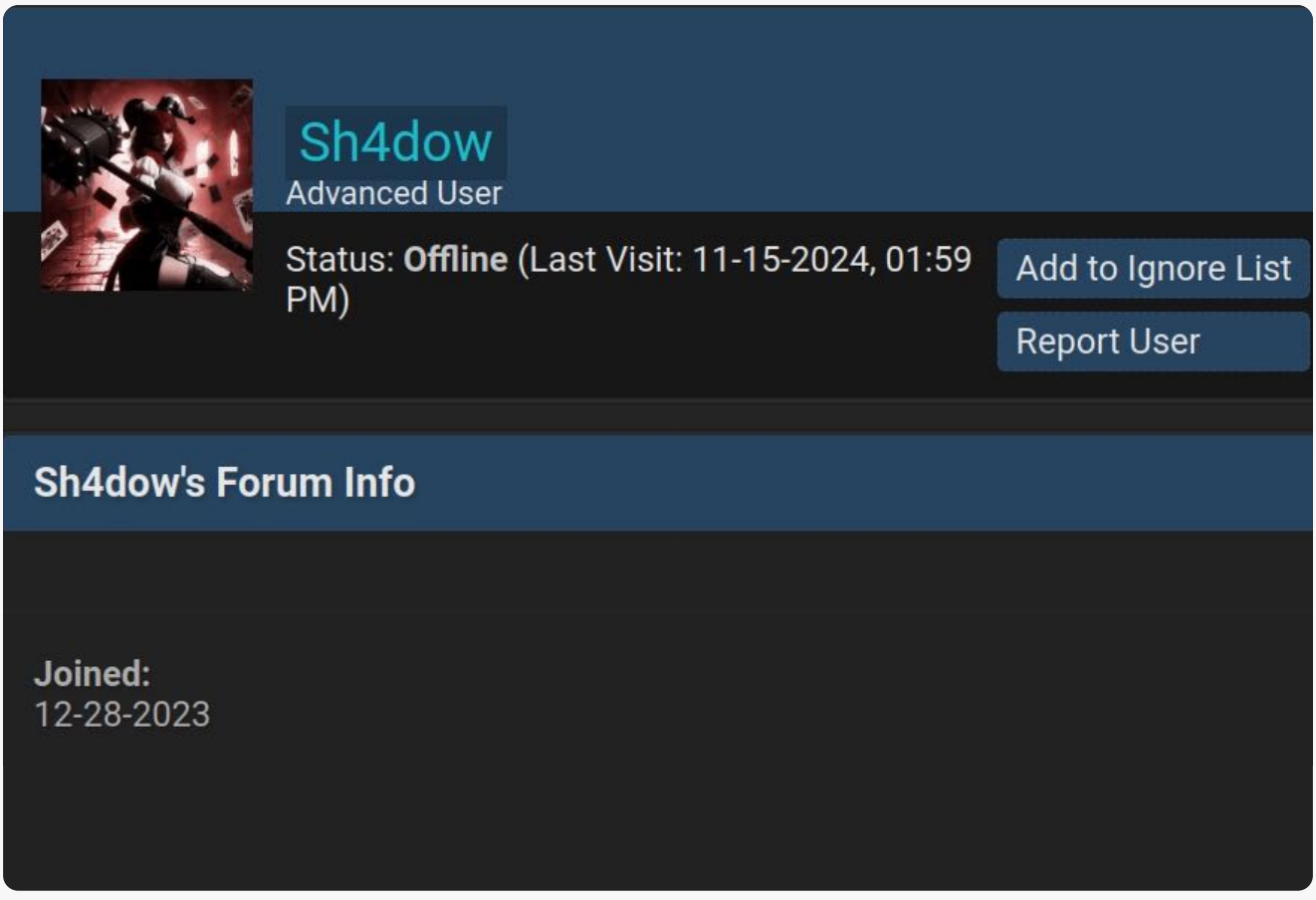


Рис. 17. Профиль злоумышленника на андеграундном форуме

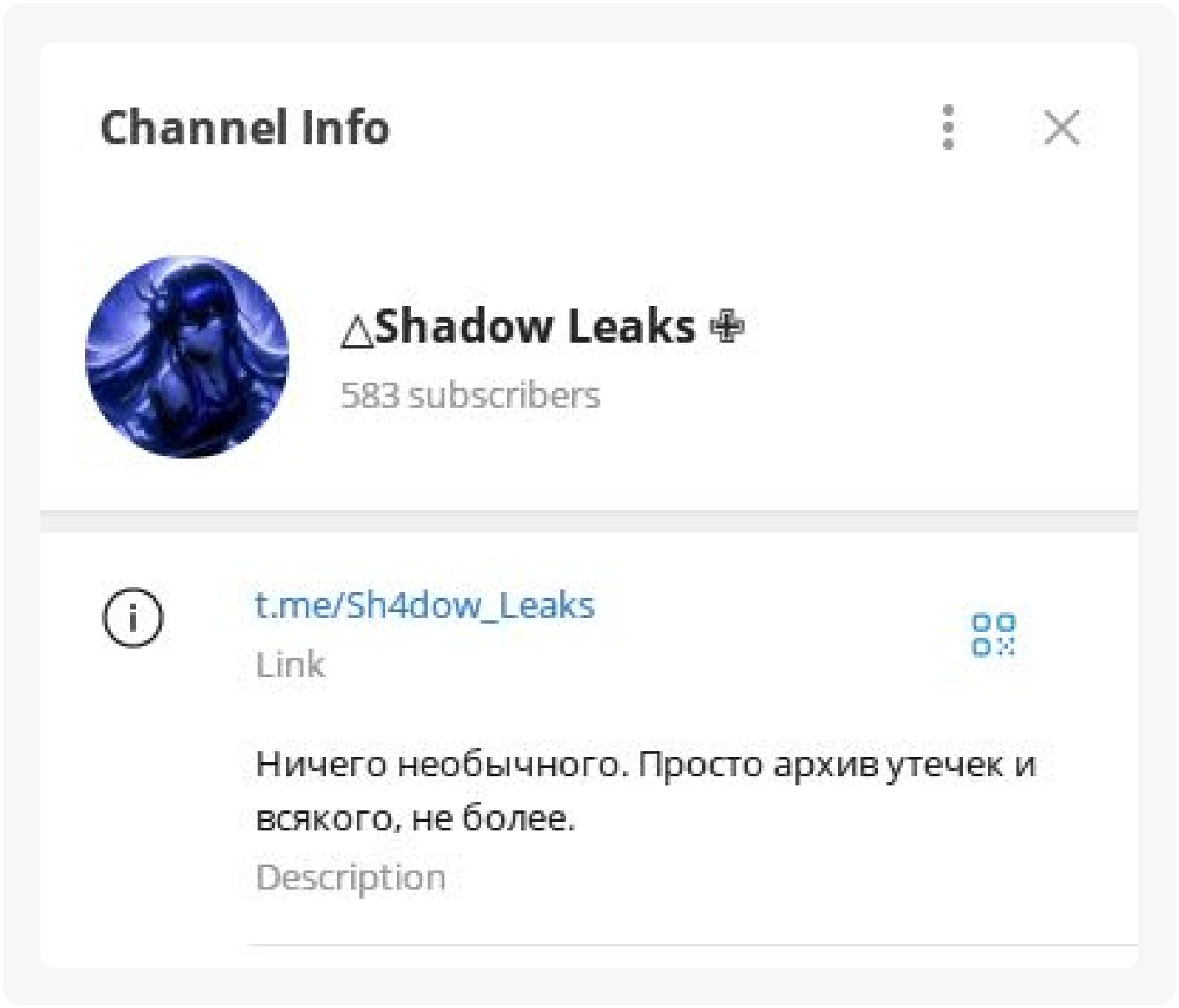


Рис. 18. Описание Telegram-канала злоумышленника

В своём Telegram-канале злоумышленник дублировал сообщения, опубликованные на андеграундном форуме, на случай, если темы будут удалены.

Sh4dow начал действовать на форуме 1 января 2024 года с продажи базы данных российского интернет-магазина товаров для маникюра и педикюра «ParisNail» (parisnail.ru). Всего за весь период активности злоумышленника в 2024 году специалистами Threat Intelligence было зафиксировано три случая продаж баз данных (с опубликованным образцом) и 45 случаев публикаций. Последнюю публикацию злоумышленник разместил 20 августа 2024 года, выложив в открытый доступ базу данных российского интернет-магазина фармацевтической продукции «Pharmacosmetica».

Petya152r5

Petya152r5 — злоумышленник, публиковавший базы данных на андеграундном форуме BreachForums с 25 января по 19 марта 2024 года. Скриншот профиля злоумышленника представлен ниже:

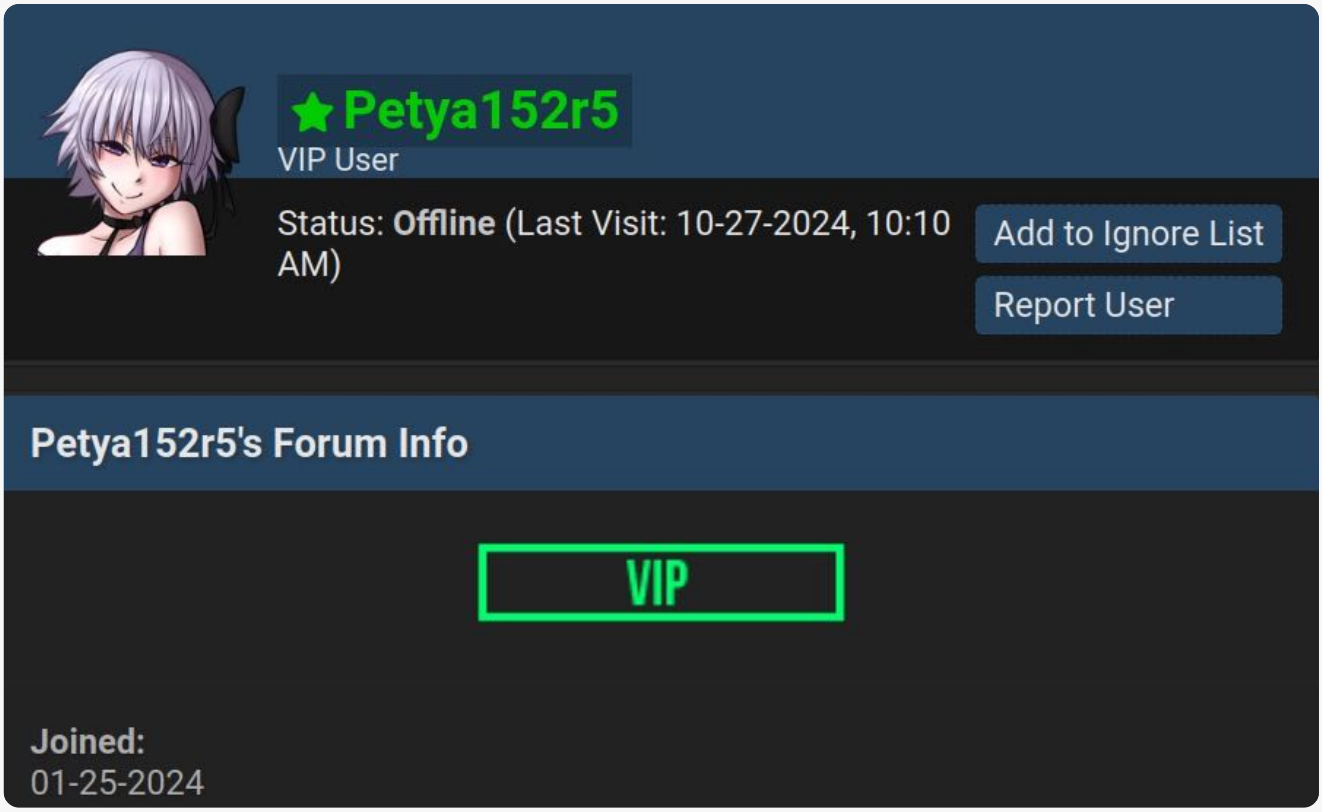


Рис. 19. Профиль злоумышленника на андеграундном форуме

Пользователь не имел никакой репутации на момент своей первой публикации на андеграундном форуме. Однако за 3 месяца своей активности он опубликовал в общей сложности 7 баз данных микрофинансовых организаций. Из них 4 — это базы данных сайтов российских организаций:

Публикации баз данных сайтов российских организаций

f6.ru

Наименование организаци	Кол-во строк
dengisrazy.ru	47 190 209
zaymer.ru	16 586 407
adengi.ru	6 697 534
qzaem.ru	3 816 319

За рассматриваемый период злоумышленником “Petya152r5” было опубликовано 74 290 469 строк персональных данных российских пользователей.

Других контактов на андеграундном форуме злоумышленник не указывал. Его публичная активность после публикации в марте базы данных «Деньги Сразу» прекратилась.

BadB

BadB — яркий представитель киберпреступности, занимался кардингом в 2000-х. Был одним из основателей известной кардинговой площадки CarderPlanet. С начала 2022 года активно занимается политической пропагандой в своем Telegram-канале под названием CyberSec’s, где публикует новостные сообщения, а также утечки баз данных.

Примечательно, что 17 сентября 2024 года злоумышленник создал отдельный Telegram-канал «BadB on the Base» для публикации баз данных.

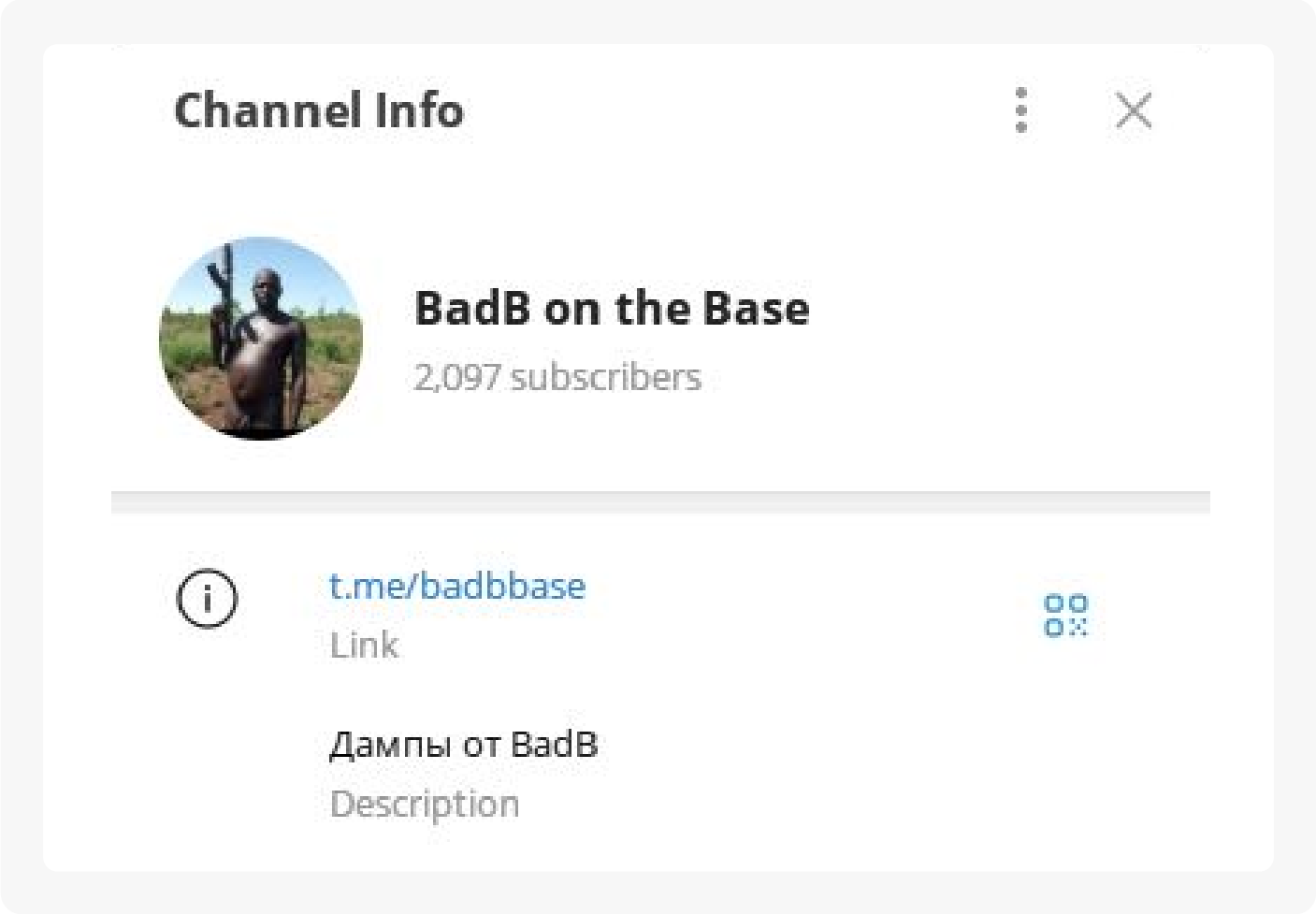


Рис. 20. Описание Telegram-канала злоумышленника

8 ноября 2024 года CyberSec’s заявили о взломе более 30 тысяч российских серверов на Битрикс. Также ими было опубликовано предложение об их продаже. В канале «BadB on the Base» злоумышленники активно публиковали базы данных, которые получили в результате взлома. С сентября по декабрь было опубликовано 22 базы данных различных российских сайтов.

Андеграунд

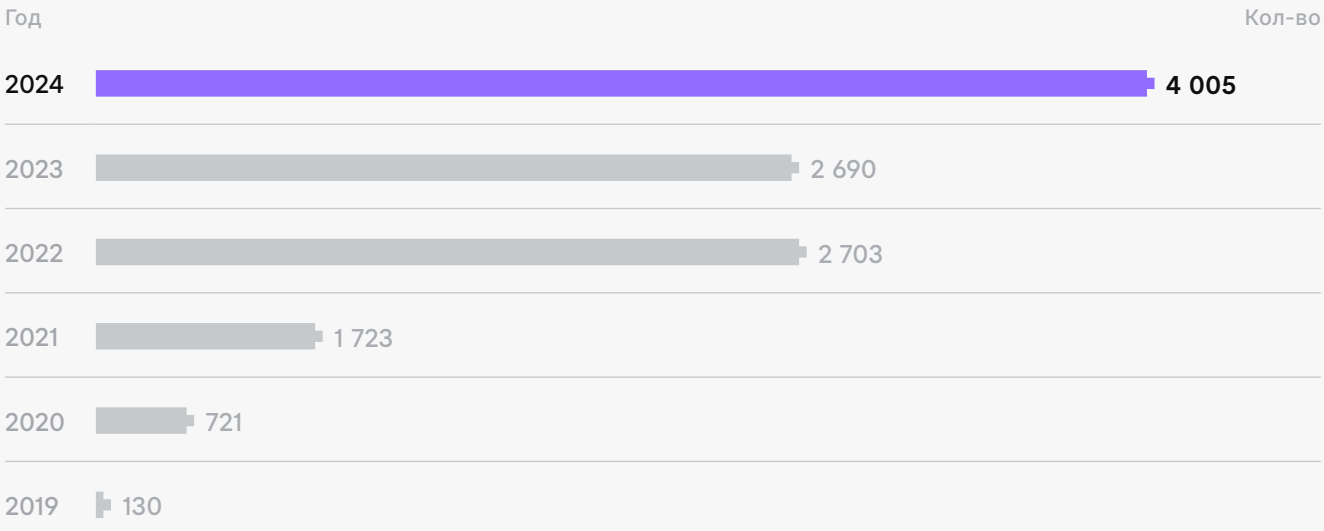
Продажи доступов в инфраструктуру компаний из стран СНГ

Продажи доступов, которые мы наблюдаем со стороны злоумышленников — это популярная практика, когда хакер получил доступ в корпоративную сеть, но далее предпочитает продать этот доступ вместо того, чтобы самостоятельно их монетизировать или использовать в дальнейшем. Услуги по продаже доступов крайне популярны у операторов программ-вымогателей — они активно сотрудничают с IAB (Initial Access Brocker-ами), покупая у них доступ в скомпрометированные корпоративные сети, а затем распространяя в них программы-шифровальщики с целью получения выкупа или преследуя какие-либо политические мотивы.

За последние 5 лет отмечается рост числа продаж доступов к корпоративным сетям компаний по всему миру. Причем нередко в рамках продажи одного лота злоумышленники предлагали набор доступов, состоящий от нескольких десятков до нескольких тысяч доступов, полученных при помощи различного вредоносного ПО.

Статистика продаж доступов по годам в виде количества лотов:

f6.ru

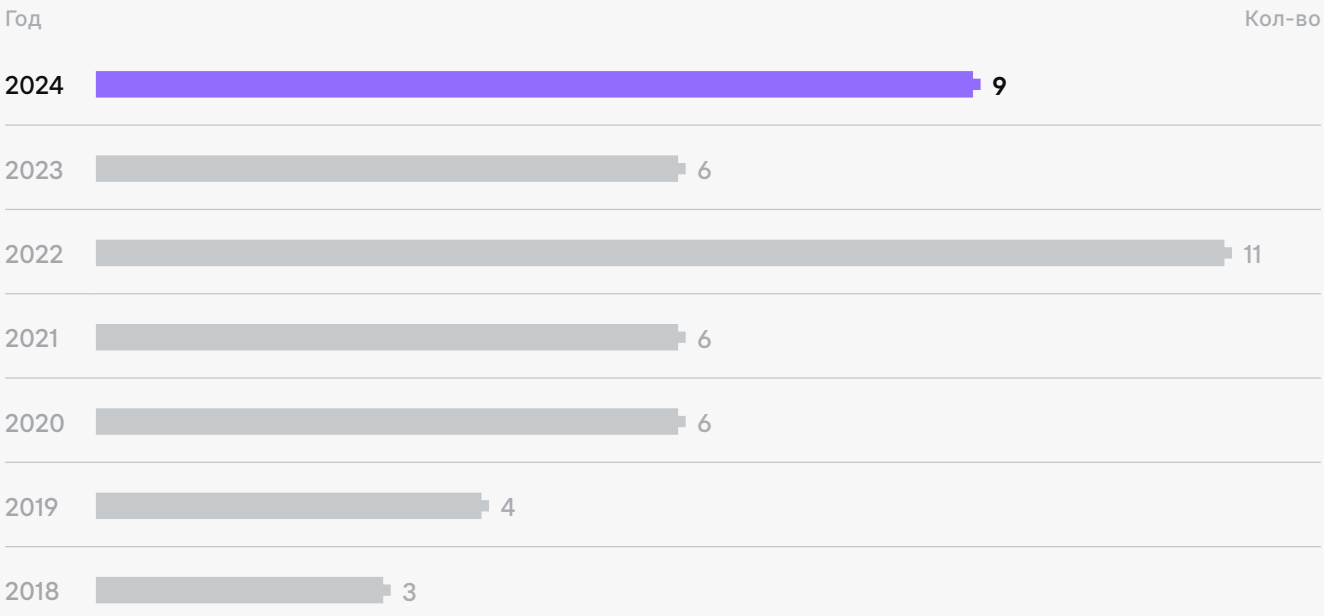


Популярность данной услуги связана с ростом популярности программ-шифровальщиков у злоумышленников в целом, а также роста количества политически-мотивированных киберпреступных группировок, активно использующих данный вид ВПО в своих атаках. При получении первоначального доступа злоумышленник может проводить сканирования внешнего периметра сети на наличие уязвимостей, открытых портов, а также, например, начать горизонтальное перемещение и, после повышение привилегий, получить доступ к управлению критически важными данными с целью нанести максимальные разрушения в работе систем.

Многие злоумышленники после получения доступа не стремятся далее его как-либо использовать. Вместо этого они предпочитают выставлять сам доступ на продажу на популярных андеграундных форумах, где его впоследствии могут приобрести любые пользователи, включая представителей той или иной киберпреступной группировки. Причина — в том, что нередко получение доступов в корпоративные сети становится «побочным продуктом» деятельности злоумышленника, например, при сборе логов с устройств, зараженных стилером.

Ранее на большинстве андеграундных площадок была полностью запрещена любая деятельность, направленная на Россию и страны СНГ. Однако после 24 февраля 2022 года в андеграунде все чаще начали встречаться объявления о продаже доступов к компаниям из данных регионов, в том числе и на известных русскоязычных площадках.

Статистика продаж доступов по годам для стран СНГ: f6.ru



Специалистами нашего подразделения Threat Intelligence за 2024 год было выявлено 9 доступов к компаниям из стран-членов СНГ, из них 5 доступов к российским компаниям, по 1 доступу к компаниям из Таджикистана, Азербайджана, Молдовы и один доступ к компании из неопределенной страны в составе СНГ. Необходимо указать, что не для всех продаваемых в андеграунде доступов возможно определить страну, а некоторые из них и вовсе могли продаваться приватно, поэтому реальное количество жертв в странах СНГ в действительности может быть существенно больше.

Многие злоумышленники стали активно искать на рынке доступов потенциальных партнёров и покупателей, из-за чего стали чаще выставлять на продажу доступы к российским компаниям, а также компаниям из СНГ.

Например, 19 апреля 2024 года злоумышленник p0inter выставил на продажу первоначальный доступ к одному из банков в Азербайджане. За $1 000 автор объявления предлагал приобрести учетные записи с различными правами доступов в домене компании.

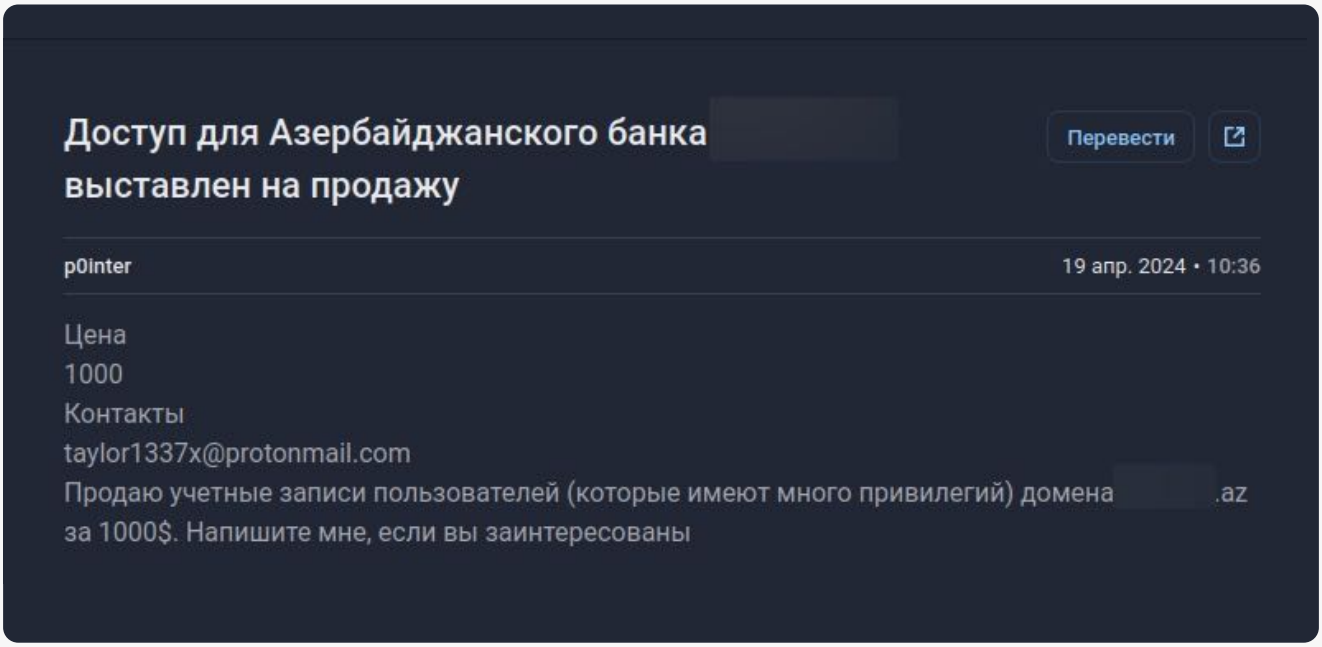


Рис. 21. Пример объявления о продаже доступа к банку в Азербайджане

Позже, 31 июля 2024 года, злоумышленник с псевдонимом zjdue123 разместил на форуме XSS объявление о продаже доступа во внутреннюю корпоративную сеть неизвестной компании, расположенной в одной из крупных стран СНГ.

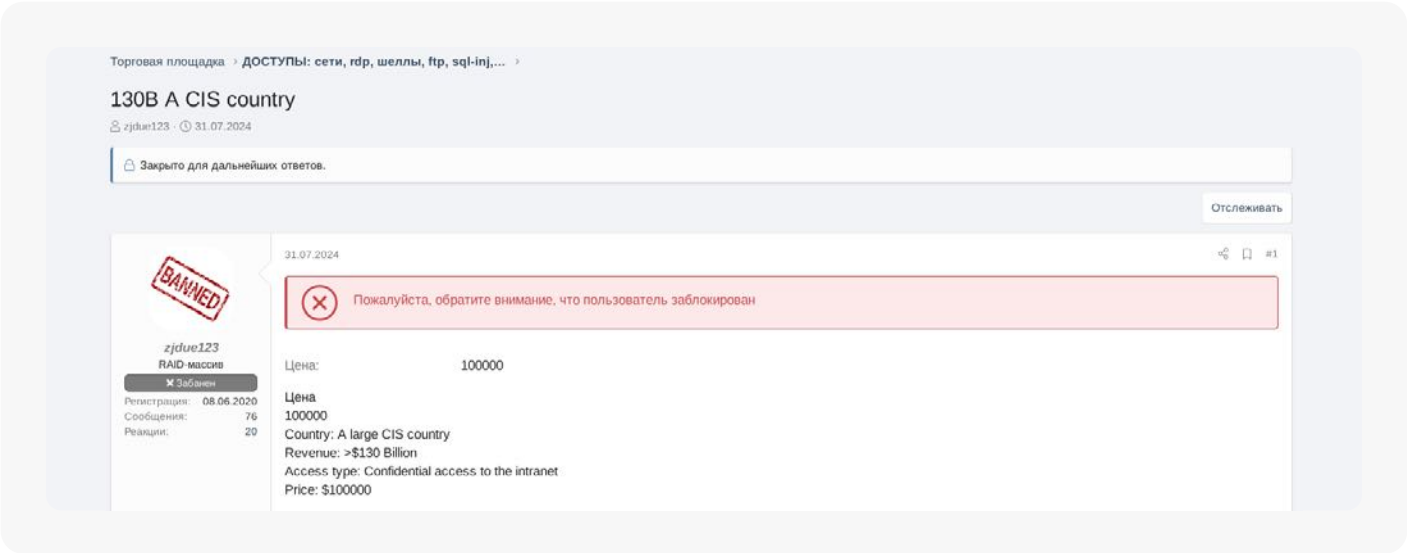


Рис. 22. Пример объявления о продаже доступа в корпоративную сеть неизвестной компании

Продавец указал, что выручка компании составляет более $130 миллиардов, а стоимость такого доступа составляет $100 000.

zjdue123 не предоставил никаких дополнительных деталей о продаваемом доступе, а позже, в этот же день, и вовсе снял доступ с продажи ввиду нарушения правила торговой площадки — не осуществлять киберпреступную деятельность в отношении России.

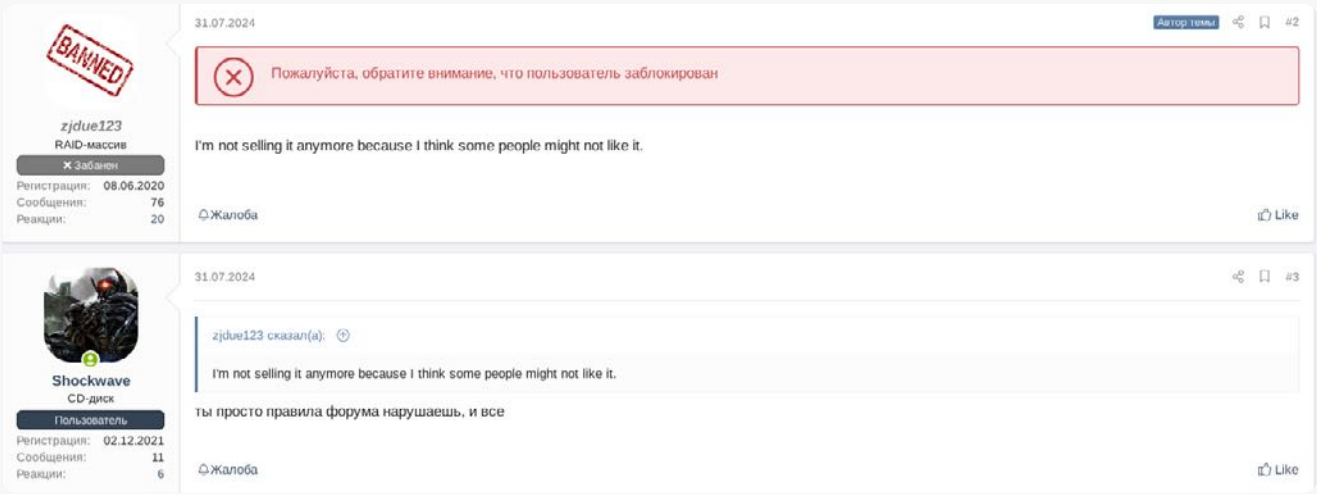


Рис. 23. Сообщения злоумышленников на андеграундном форуме

В настоящий момент автор заблокирован администрацией форума XSS.

Запреты на форумах, касающиеся работы злоумышленников по определенным странам, также распространяются и на те страны, которые вышли из состава СНГ. В 2024 году было зафиксировано несколько подобных продаж доступов. Например, alexalexisgan 2 января 2024 года выставил на продажу архив, содержащий в себе VNC-доступы к компаниям из разных стран, включая Украину. Позже автор был заблокирован андеграундном форуме XSS за работу по экс-странам СНГ.

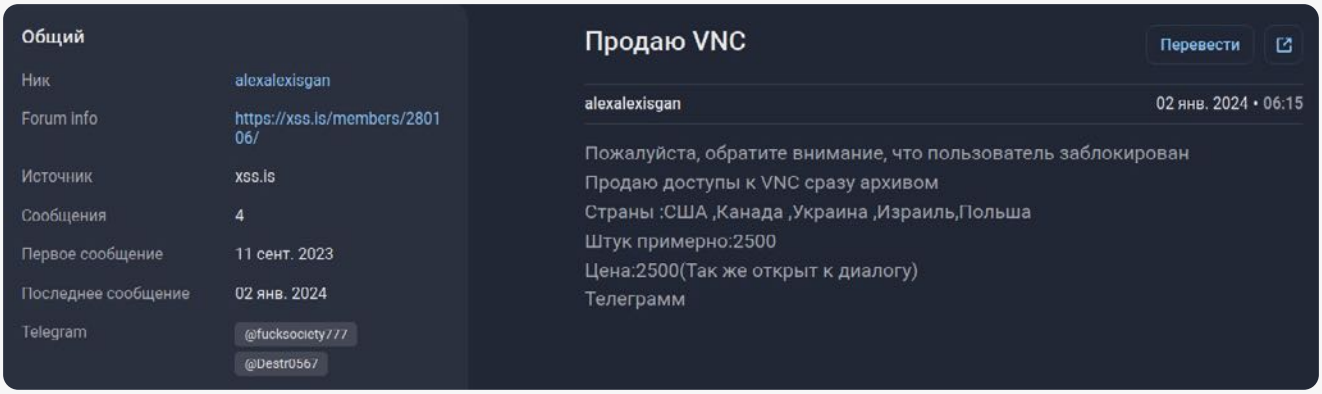


Рис. 24. Пример объявления о продаже VNC-доступов

Еще один доступ был выставлен на продажу 14 августа 2024 года пользователем kiberphant0m. Злоумышленник опубликовал объявление о продаже доступа к серверу одной из правительственных организаций Украины на форумах Exploit и XSS, но вскоре был заблокирован за нарушение правил работы форумов, а его темы были удалены администрацией.

Скриншот сообщения из системы Threat Intelligence представлен ниже:

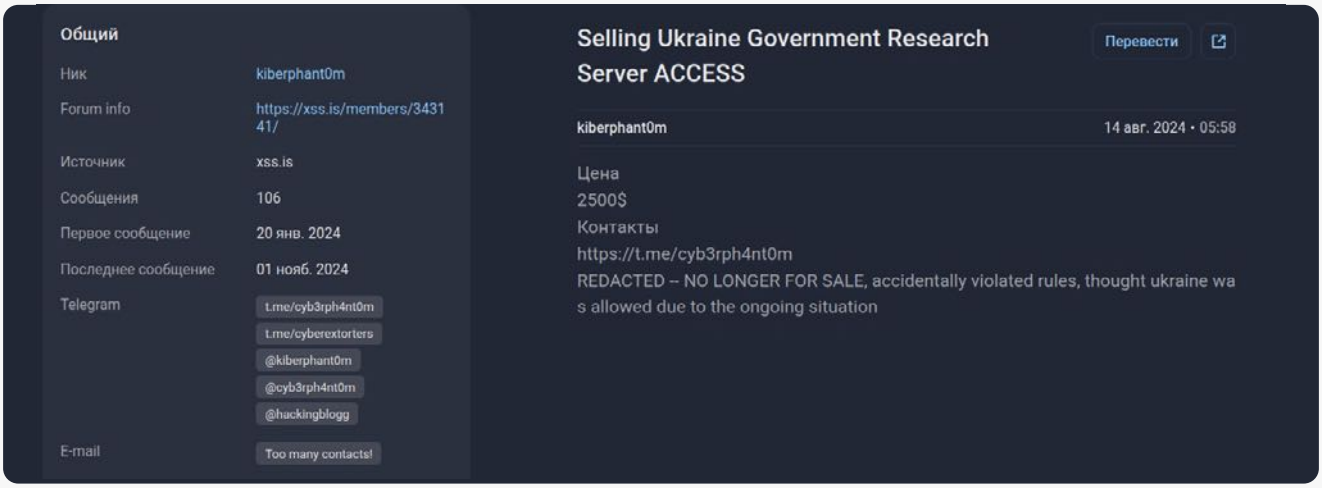


Рис. 25. Скриншот сообщения из системы Threat Intelligence

Несмотря на то, что вскоре тему закрыли за нарушение правил работы на форуме, автор дополнил объявление, что якобы ввиду текущей политической ситуации он считал, что могли быть пересмотрены и ограничения площадки на продажи доступов в данном регионе.

Довольно часто на даркнет-площадках публикуют объявления о продажах доступов в панели управления различных сайтов. Это связано с тем, что для получения подобного доступа в большинстве случаев не требуется реализация сложных атак, так как злоумышленники ограничиваются в основном такими атаками, как поиск и эксплуатация SQL-инъекций, получение данных для входа в аккаунты с логов вредоносного ПО или из других источников.

6 октября 2024 года zerTax создал тему на форуме XSS о продаже доступа к панели управления одного из российских сайтов. Вскоре и тему, и автора объявления заблокировали за нарушение.

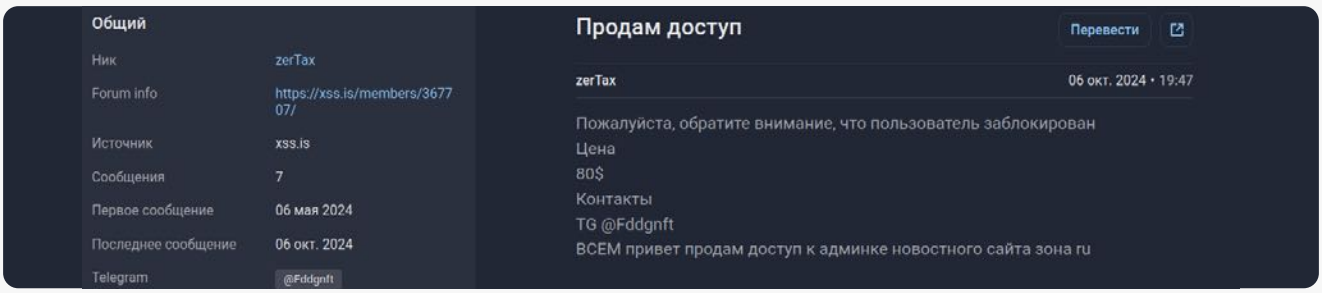


Рис. 26. Пример объявления о продаже доступа к панели управления одного из российских сайтов

19 октября 2024 года злоумышленник TERM1NATOR выставил на продажу доступ к панели управления сайта банка в Таджикистане.

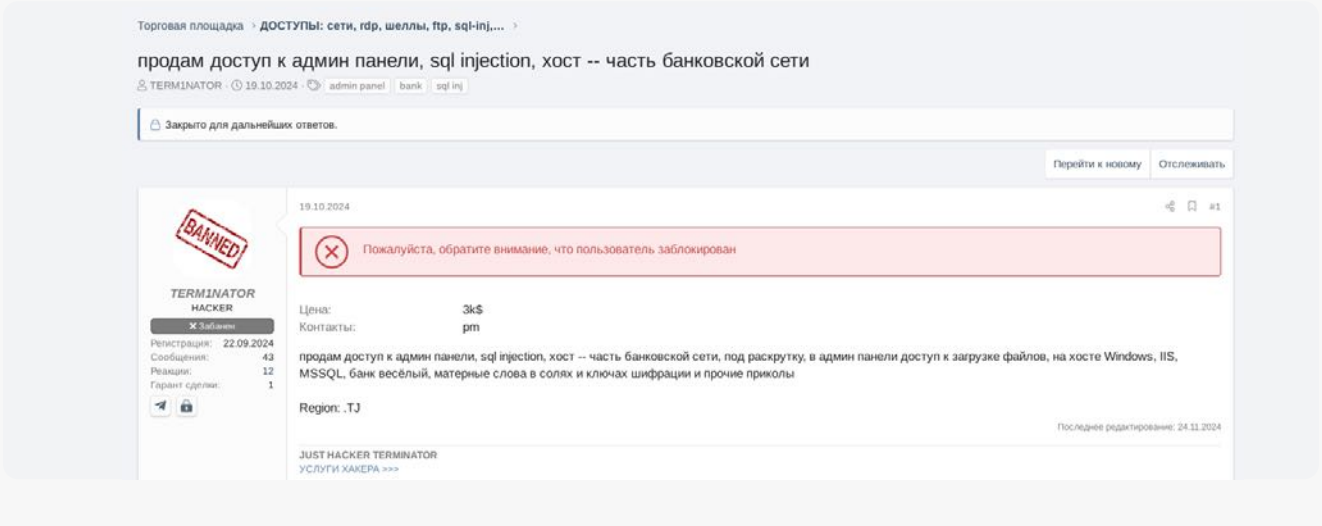


Рис. 27. Пример объявления о продаже доступа к панели управления сайта банка в Таджикистане

Автор был заблокирован модератором за работу по СНГ.

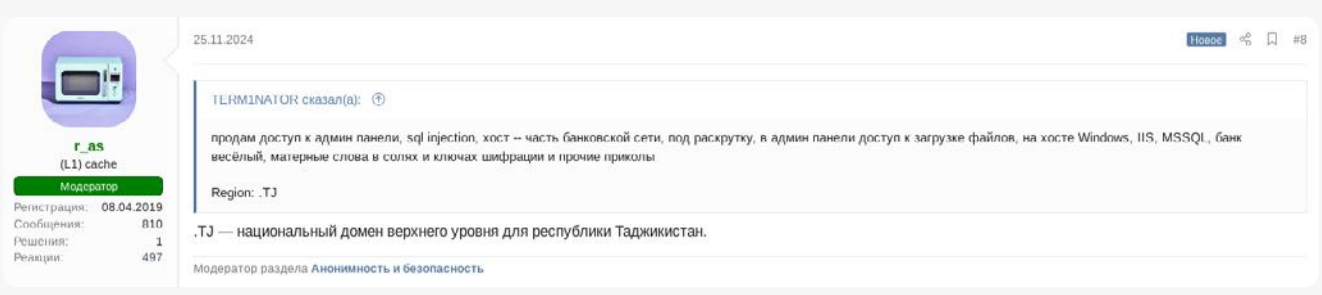


Рис. 28. Сообщение модератора на форуме

Модератор отметил в комментарии, что прямая работа по странам СНГ, а также по тем, которые больше не входят в содружество, запрещена. Однако правила форума не ограничивают продажу наборов данных (так называемых «миксов»), содержащих информацию из разных стран, включая доступы к компаниям из СНГ.

Рис. 29. Сообщение модератора на форуме

27 ноября 2024 года еще один из пользователей форума XSS под псевдонимом U3701 опубликовал сообщение о продаже доступа к сайту и серверу организации из Молдовы.

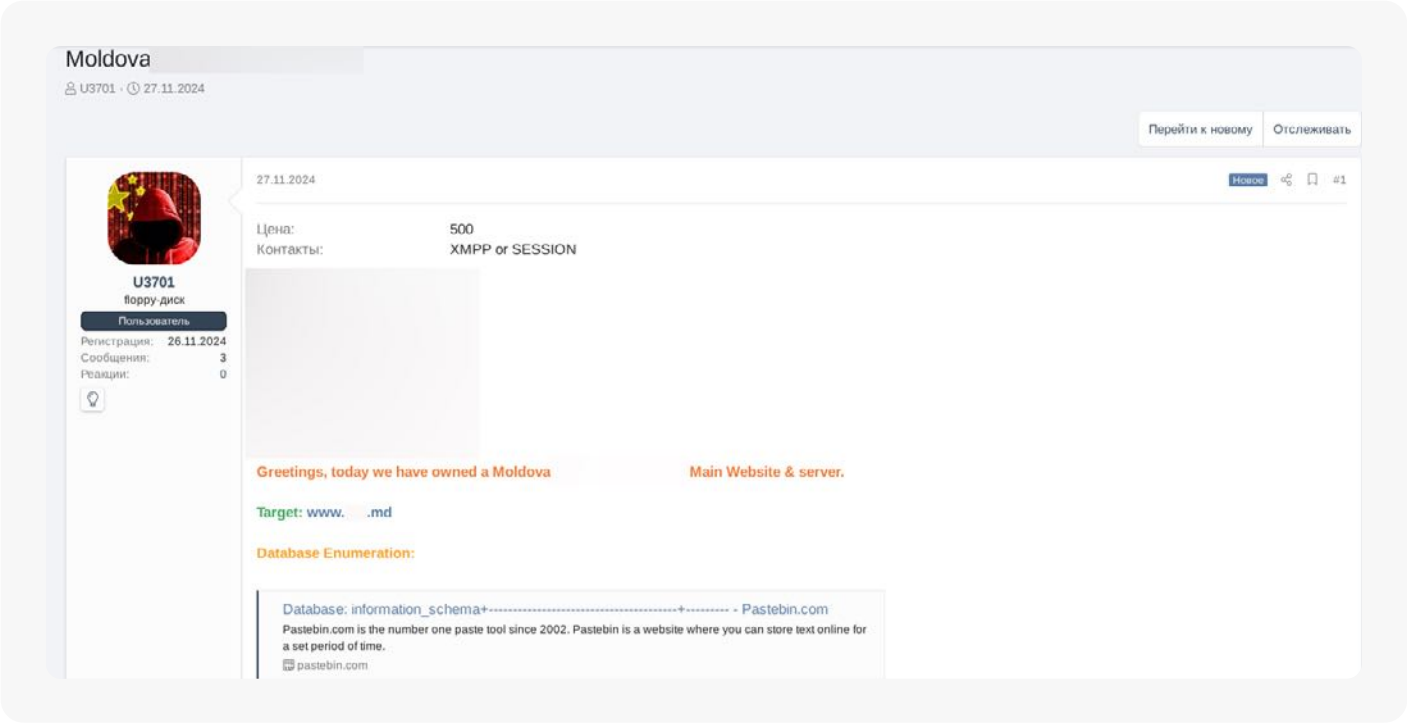


Рис. 30. Пример объявления о продаже доступа к сайту и серверу организации из Молдовы

Как уже отмечалось ранее, любая андеграундная площадка представляет собой сообщество пользователей, преследующих те или иные цели, постоянно коммуницирующих между собой. Для каждого вида товаров или услуг существует своя ниша «целевого потребителя» на различных ресурсах.

Примечательно то, что из-за запрета на работу по России и странам СНГ многие киберпреступники, заинтересованные в таких услугах, начали переходить на другие андеграундные площадки, где подобные ограничения условные, отсутствуют или же, наоборот, эта активность всячески поощряются.

Примером одной из таких площадок является популярный андеграундный ресурс — Breachforums. Помимо финансово-мотивированных злоумышленников на площадке ведут активную деятельность и представители различных политически-мотивированных хакерских групп, выкупая первоначальные доступы и данные целевых компаний в регионах своей активности.

Одно из таких объявлений было создано 22 ноября 2024 года злоумышленником под псевдонимом RussianCitizen. В тексте указывалось, что злоумышленник продавал доступ к серверам крупного агентства недвижимости, находящегося в Москве.

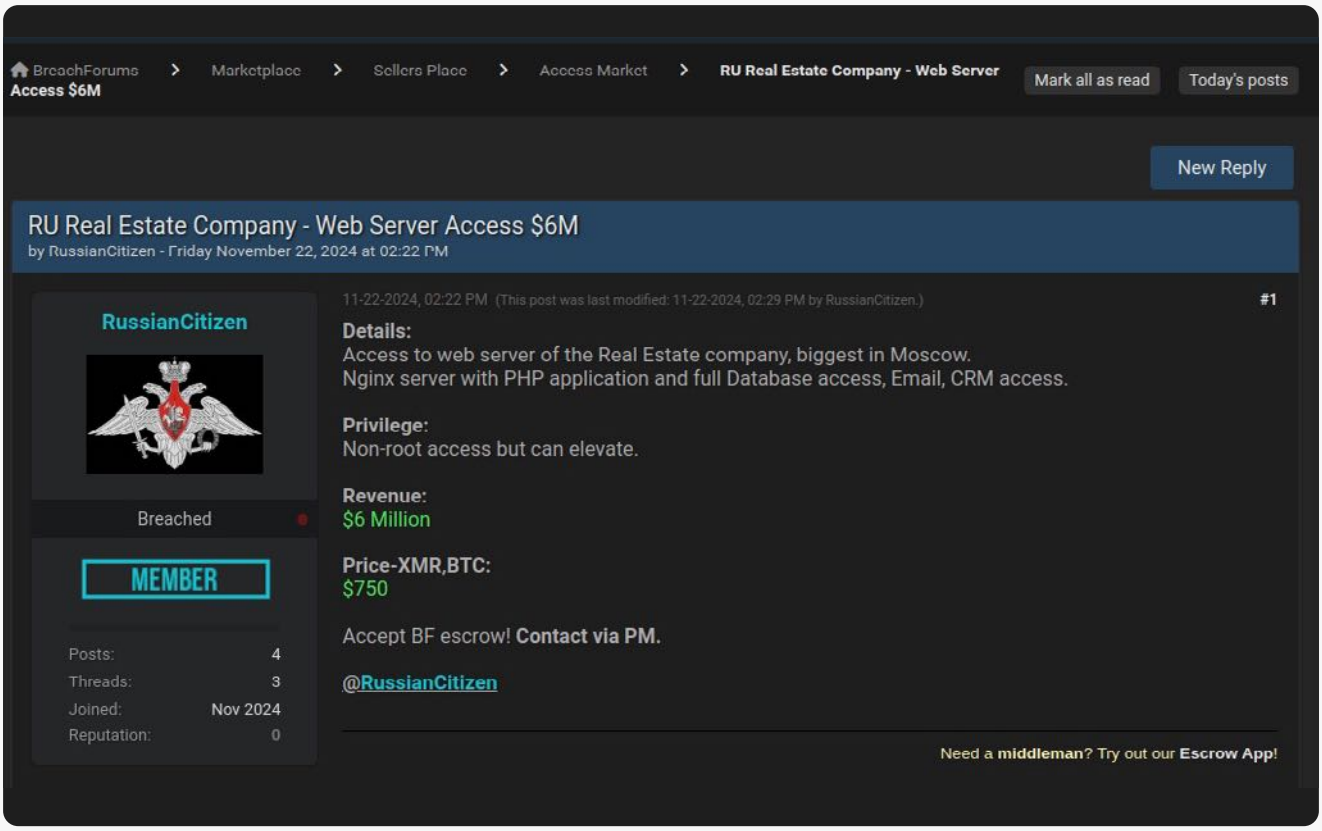


Рис. 31. Пример объявления о продаже доступа к серверам российской компании

Стоит отметить, что данный пользователь был зарегистрирован всего за пару дней до создания своего объявления. Судя по его активности, а также общему профилю на форуме, можно сделать вывод, что данный злоумышленник целенаправленно действует для привлечения потенциальных покупателей из рядов политически-мотивированных киберпреступников, заинтересованных в атаках на российские компании.

11 сентября 2024 года злоумышленник Lista также опубликовал на Breachforums объявление о продаже SSH-доступа к серверу, якобы принадлежащему российской страховой компании.

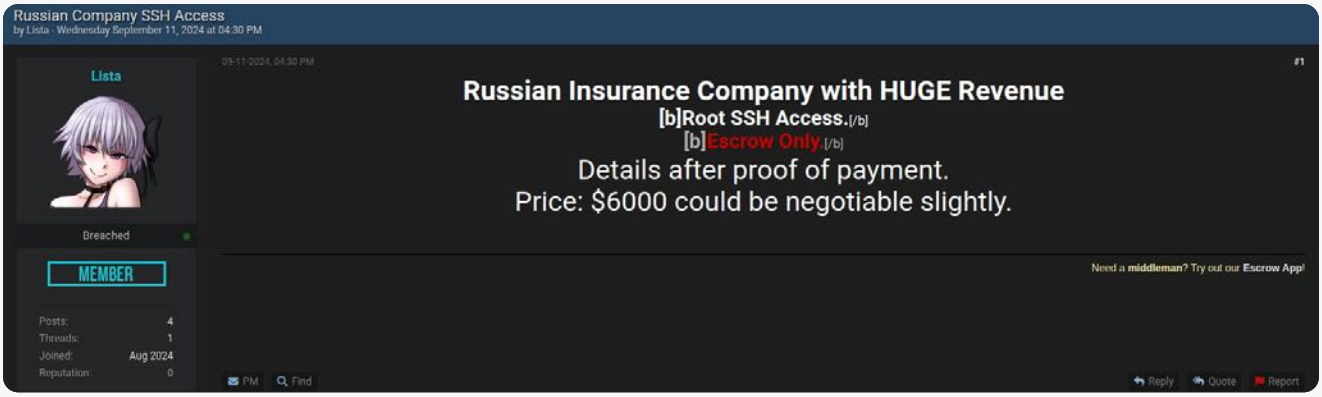


Рис. 32. Пример объявления о продаже SSH-доступа к серверу российской компании

Наши аналитики в рамках исследования выяснили, что данный злоумышленник действовал под разными псевдонимами, в том числе и на форумах, где запрещена работа по России и СНГ. Большинство его профилей было заблокировано на площадках за мошенничество, поэтому надежность подобного объявления весьма сомнительна. Однако сам факт того, что злоумышленник перешел на тот форум, где каких-либо строгих политических запретов нет, может свидетельствовать о потенциальном увеличении на указанном форуме активности хакеров, атакующих Россию и страны СНГ.

Другим примером андеграундного форума является Dumpforums, принадлежащий одноименной группе проукраинских хакеров. В отличие от прочих даркнет-площадок, данный ресурс «заточен» на причинение ущерба любым российским компаниям, а также компаниям из стран, сотрудничающих с организациями из России.

Практически вся информация, публикуемая на данном ресурсе, представляет собой скомпрометированные базы данных российских пользователей, продажи первоначальных доступов или другую информацию, полученную в результате атак на ту или иную организацию.

Например, 5 октября 2024 года злоумышленник alekimano создал на Dumpforums тему о продаже SSH-доступа с уровнем привилегий администратора к серверам крупной сети аптек, на которых также находилась база данных **1 200 000 пользователей**.

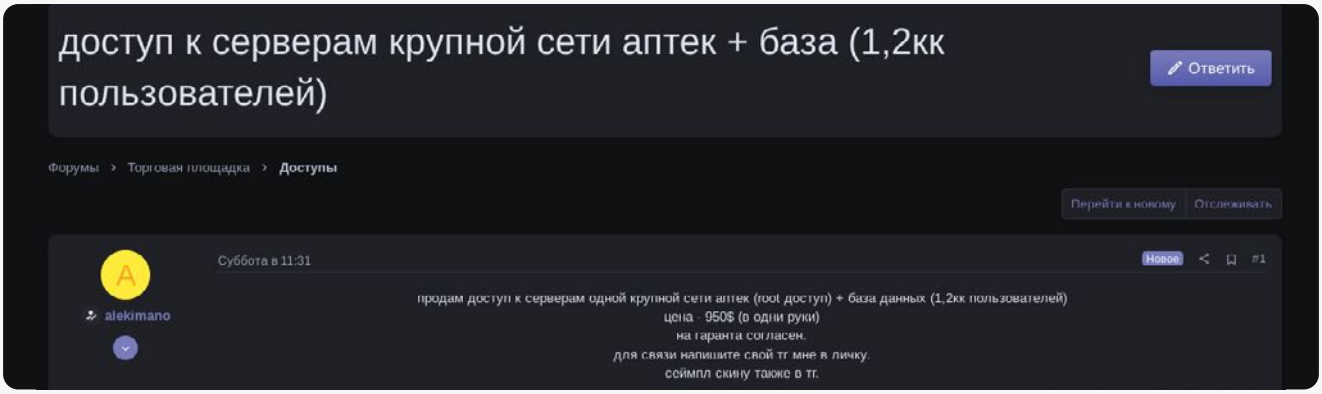


Рис. 33. Пример объявления о продаже доступа к серверам сети аптек

Позже, 28 октября 2024 года, еще один пользователь под псевдонимом Pers0na выставил на продажу на данной площадке доступ к различным компаниям из России. По его словам, он целенаправленно атакует именно российские компании и не имеет доступов к организациям из других стран.

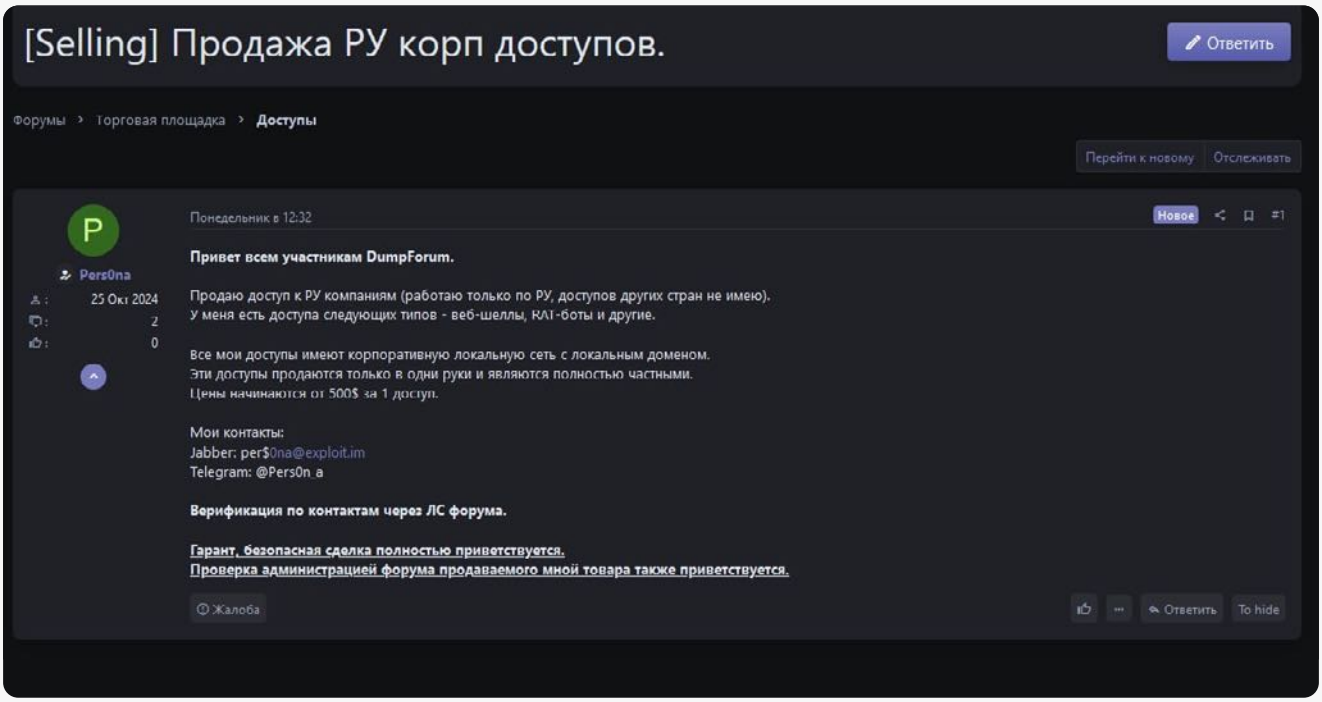


Рис. 34. Пример объявления о продаже доступов к различным компаниям

Специалисты нашего подразделения Threat Intelligence связались с злоумышленником для уточнения деталей. По его словам, он обладает постоянным доступом к российским организациям — от юридических фирм в Санкт-Петербурге до крупных фармацевтических компаний. Однако точное количество доступов он не раскрыл. Кроме того, злоумышленник утверждает, что периодически получает новые доступы к организациям.

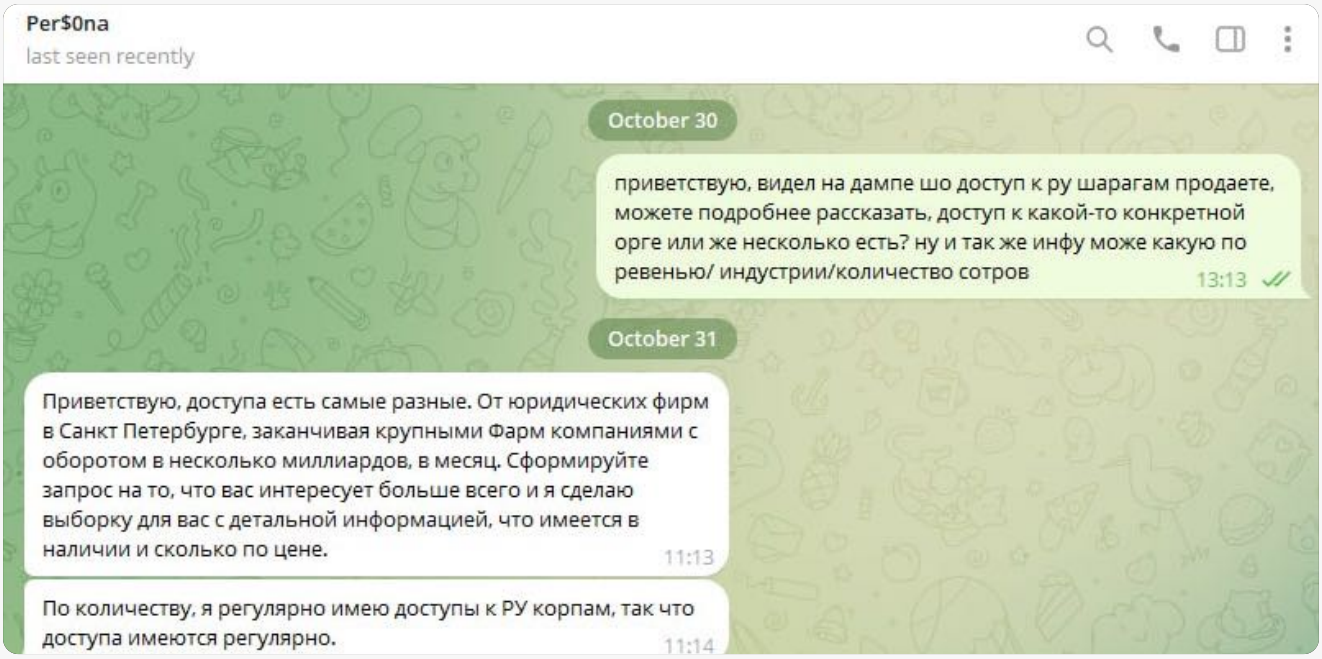


Рис. 35. Информация, предоставленная злоумышленником в переписке

Публикация доступов в инфраструктуру компаний из стран СНГ

Глава 5. Андеграунд

Помимо продаж доступов, некоторые пользователи форумов могут выкладывать данные в свободном доступе. Это возможно по нескольким причинам: автор не смог продать полученный доступ каким-либо доступным способом, либо не заинтересован в дальнейшем использовании полученной скомпрометированной информации.

Пример такой активности был замечен на форуме XSS, где пользователь Lupin опубликовал список аутентификационных данных для подключения к удаленному рабочему столу посредством протоколов Citrix, RDWeb, GlobalProtect и прочим протоколам удаленного доступа.

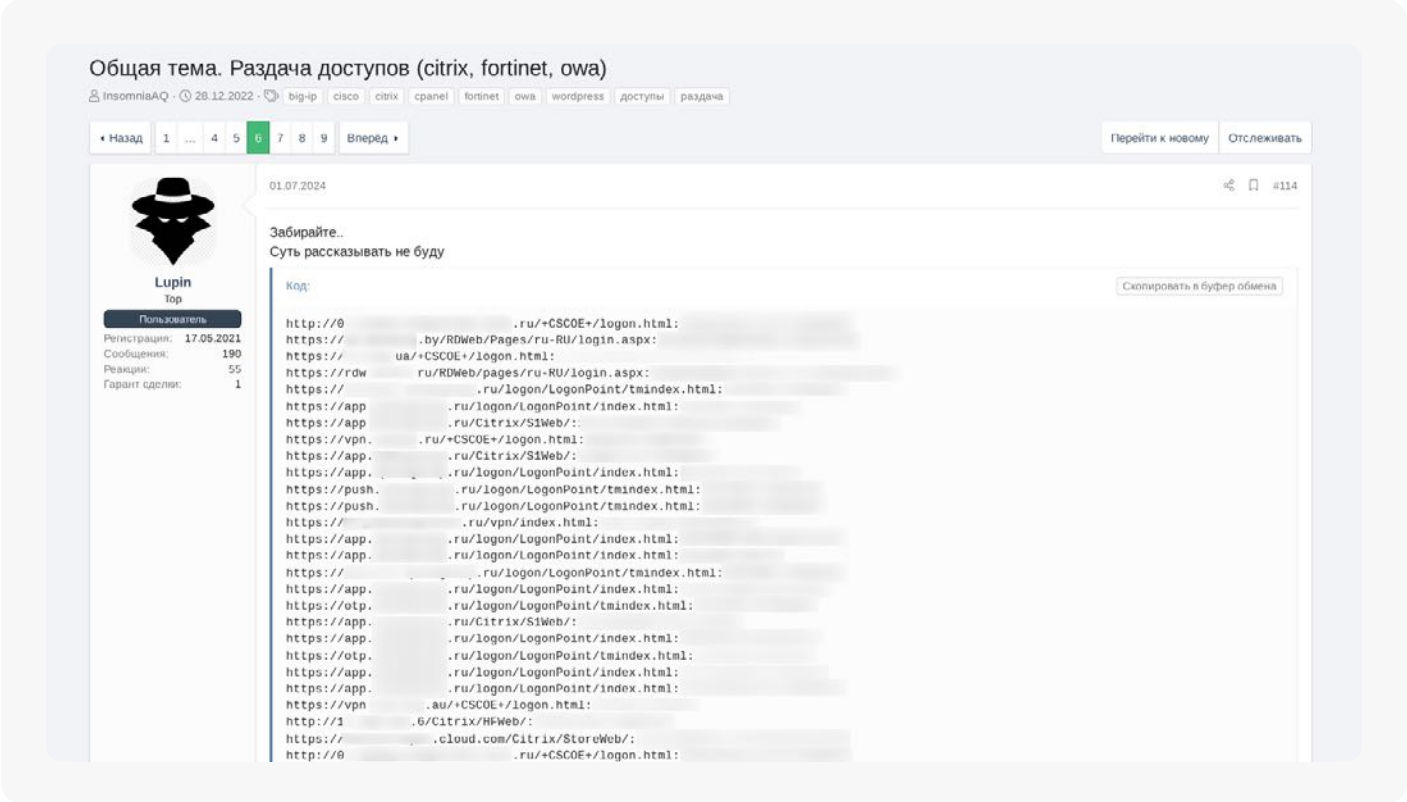


Рис. 36. Раздача доступов к различным компаниям

В опубликованном списке было представлено 22 доступа к компаниям из стран-участников СНГ, из них 21 доступ принадлежит пользователям из российских компаний, 1 — к компании из Беларуси, а также к 1 компании из Украины.

Автор указал, что не проверял данные на принадлежность к той или иной стране, поэтому выложил их общим списком, чтобы не нарушать правила андеграундного форума.

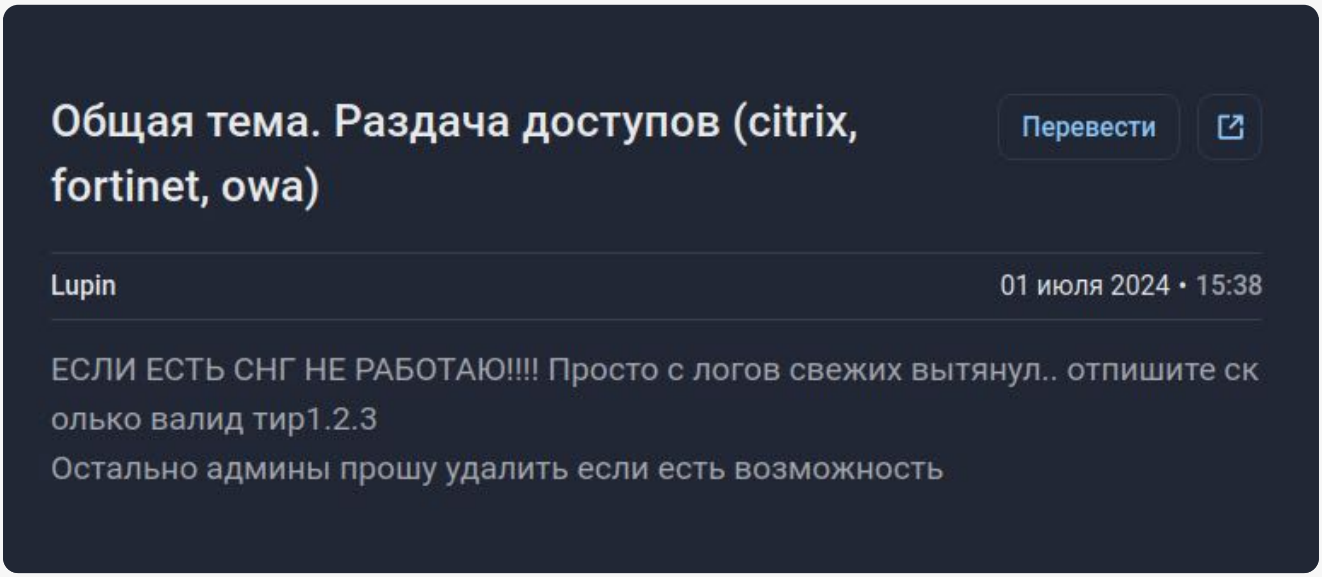
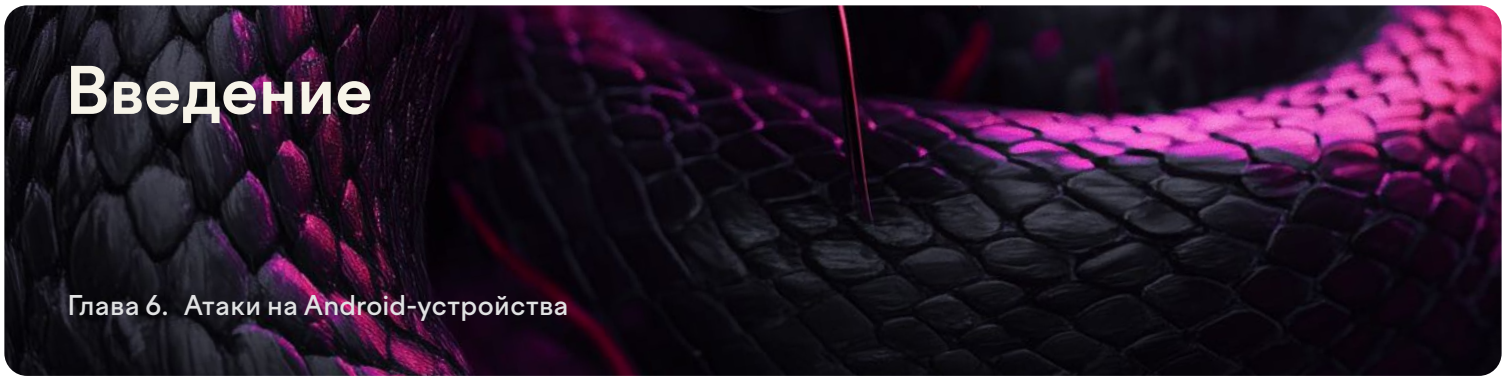


Рис. 37. Раздача доступов к различным компаниям

Данная ситуация может косвенно свидетельствовать о возможной ротации членов андеграундных сообществ, поддерживающих киберпреступные цели. Это, в свою очередь, может потенциально повлечь за собой как частичное, так и полное снятие каких-либо ограничений в работе по странам СНГ, а также создание новых политически-мотивированных андеграундных форумов.

Атаки на Android-устройства



Введение

Глава 6. Атаки на Android-устройства

В 2024 году мы наблюдали всплеск мошеннической и вредоносной активности с использованием атак на пользователей Android. Мы выделили несколько преступных групп в этой категории. Общим для них является маскировка ВПО под легитимные приложения. Процесс заражения в большинстве случаев происходит с использованием приёмов социальной инженерии.

Атаки на Android-устройства остаются одной из крупнейших угроз в сфере мобильной безопасности, поскольку эта операционная система имеет широкое распространение, а её уязвимости привлекают злоумышленников. С ростом популярности мобильных устройств хакеры продолжают развивать новые методы атак, включая использование вредоносных приложений, фишинг и социальную инженерию.

Основным способом распространения вредоносных программ на Android являются фишинговые сообщения, которые побуждают пользователей скачать под видом обновлений популярных приложений заражённые APK-файлы. Этот метод особенно эффективен в связи с отсутствием строгих мер по проверке приложений вне официальных магазинов, таких как Google Play. Также широко используются уязвимости в приложениях, которые позволяют получать удалённый доступ к устройствам и извлекать персональные данные, такие как пароли, SMS, истории звонков и список контактов.

Многие злоумышленники работают по схеме «Мамонт». Такие группы предоставляют доступ к своему сервису через боты в Telegram. Сервисы предоставляют возможность заниматься киберпреступностью и похищать денежные средства жертв, не имея технических навыков. ВПО для Android предоставляется бесплатно и буквально в пару кликов в виде APK, замаскированного под легитимное приложение, либо ссылки на скачивание APK с фейкового сайта, созданного операторами сервиса. Под каждое легитимное приложение или сайт злоумышленники разработали рекомендации (сценарии), как обманом заставить жертву перейти по ссылке, скачать APK и так далее. ВПО для Android, используемое группами, предназначено для получения доступа к СМС жертвы. Операторы сервиса, получая доступ к СМС, могут похитить средства с банковских счетов, оформить кредиты и так далее. Затем они отдают процент от украденных средств своим пользователям «воркерам».

CraxsRAT

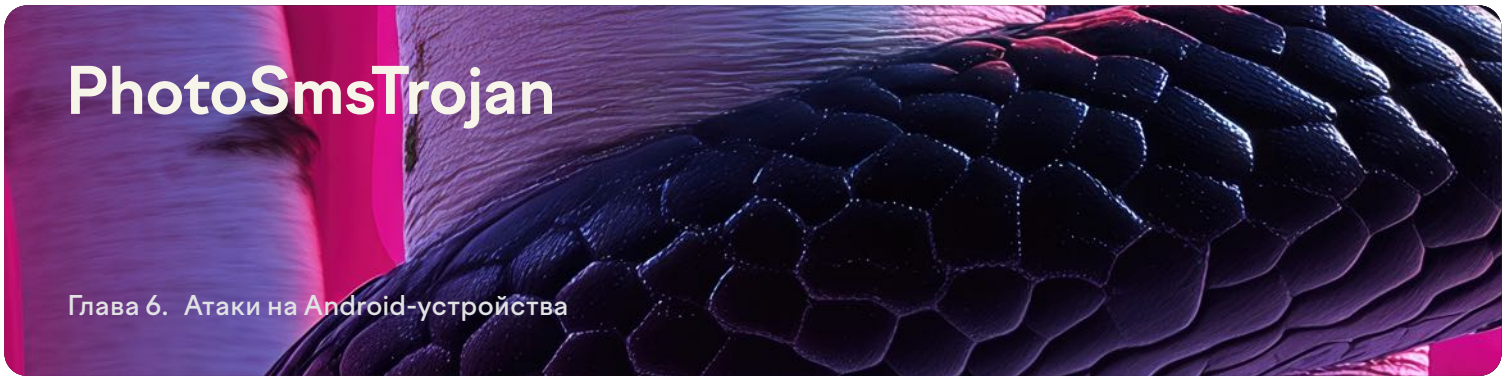
С лета 2024 года наши специалисты начали фиксировать многочисленные атаки на владельцев Android-устройств в России и Беларуси с использованием вредоносного программного обеспечения CraxsRAT. Этот многофункциональный Android-троян основан на исходных кодах SpyNote и был разработан автором с псевдонимом EVLF DEV. В ходе исследований было выявлено более 140 уникальных образцов CraxsRAT. Атаки, вероятно, развиваются через социальную инженерию: злоумышленники предлагают пользователям через мессенджеры, такие как WhatsApp, скачать вредоносные APK-файлы, мимикрирующие под легитимные обновления приложений. Часто эти фейковые приложения имитируют антивирусное ПО, операторов связи, сервисы государственных и информационно-справочных услуг, например, Госуслуги, Минздрав, Минцифры России, Центральный банк РФ и др

Функциональные возможности CraxsRAT v6.7:

- получение информации об устройстве;
- закрепление в системе;
- управление файловой системой телефона;
- извлечение списка контактов и отправка им сообщений;
- извлечение и отправка SMS;
- отслеживание и запись звонков;
- отслеживание GPS;
- перехват 2FA;
- перехват нажатий и отображаемых событий;
- запись звонков и звука с микрофона;
- управление камерой;
- выполнение звонков на указанный номер;
- создание скриншотов экрана;
- даленное управление экраном устройства;
- выполнение сценариев кликов и вставки текста на устройстве;
- отображение уведомлений-приманок;
- перехват логинов, паролей и файлов cookie сайтов;
- установка произвольных дополнительных приложений;
- установка VPN и запрет выхода в сеть определенным приложениям;
- отслеживание запуска и остановки определенных приложений;
- запрет запуска определенных приложений;
- удаленная очистка устройства.

Вредоносное ПО маскируется под легитимные приложения, что значительно повышает его эффективность в атаках, используя доверие пользователей к известным сервисам. Исследования показывают, что CraxsRAT представляет серьёзную угрозу для Android-устройств, так как обладает множеством механизмов обхода защитных систем, что затрудняет его обнаружение. В дальнейшем можно ожидать, что CraxsRAT будет развиваться, улучшая свои возможности и методы обхода защиты.

Рис. 38. Административная панель CraxsRAT



PhotoSmsTrojan

PhotoAndroidMalware — ВПО типа RAT, появившееся как минимум в 2024 году. Предназначен для кражи данных и обработки SMS, уведомлений, а также выполнения денежных переводов с помощью SMS на номер 900. Данная вредоносная программа массово распространяется в Telegram под видом фотографий.

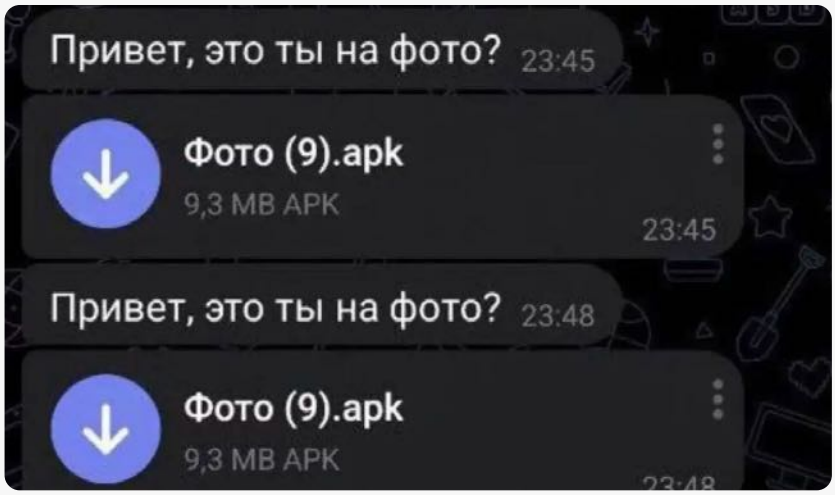


Рис. 39. Пример распространения ВПО PhotoSmsTrojan

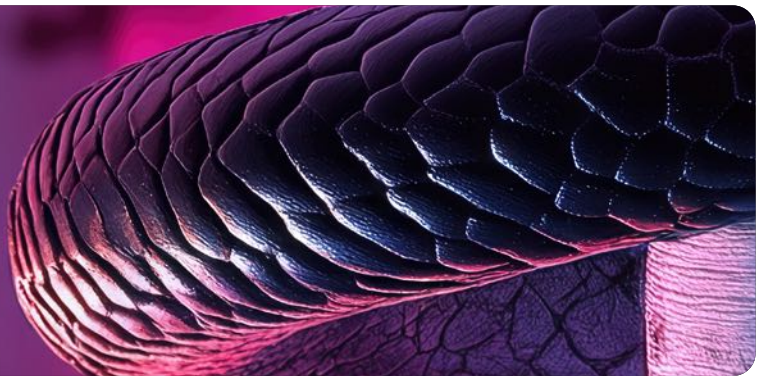
Функциональные возможности ВПО:

- эксфильтрация SMS;
- эксфильтрация и сокрытие push-уведомлений;
- отправка SMS (может также использоваться для выполнения команд на номер 900);
- эксфильтрация информации об устройстве (номера телефонов, модель сборки, SDK устройства);
- отображение произвольных URL-ссылок через WebView.

Приложение выполняет обработку SMS и уведомлений на предмет поиска интересующих его данных:

- SMS с номера 900 (Сбер);
- PIN-код от DC Wallet;
- Koronapay-переводы;
- подтверждение платежей в случае, если SMS было отправлено с номера нескольких мобильных операторов.

NFCGateCIS



NFCGateCIS — новое оружие злоумышленников, которое с конца 2024 года используется для атак, применяя ВПО для Android и NFC-чип для кражи средств у жертв. Вредоносное приложение основано на проекте с открытым исходным кодом NFCGate, предназначенном для анализа и модификации NFC-трафика. Его можно использовать в качестве исследовательского инструмента для реверса или оценки безопасности протоколов. Итоговая цель злоумышленников — добиться того, чтобы жертва с установленным ВПО на мобильном устройстве приложила свою банковскую карту к телефону и ввела PIN-код. Используя NfcData (для клонирования тега), данные карты и PIN-код, злоумышленники могут снять денежные средства в банкоматах.

Исследователи F6 обнаружили, что злоумышленники создали более 100 модификаций NFCGate, маскируя их под популярные приложения, такие как «Госуслуги» и сервисы Федеральной налоговой службы. Например, одна из модификаций полностью имитировала интерфейс приложения «Госуслуги», предлагая пользователю ввести данные банковской карты и PIN-код под предлогом «верификации». Другие приложения представлялись официальными сервисами Центрального банка или платежными приложениями, такими как MirPay. Эти вредоносные версии скрывали уведомления, подменяли интерфейс и автоматически отправляли данные на серверы злоумышленников.

Благодаря глубокому анализу серверной инфраструктуры эксперты F6 получили доступ к коду вредоносных приложений и серверов. В рамках исследования были выявлены таблицы баз данных, хранящие украденные данные банковских карт, PIN-коды, а также сведения о местоположении жертв. Обнаружены и системы автоматической сборки вредоносных APK-файлов, что указывает на существование модели «Malware-as-a-Service». Это позволяет злоумышленникам легко адаптировать приложения под конкретные цели и распределять жертв между различными группами.

BONVI

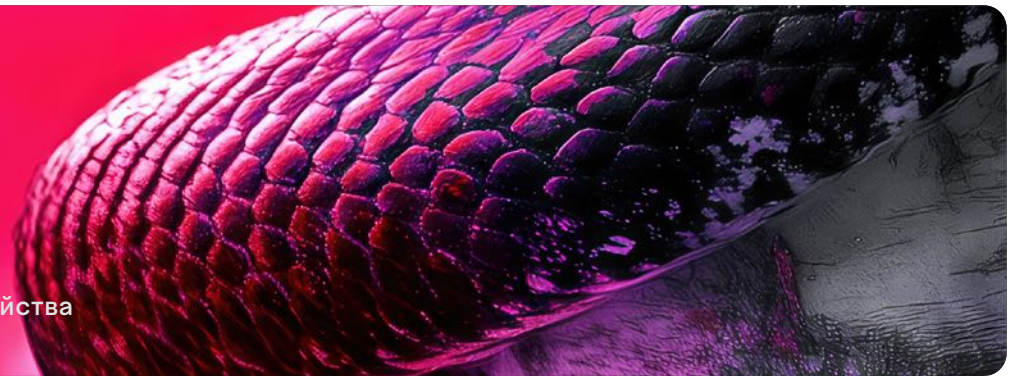
Сервис BONVI TEAM активен как минимум с августа 2024 года. Злоумышленники предлагают для распространения скачать вредоносное приложение для Android напрямую из Telegram. Данное ВПО получило название DeliveryRAT. Также злоумышленники получают ссылку на фейковый сайт RuStore. DeliveryRAT позволяет перехватывать и отправлять SMS с устройства, скрывать PUSH-уведомления, маскируется под легитимные приложения доставки, маркеты и банковские приложения. Также похищает введённые данные карты, которую пользователь вводит в ходе взаимодействия с ним. Целью злоумышленников, судя по описанию из Telegram-бота, является сбор конфиденциальных данных для оформления кредитов, МФО, кража денежных средств через онлайн-банкинг.

Троян маскируется под различные приложения:

- AvitoTracker,
- CdekTracker,
- BlablaTracker,
- BusforTracker,
- OzonTracker,
- ProfiTracker,
- TinkoffId,
- WildberriesTracker,
- YandexDostavkaTracker,
- YandexMarketTracker,
- YandexNedvizimostTracker,
- YandexUslugiTracker,
- YouDoTracker,
- YoulaTracker.

Троян передаёт владельцам сообщения от следующих отправителей (написание соответствует оригиналу): «900», «Alfa-Bank», «Tinkoff», «Gazprombank», «Sovkombank», «BankTochka», «Rencredit», «MTS-Bank», «OTKRITIE», «VTB», «OTP Bank», «POCHTABANK», «Raiffeisen».

MoneyGlot



MoneyGlot — вредоносная активность, обнаруженная специалистами Threat Intelligence компании F6 в апреле 2024 года. Злоумышленники используют Android-трояны MoneyGlot.SMS и MoneyGlot.AutoClick, нацеленные на пользователей российских банков.

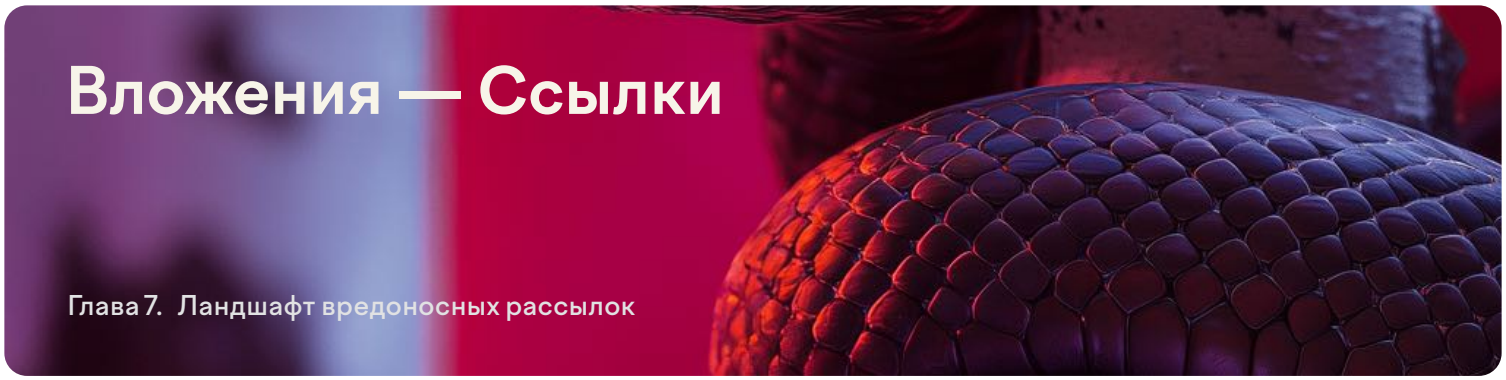
MoneyGlot.AutoClick содержит реализацию ATS-сценариев, направленных на выполнение транзакций с использованием легитимных приложений российских банков. Вредоносное ПО мимикрирует под приложения различных сервисов для провокации пользователя выдать права на использование Accessibility Service и запуска легитимного приложения банка.

MoneyGlot.SMS является SMS-трояном и имеет функциональные возможности для выполнения SMS-команд путем отправки SMS на номер 900. Данный троян нацелен на выполнение денежных транзакций с устройства жертвы с помощью SMS-команд «Телефон и «Киви». Первая команда используется для оплаты мобильной связи, вторая — для пополнения QIWI-кошелька.

World Team

Сервис World Team активен как минимум с лета 2023 года. Злоумышленники предоставляют ссылки на лендинговые страницы, мимикрирующие под российские организации. Целью злоумышленников является установка ВПО для Android, которое получило название WORLDTEAM BOT, на устройство жертвы для получения данных карты и перехвата SMS от определённых банков. WORLDTEAM BOT позволяет злоумышленнику управлять устройством удаленно: получать содержимое SMS, отправлять произвольные SMS, получать подробные данные о системе, буфере обмена, перенаправлять пользователя на фишинговую страницу и отправлять пользовательский ввод на C2-сервер злоумышленников.

Ландшафт вредоносных рассылок

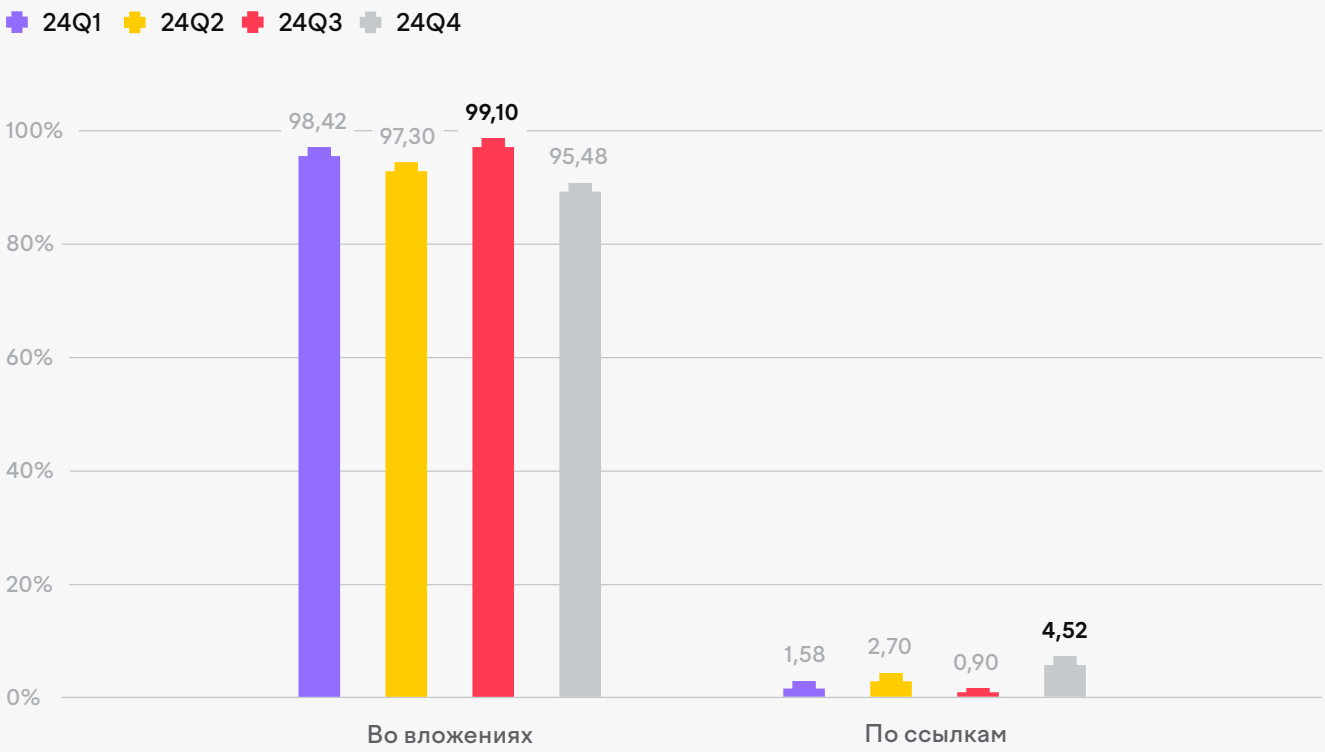


Вложения — Ссылки

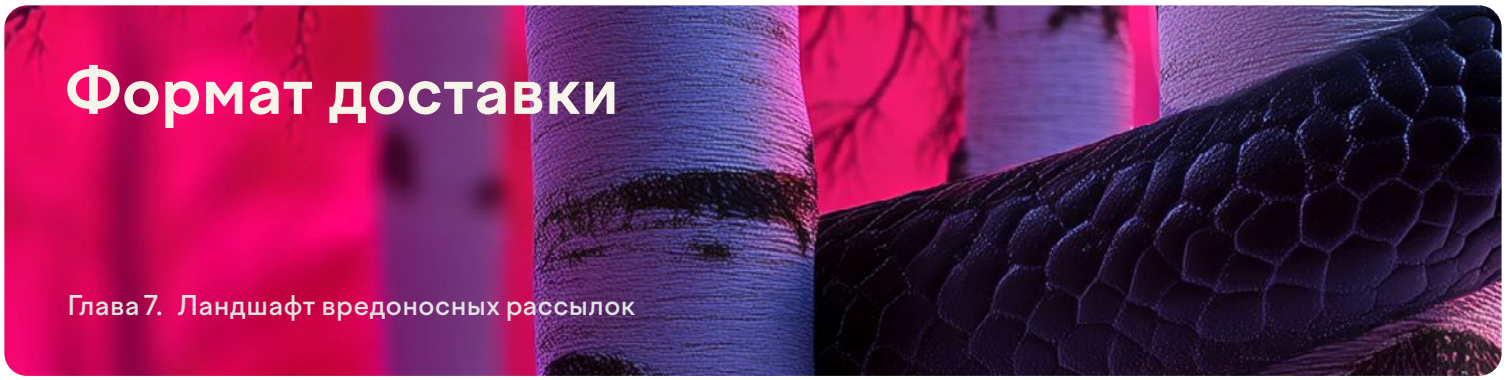
В подавляющем большинстве фишинговых писем вредоносное ПО доставлялось с помощью вложений, которые являются для злоумышленников в рамках массовых/веерных фишинговых кампаний наименее затратным способом доставки вредоносного ПО потенциальной жертве. Такой способ, в отличии от ссылок, не требует размещения вредоносное ПО на внешних ресурсах, контроля и обеспечения его доступности.

Распределение способов доставки ВПО из писем (в %)

f6.ru



Стоит отметить, что ссылки в письмах остаются одним из характерных атрибутов целевых фишинговых атак (но не обязательно таковыми), когда злоумышленники профилируют свою потенциальную жертву, позволяя с помощью ссылок дополнительно проводить проверки — кто и при каких условиях кликает по ссылке в письме. По результатам такой проверки атакующие могут принимать решение отдавать конечному пользователю вредоносную нагрузку либо безопасный файл, если идентифицируют применение на стороне пользователя определенных средств защиты или отдельных вендоров безопасности.

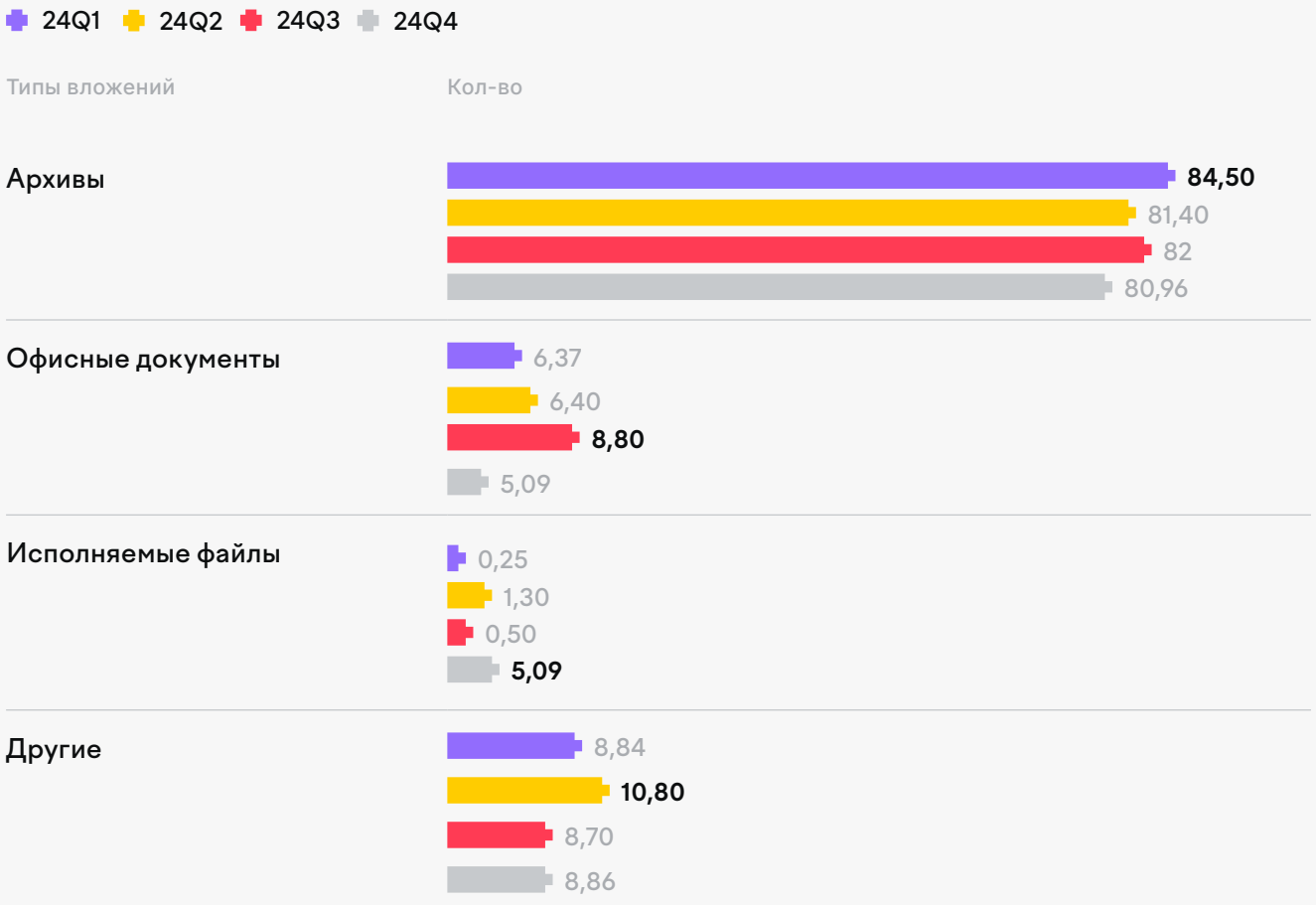


Формат доставки

Самыми популярными вредоносными вложениями в письмах остаются архивы, с заметным отрывом лидируют форматы «.zip» и «.rar». На втором месте по частоте использования в 2024 году находятся офисные документы.

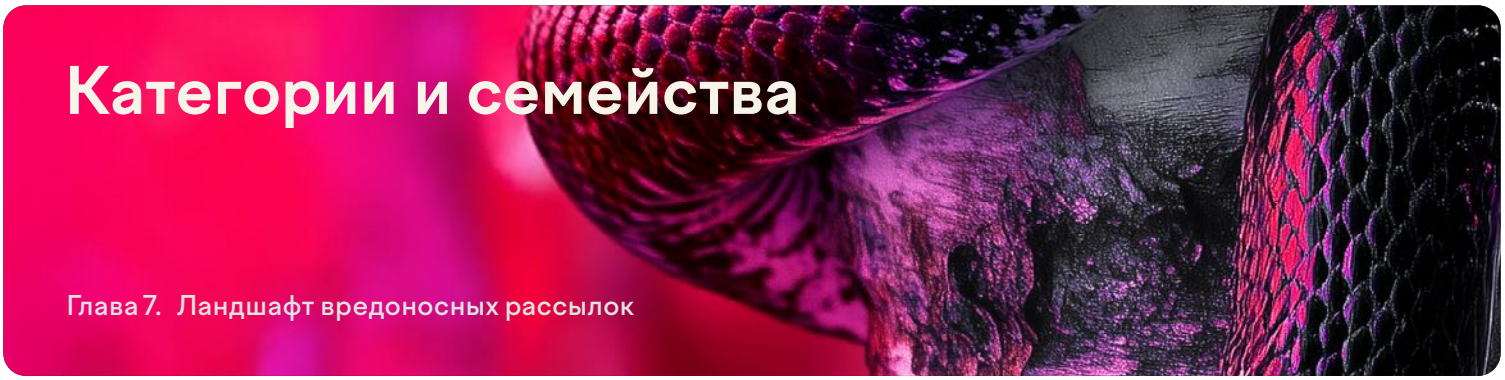
Типы форматов вложений из писем (в %)

f6.ru



Архивы продолжат оставаться самым популярным доставщиком вредоносной нагрузки первого этапа ввиду простой реализации обхода от детектирования традиционными средствами защиты. Атакующие продолжат экспериментировать со способами упаковки основных вредоносных элементов — делая многоуровневые вложения «матрешки», шифруя архивы — с различными способами доставки этого пароля конечному пользователю.

Категории и семейства



Шпионское ПО и инфостилеры являются самым популярным вредоносным ПО в рассылках. В течение 2024 года их доля варьировалась от 70% до 80% от всех категорий вредоносного ПО, задействованных в фишинговых рассылках.

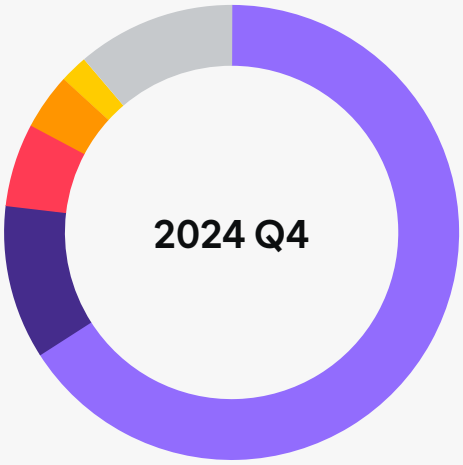
Шпионское ПО в таком масштабе сегодня представляет особую опасность как для рядовых пользователей интернета, компрометируя их личные данные, так и для самих компаний, компрометация работников которых открывает двери злоумышленникам в инфраструктуру. У атакующих появляются широкие возможности — от шантажа публикацией украденных данных до развития более сложной кибератаки, приводящей к остановке бизнес-процессов скомпрометированной компании и утечки данных.

В первой половине 2024 года самым популярным вредоносным ПО, как и в последние года, оставалось шпионское ПО Agent Tesla. Со второй половины 2024 года доля Agent Tesla резко начала сокращаться, уступив лидирующие позиции FormBookgrabber.

Причиной утери лидирующих позиций Agent Tesla является выключение в середине июня инфраструктуры оператора, на которой предоставлялся данный «сервис» вредоносного ПО. Об этом было сообщено 1 июля в телеграмм-канале сервиса одним из злоумышленников, стоявших за разработкой и распространением Agent Tesla. Даже после ликвидации инфраструктуры вредоносного ПО благодаря своей популярности и старым сборкам Agent Tesla продолжает удержаться в топ-3 по популярности во вредоносных рассылках в третьем и четвертом кварталах 2024 года.

FormBookFormgrabber, хоть и входил в топ-10 в последнее время, показал со второй половины 2024 года особый рост популярности среди ВПО в фишинговых рассылках по сравнению с предыдущими периодами. Точных причин такого стремительного роста данного вредоносного ПО неизвестно, но, скорее всего, FormBook стал одной из основных альтернатив взамен раннее неоспоримого по популярности Agent Tesla.

Изменения в популярных семействах вредоносного ПО, задействованных в фишинговых рассылках (в %)



Вредоносное ПО	%
Agent Tesla	58
FormBook	13
Remcos	11
CloudEyE	6
DarkWatchman	4
Другое	8

Вредоносное ПО	%
FormBook	66
Agent Tesla	11
Redline Stealer	6
CloudEyE	4
Remcos	2
Другое	11

Фишинг и скам

Введение

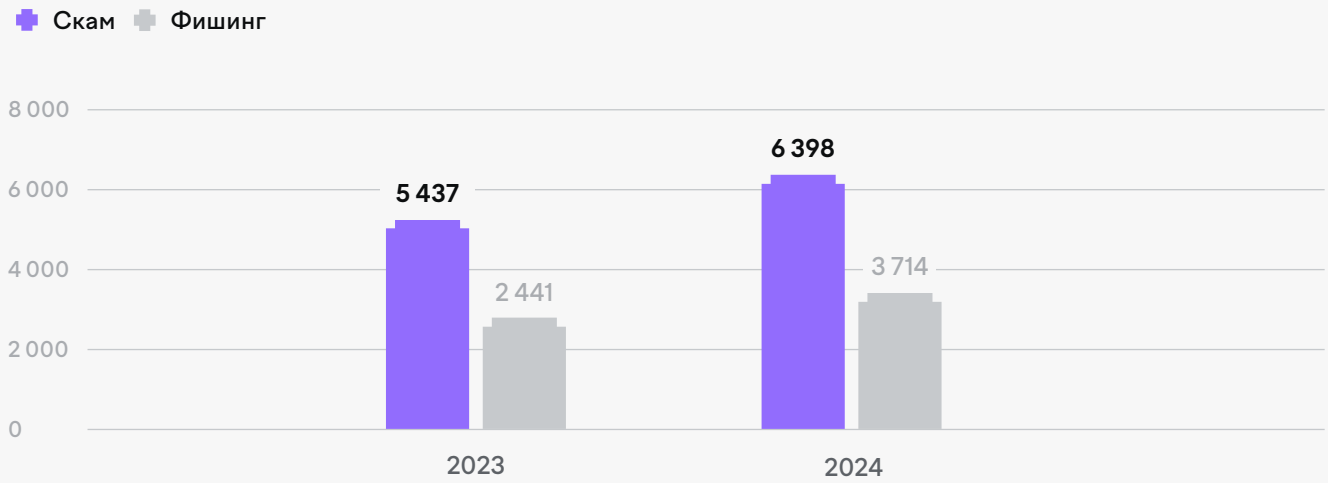
Глава 8. Фишинг и скам

Киберпреступники не перестают наращивать объемы фишинговых и скам-атак на российские компании. Ежегодно специалисты Digital Risk Protection фиксируют рост количества создаваемых ресурсов, эксплуатирующих бренды компаний. В 2024 году среднее количество создаваемых фишинговых сайтов на один бренд увеличилось на 52,15% по сравнению с 2023 годом, среднее количество создаваемых мошеннических ресурсов на один бренд увеличилось на 17,68%.

Рост угроз обусловлен продолжающимся развитием мошеннических сообществ и партнёрских программ. Автоматизация создания контента, имитирующего сайты брендов компаний, и простые в использовании инструменты для совершения преступлений вовлекают новых участников схем, что, в свою очередь, влияет на количество задействованных в схемах ресурсов, количество жертв и украденных денежных средств

Среднее кол-во создаваемых фишинговых и мошеннических ресурсов на 1 бренд

f6.ru

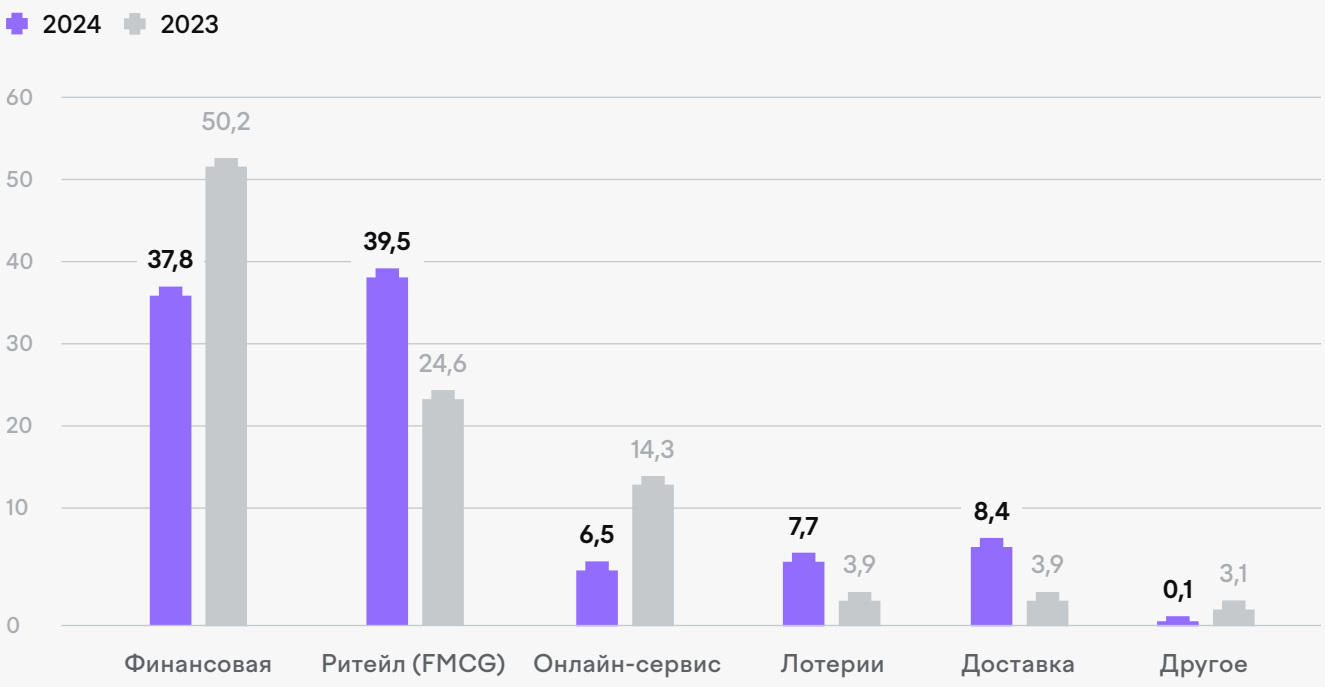


Атаки на индустрии

Фишинговые атаки остаются серьезной угрозой, как для клиентов компаний, так и для ее сотрудников. В 2024 году финансовый сектор, как и годом ранее, активно подвергался фишинговым атакам (37,8% от общего числа). Использование брендов банков, платежных систем и переводов эксплуатируются во множестве схем: для кражи данных банковских карт и данных входа в личный кабинет банка. Под электронную коммерцию также создается большое количество фишинговых ресурсов (39,5% от общего числа) — сайты оплаты товаров и услуг, входа в аккаунт, а также сайты-клоны магазинов и розыгрыши от имени брендов.

Фишинговые атаки по индустриям (в %)

f6.ru



Схемы с фейковыми лотереями всегда были популярны, в 2024 году количество создаваемых фишинговых ресурсов, связанных с лотереями, составило 7,7% от общего числа выявленных и заблокированных сайтов. Мошеннические партнерские программы предоставляют своим участникам различные варианты шаблонов лотерейной тематики для последующего распространения реферальных ссылок различными способами. Создание фишинговых страниц в различных дизайнах касается и других индустрий, чьи бренды эксплуатируются.

Также в 2024 году выросло использование брендов логистических компаний до 8,4% от общего количества нарушений, их злоумышленники часто эксплуатируют в схеме «Мамонт».

Существует множество мошеннических схем с разными сценариями кражи денежных средств, и для конкретной атакуемой сферы бизнеса может быть уникальный сценарий, позволяющий скамерам обогащаться за счет эксплуатирования брендов компаний.

Мошеннические атаки по индустриям (в %)

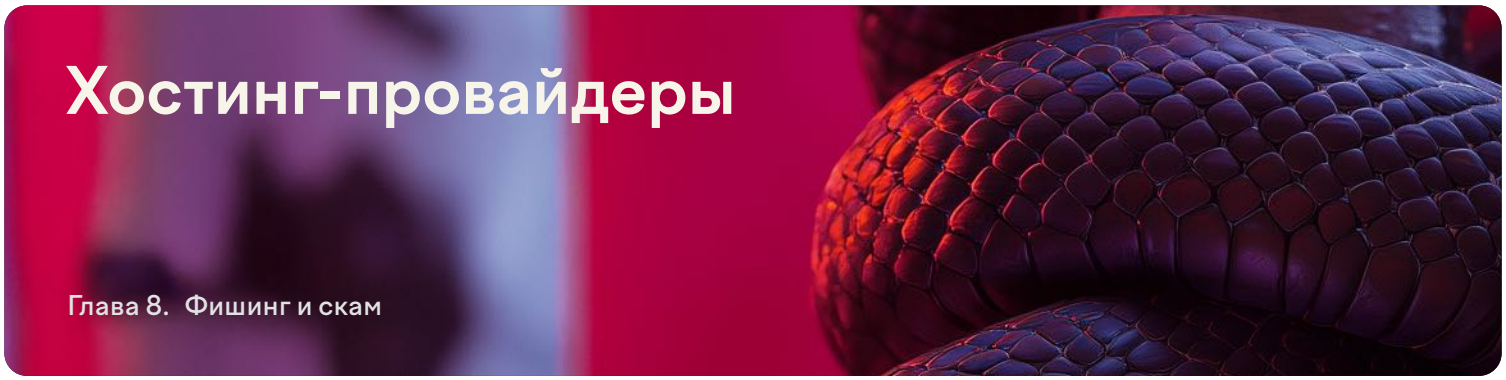
f6.ru

Лидером среди отраслей, под которые создаются мошеннические ресурсы, стала финансовая индустрия (48,2% от общего числа) — здесь киберпреступники создают множество поддельных сайтов и групп с аккаунтами в социальных сетях и мессенджерах для распространения схем инвестиционного мошенничества. Также много создаваемых мошеннических ресурсов приходится на бренды в сфере электронной коммерции (20,1% от общего числа) — фейковая работа от имени бренда, продажа бонусных карт.

Основной угрозой для компаний топливно-энергетического комплекса является большое количество инвестиционного мошенничества с упоминанием брендов. Также регулярно используются схемы с фейковой работой от имени бренда, продажей бонусных карт и продукции бренда.

В 2024 выросло количество мошенничества, направленного на телеком индустрию (12,2%). На этом направлении зафиксированы следующие нарушения: использование бренда в схемах инвестиционного мошенничества, фальшивые вакансии от имени бренда, поддельная продажа продуктов и услуг, а также таргетированное мошенничество.

Кроме того, участились случаи мошенничества, направленного на кстраховые компании (8,3%).

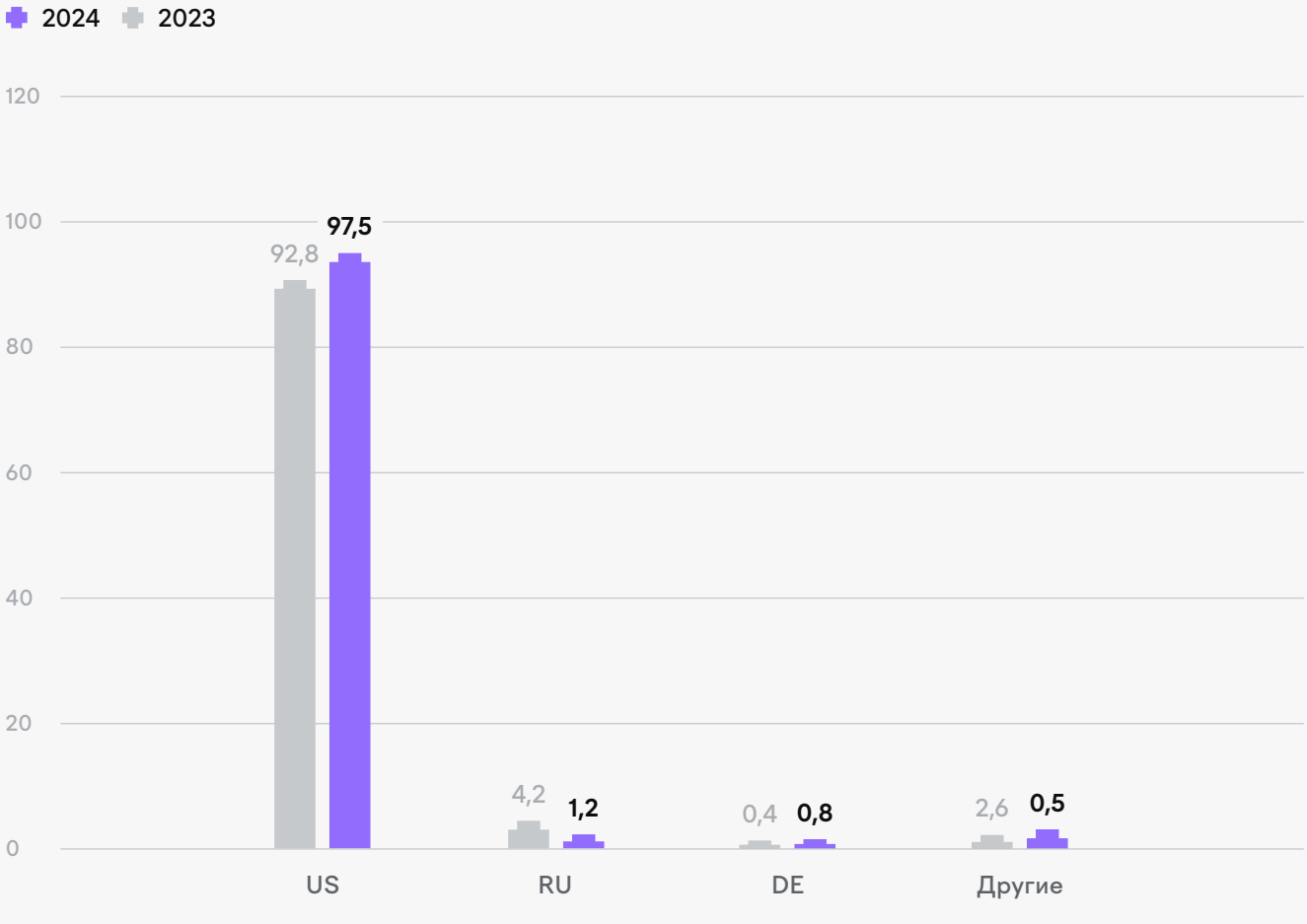


Хостинг-провайдеры

В 2024 лидерство по размещению фишингового и мошеннического контента держат американские хостинг-провайдеры. Мошенники пользуются тем, что система DNS компании Cloudflare, предназначенная для кэширования содержимого сайта с целью улучшения качества работы пользователей, может защитить IP-адрес сайта от прямого воздействия. Это может замедлить процесс общения с хостинг-провайдером мошеннического сайта по вопросу устранения нарушений, что потенциально продлевает срок жизни фишинговых и мошеннических ресурсов. Cloudflare может раскрыть хостинг-провайдера по запросу, но некоторые хостинг-провайдеры отказываются признавать нарушения, поскольку видят IP-адреса Cloudflare, а не свои собственные.

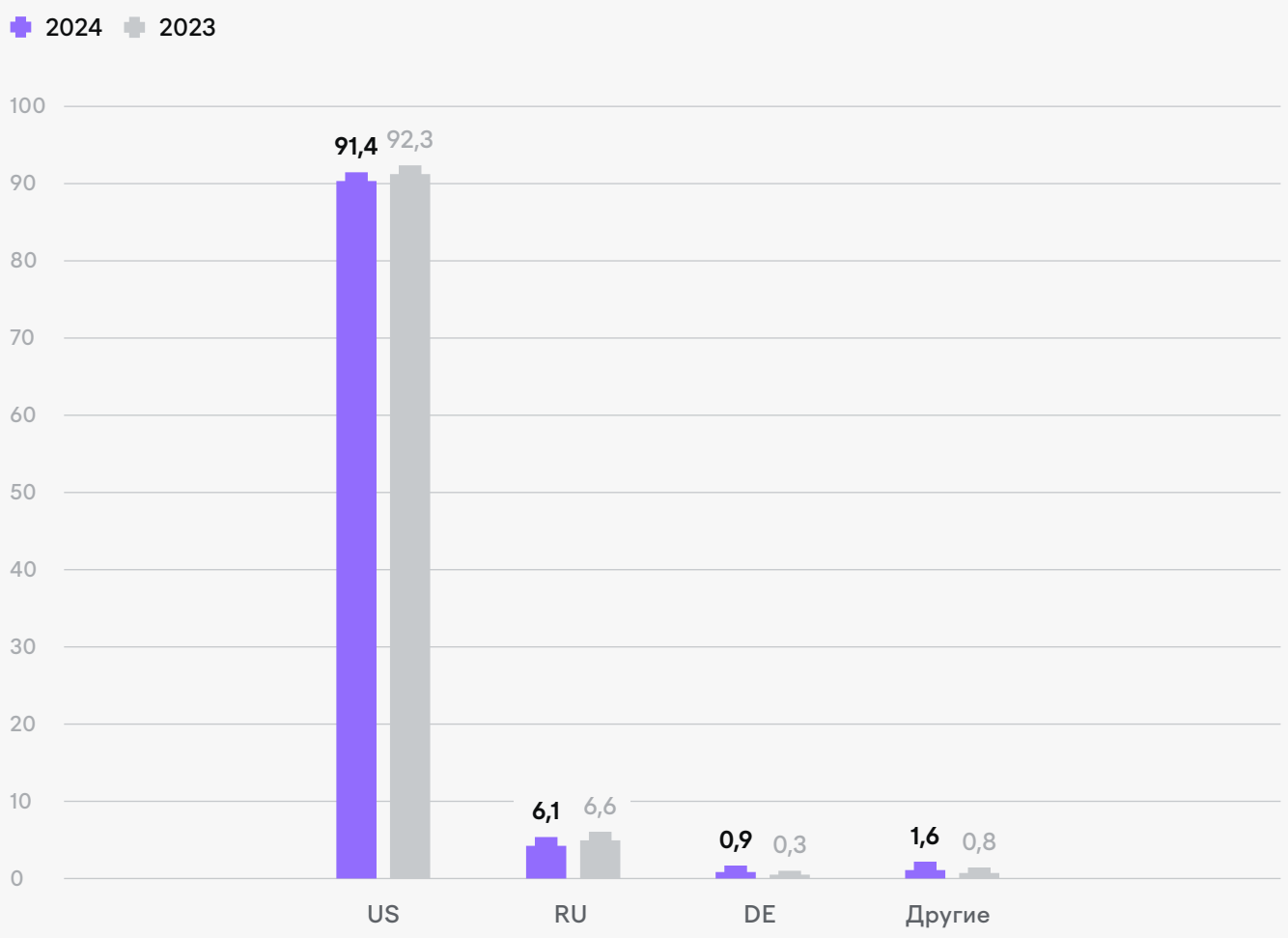
Распределение по хостинг провайдерам фишинговых ресурсов (в %)

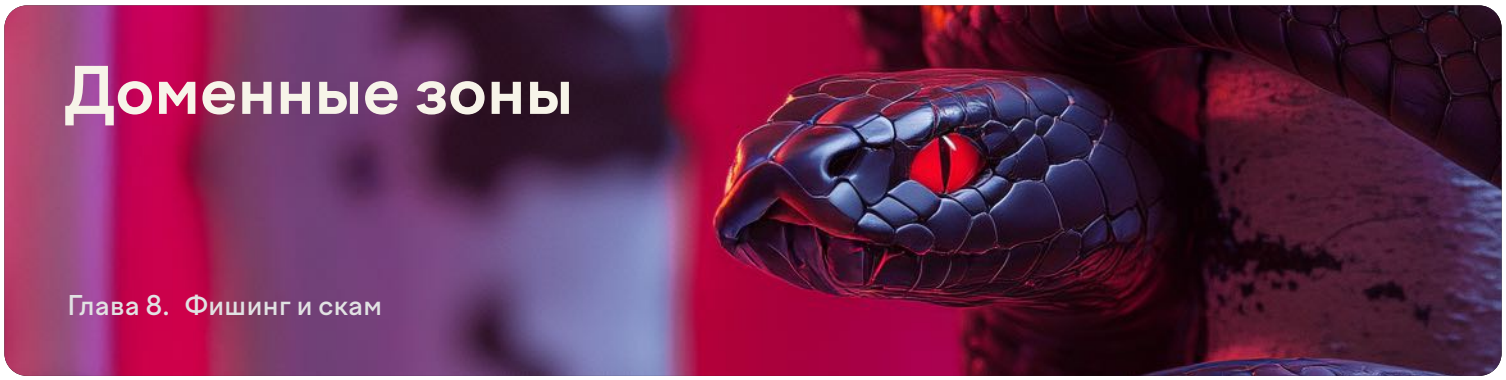
f6.ru



Распределение по хостинг провайдерам мошеннических ресурсов (в %)

f6.ru

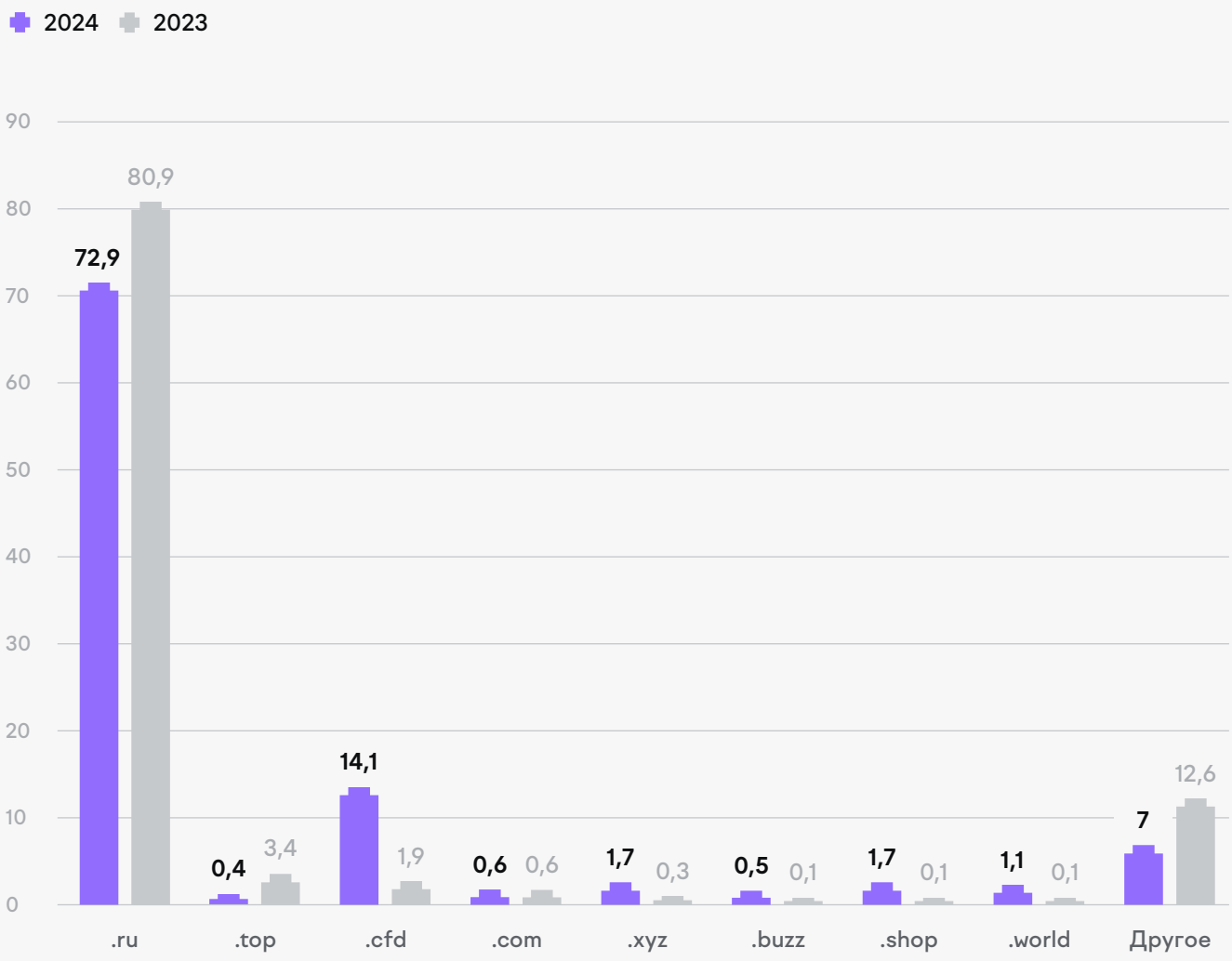




Доменные зоны

Распределение регистрируемых фишинговых доменов по зонам (в %)

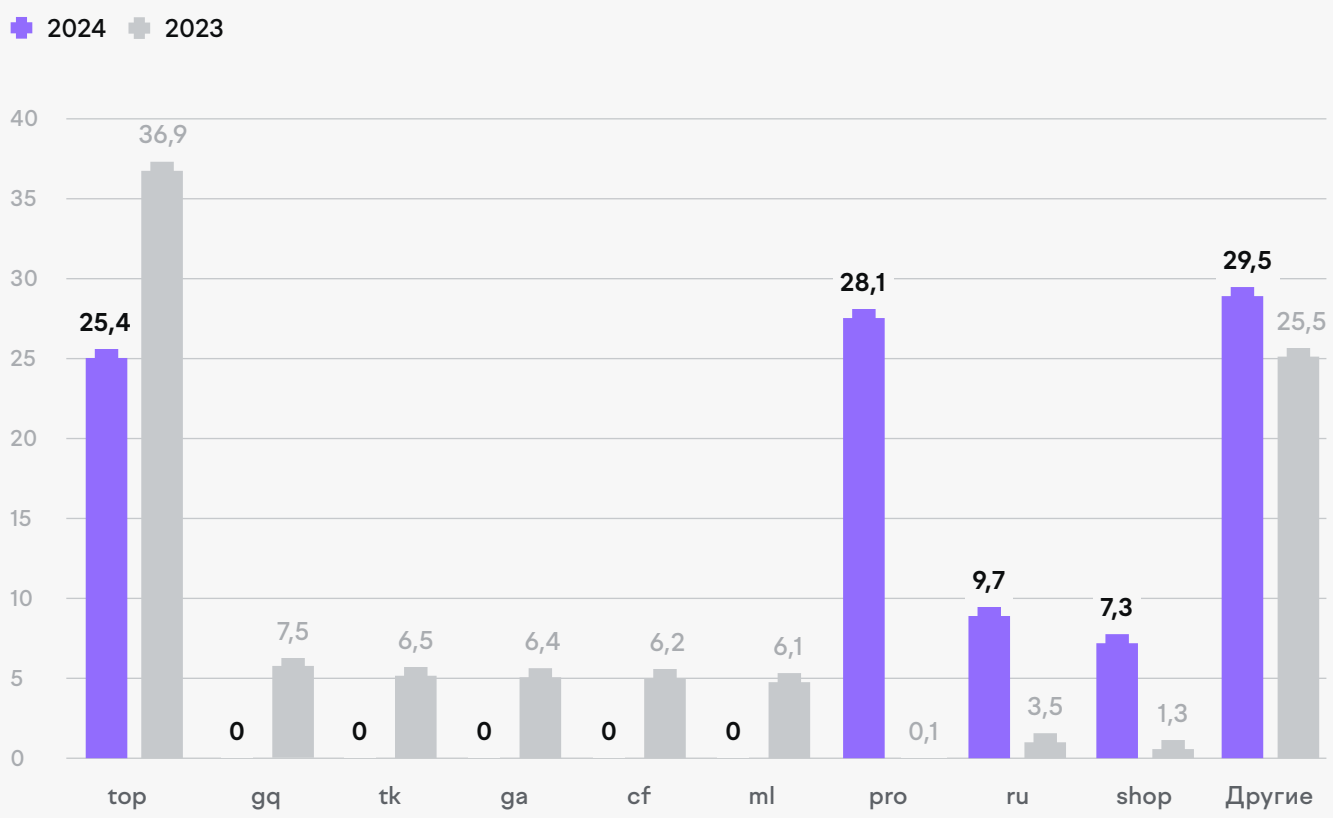
f6.ru



При выборе доменной зоны для регистрации доменного имени под фишинговые атаки злоумышленники зачастую выбирают зону .ru. Это обусловлено более низкой стоимостью регистрации в данной зоне по сравнению с другими, а также для созвучности с доменными именами брендов, на которые нацелены фишинговые атаки. В 2024 увеличилось количество фишинговых доменов в зоне .cfd: киберпреступные партнерские программы стали чаще использовать эту доменную зону для размещения фишинг-контента.

Распределение регистрируемых мошеннических доменов по зонам (в %)

f6.ru

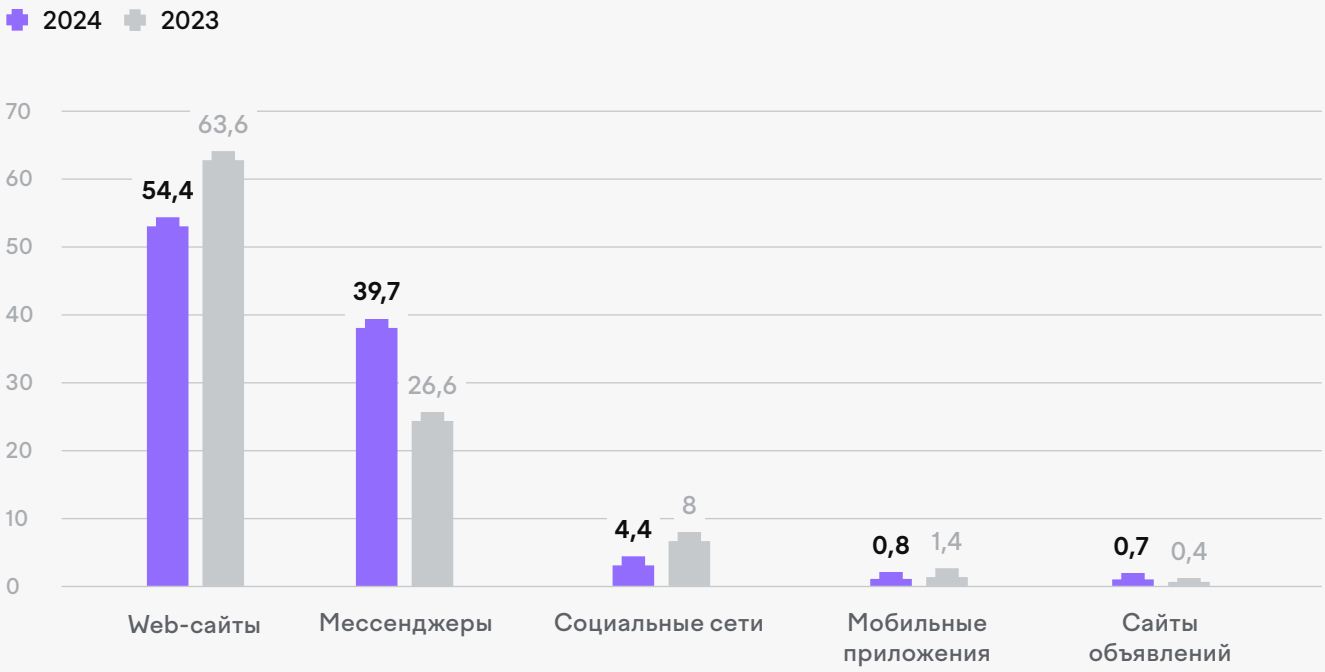


До 2023 года злоумышленники активно использовали бесплатные домены (в зонах .tk, .gq, .cf, .ml, .ga,), предоставляемые компанией Freenom, также известной как OpenTLD, для размещения мошеннического контента. После того, как компания Freenom вышла из доменного бизнеса в начале 2024 года, скамеры мигрировали на другие доменные зоны, в основном на .pro и .ru.

Типы мошеннических ресурсов

Распределение мошеннических ресурсов по типу (в %)

f6.ru



Основным элементом в мошеннических схемах является web-сайты. Социальные сети и мессенджеры обычно используются для привлечения трафика на эти web-сайты. Рост популярности мессенджеров у интернет-пользователей и компаний из России влияет на увеличение создаваемых поддельных аккаунтов, каналов, чат-ботов от лица реальных брендов, опережая по количеству фейки в социальных сетях.

В меньшей степени распространяются мобильные приложения компаний в неофициальных или фейковых магазинах приложений, но это не отменяет серьезность угрозы в виде загрузки троянов на устройства жертв.

Также злоумышленники могут создавать фейковые приложения в официальных сторах, размещая в них фишинговые страницы. Данная проблема больше затрагивает российские банки, приложения которых были удалены из официальных магазинов.

В некоторых случаях злоумышленники могут размещать объявления на бесплатных онлайн-площадках, в которых под именем бренда предлагают трудоустройство, продажу бонусных баллов или скидки.

Основные фишинговые и мошеннические схемы на бренды в 2024

Мошеннические схемы в интернете напоминают микроорганизмы, которые непрерывно эволюционируют, чтобы оставаться жизнеспособными и эффективно наносить удары. Для выживания им необходимо адаптироваться к изменениям в технологиях и защите, разрабатывать тактики взаимодействия с жертвами и внедрять новые техники для увеличения прибыли. Существует множество сценариев обмана интернет-пользователей, однако есть несколько наиболее устойчивых и широко распространённых схем, на которые приходится наибольшая часть угроз для компаний. Эти схемы, несмотря на свою давнюю историю, продолжают масштабироваться, совершенствоваться и представлять серьёзную угрозу. О них мы и расскажем далее.

Мамонт

Масштабная гибридная схема с элементами скама и фишинга, появившаяся в 2019 году, продолжает развиваться, пополняясь новыми брендами и техниками атак.

Напомним, что цель схемы — кража денежных средств, реализуемая путем фишинговых атак для получения данных банковских карт или переводов по реквизитам мошенников. Злоумышленники создают фейковые аккаунты в социальных сетях, мессенджерах и легальных сервисах, а также фишинговые сайты, имитирующие реальные бренды, которые создаются с помощью специализированных Telegram-ботов, предоставляемых участникам киберпреступных сообществ по этой схеме.

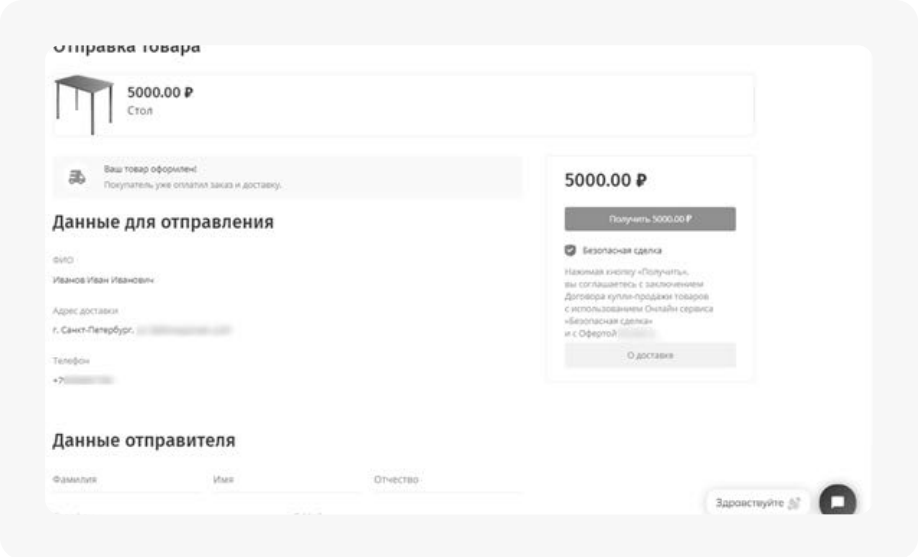


Рис. 40. Пример сгенерированной фишинговой страницы по схеме «Мамонт»

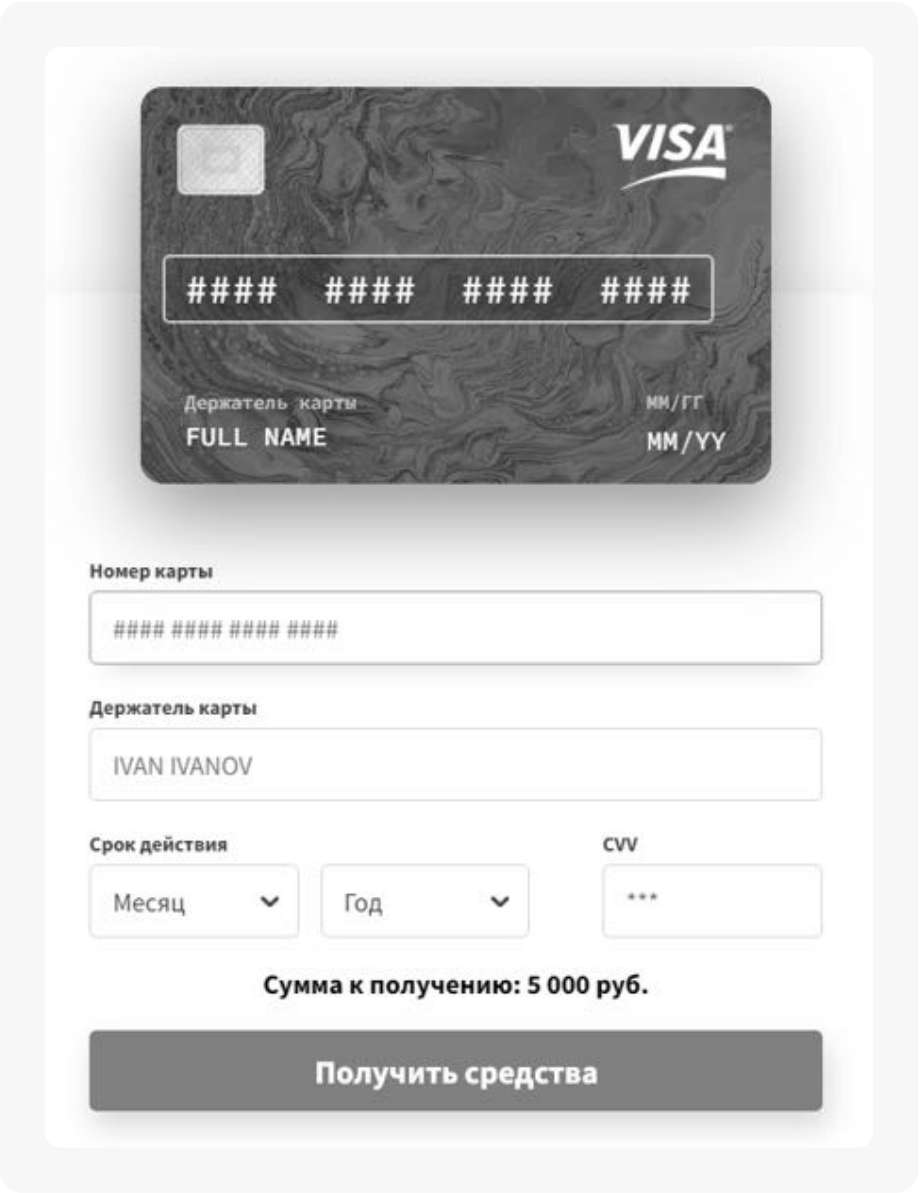
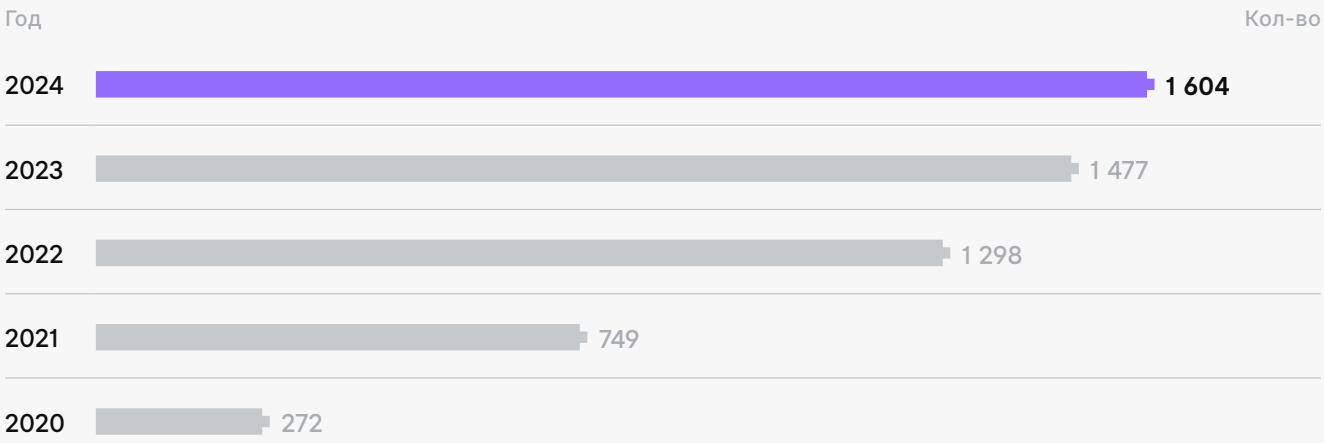


Рис. 41. Пример фишинговой формы ввода данных банковской карты

Вся экосистема групп находится в мессенджере Telegram: бот для генерации фишинговых ссылок, канал с выплатами, чат для коммуникации участников групп. Отдельные группы предлагают своим участникам инструкции по совершению мошенничества и ботов-отрисовщиков для подделки документов.

Количество основанных скам-групп по схеме «Мамонт»

f6.ru



Специалистам Digital Risk Protection известно более чем о 1 600 различных группах, созданных с начала 2020 года по конец 2024 года. Среди них есть как те, которые продолжают работать по схеме «Мамонт» в настоящее время, так и прекратившие деятельность. Большинство таких групп действуют недолго, но на смену закрывшимся почти сразу появляются новые.

В схеме задействовано множество индустрий, связанных с онлайн-платежами за покупку/продажу товаров или услуг.

Индустрии, чьи бренды используются в схеме «Мамонт»

f6.ru

Вредоносное ПО	%
Банковский перевод	33
Доставка	27
Доски объявлений	10
Маркетплейс/ритейл	10
Перевозки	8
Недвижимость	3
Услуги	3
Отели	3
Авиа	2
Господдержка	1

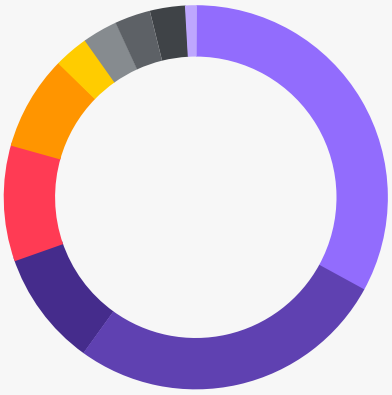


Рис. 42. Индустрии, чьи бренды используются в схеме «Мамонт»

С каждым годом схема совершенствуется, позволяя скамерам максимизировать прибыль от атак на интернет-пользователей.

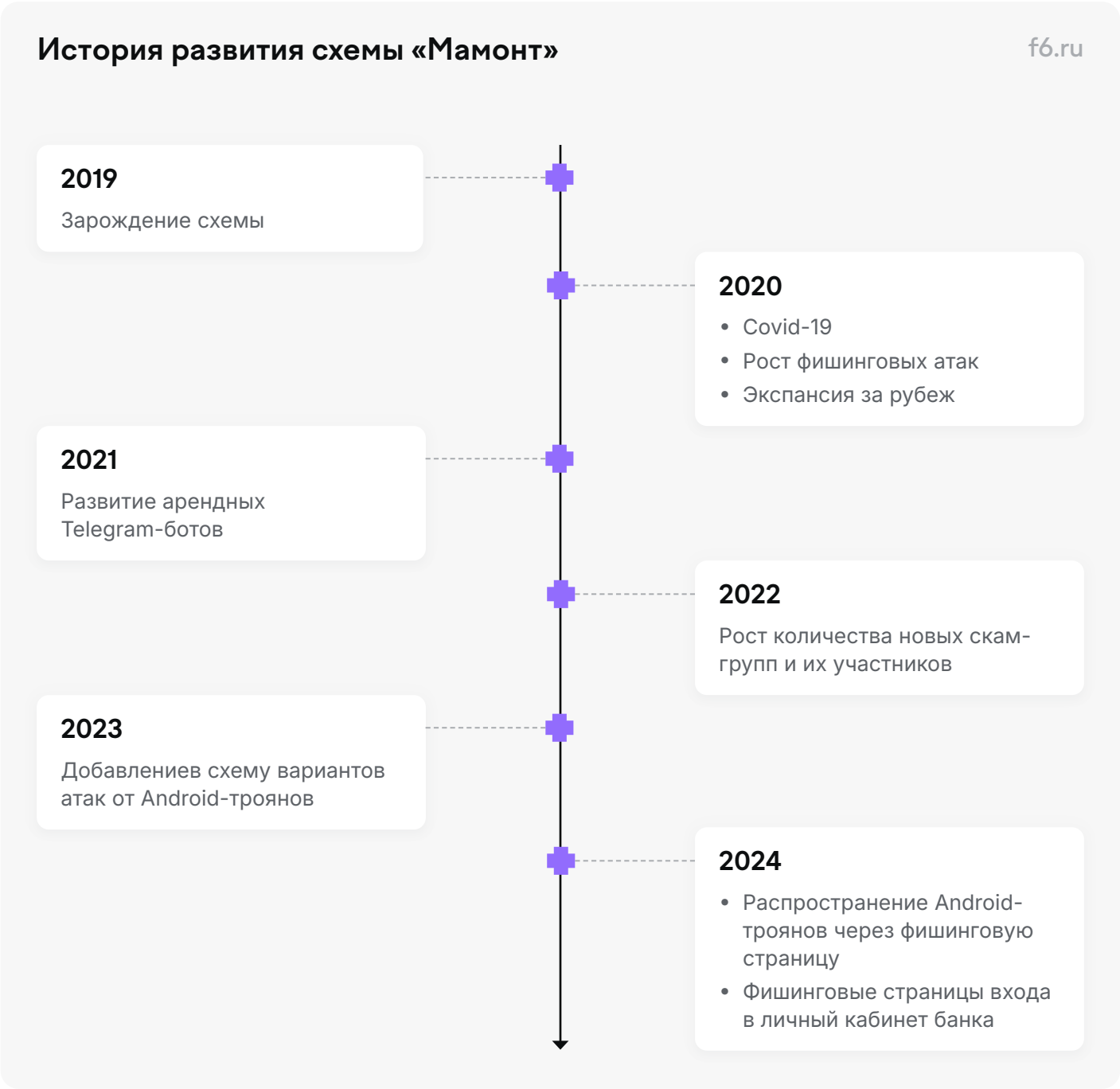


Рис. 43. История развития схемы «Мамонт»

Летом 2023 года была основана новая киберпреступная группа World Team, взявшая за основу архитектуру устройства скам-групп по «Мамонту». Эта группа предлагала своим участникам распространение Android-трояна под видом легитимного приложения.

В 2024 году некоторые скам-группы переняли идею с распространением Android-трояна. Сразу после оплаты на фишинговой странице жертве, как и раньше, предлагают скачать приложение для отслеживания доставки только что оплаченного заказа. Но если раньше пользователю предлагалось сначала перейти по ссылке на фейковый GooglePlay, чтобы скачать вредоносный APK-айл, то сейчас предлагают скачать его сразу на странице оплаты фейкового заказа.

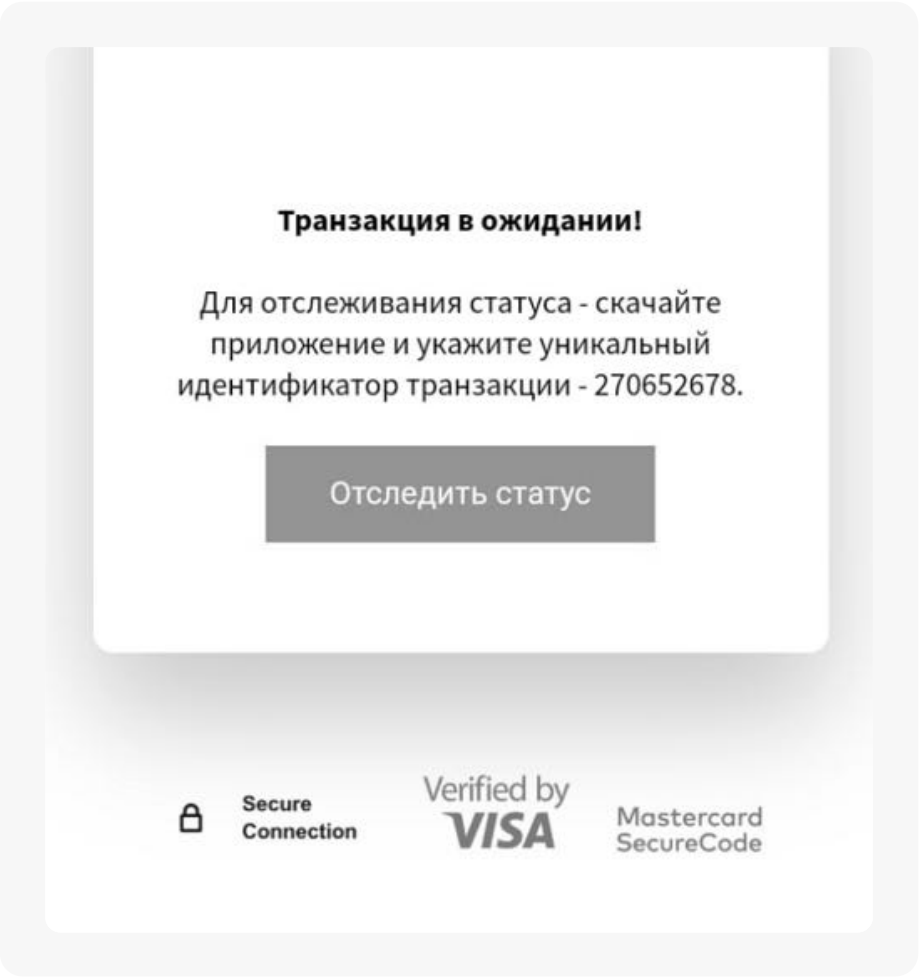


Рис. 44. Пример страницы для скачивания Android-трояна

Злоумышленники улучшили фишинговые страницы, предназначенные для потенциальных жертв в некоторых странах. Теперь они включают поддельные страницы входа в личные кабинеты местных банков таких государств, как Армения, Кыргызстан, Узбекистан, Азербайджан и Казахстан. На этих страницах жертве предлагают ввести учетные данные своих банковских аккаунтов. Мошенники собирают эти данные, входят в счета жертв и переводят деньги на счета дропов.

В октябре 2024 года в Telegram-ботах появилась возможность генерации фишинговых страниц входа в личные кабины российских банков, что позволило киберпреступникам списывать денежные средства со всех карт жертвы.

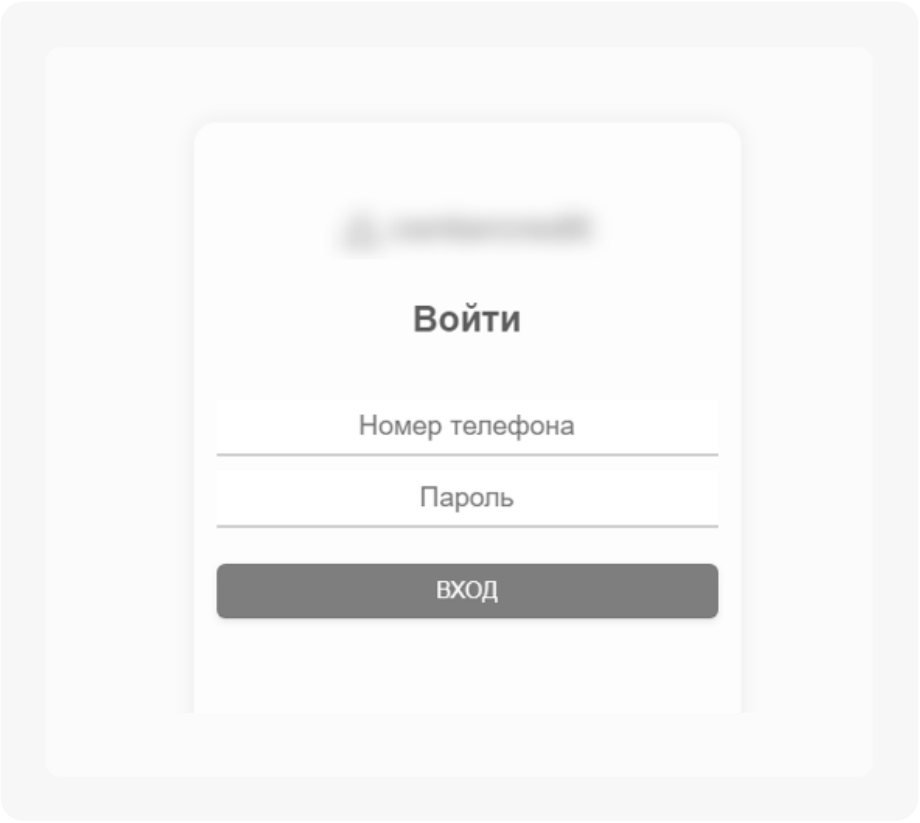


Рис. 45. Пример ввода данных от личного кабинета банка на фишинговом сайте

Также в 2024 году произошло объединение схем «Мамонт» и FakeDate (популярная схема мошенничества, которая появилась в 2018 году: злоумышленники от имени девушек на сайтах знакомств и в социальных сетях предлагали жертвам пойти с ними в кино, после чего присылали ссылку на фишинговый сайт). Теперь некоторые крупные команды из схемы «Мамонт» добавили в свой функционал возможность создания ссылок по схеме FakeDate.

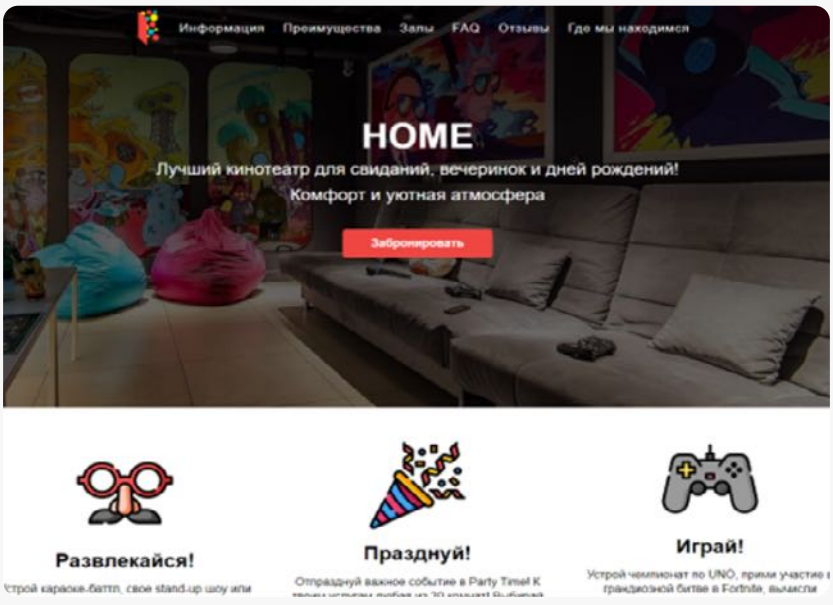


Рис. 46. Пример фишингового сайта по схеме FakeDate

Суммы краж и количество успешных фишинговых атак в России по этой схеме ежегодно только увеличиваются. На примере 8 крупных скам-групп, действующих по схеме «Мамонт», в 2024 был зафиксирован рост похищенных средств на 53,8% - с 620 млн рублей в 2023-м до 953 млн рублей в 2024-м. Количество успешных фишинговых атак выросло на 17,1% — 86 300 списаний в 2023 году и 101 071 в 2024.

В схеме «Мамонт» по странам СНГ активно используется 128 уникальных брендов, некоторые из них — по нескольким странам.

Бренды, используюемые в схеме «Мамонт»

f6.ru

Страна	Кол-во
Россия	42
Армения	30
Азербайджан	18
Казахстан	16
Узбекистан	11
Кыргызстан	6
Таджикистан	5
Всего	128

А также 39 брендов на этапе входа в личный кабинет банка.

Бренды на этапе входа в личный кабинет банка

f6.ru

Вредоносное ПО	Кол-во
Армения	13
Кыргызстан	9
Узбекистан	9
Азербайджан	4
Казахстан	3
Россия	1
Всего	39

Партнерские программы

Рис. 47. Пример фейкового розыгрыша призов

Как и схема «Мамонт», мошеннические партнерские программы существуют уже давно. Организаторы программ предлагают своим участникам каталог из шаблонов с дизайнами фишинговых и мошеннических страниц. Выбрав оффер (предложение — шаблон дизайна веб-страницы), участник получает реферальную ссылку, которую распространяет всевозможными способами.

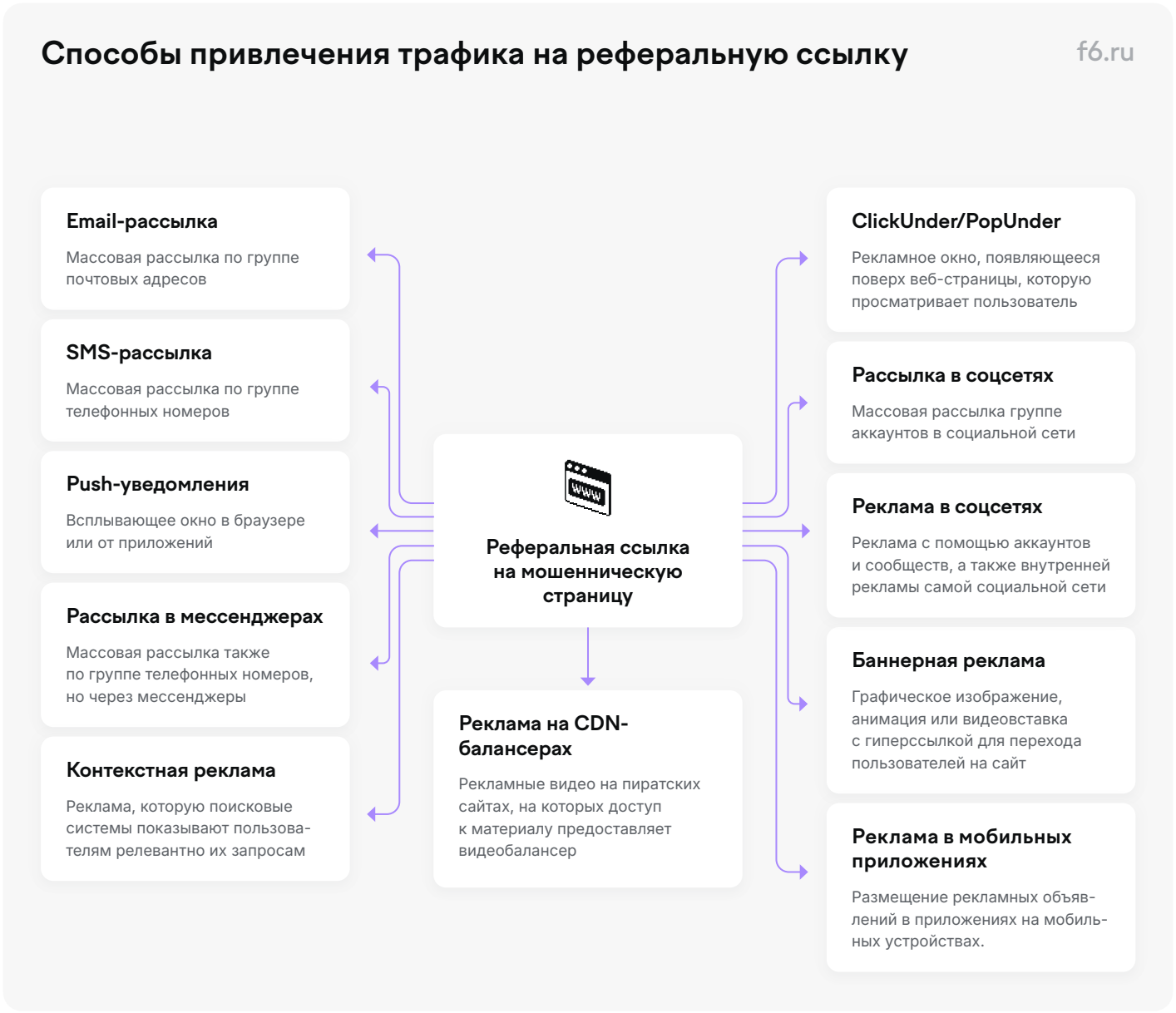
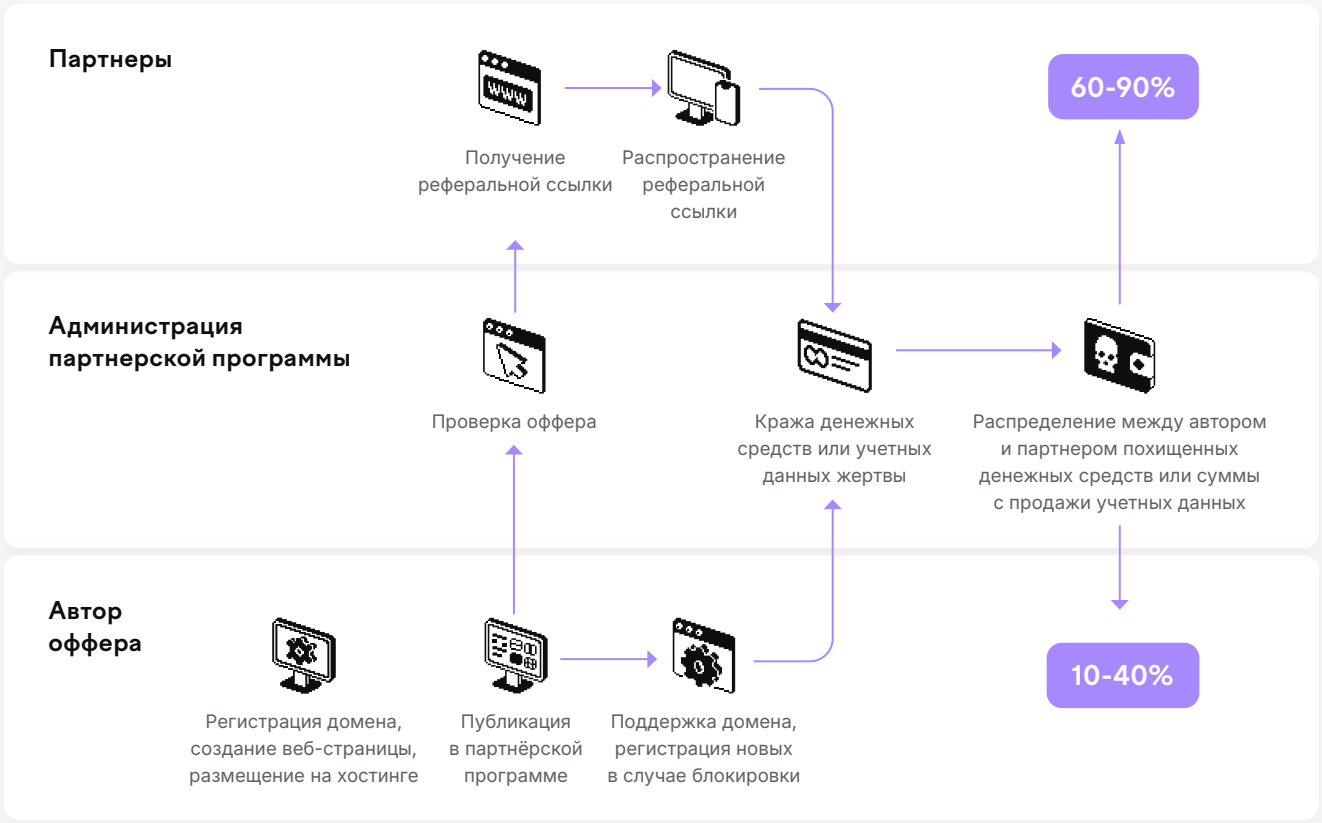


Рис. 48. Способы привлечения трафика на реферальную ссылку

Большинство партнёрских программ работают следующим образом:

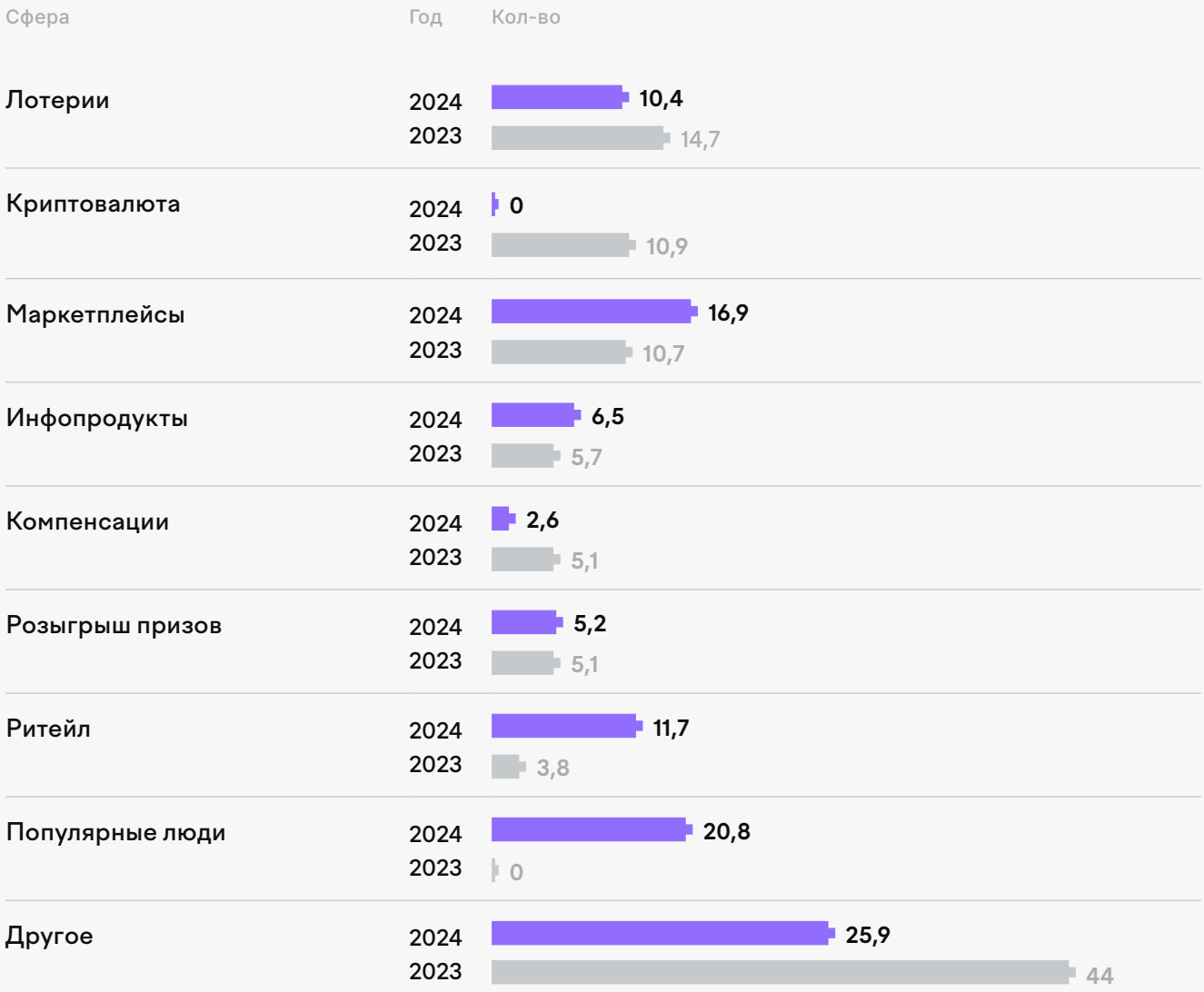
- Автор оффера (предложения) регистрирует домен, создает мошеннические веб-страницы, размещает их на хостинге. После этого регистрируется и заходит на сайт партнерской программы, где размещает оффер с созданным сайтом и тематическим дизайном веб-страницы.
- Администрация партнерской программы проверяет размещенный ресурс и, в случае успешной проверки, предоставляет фишинговые формы или формы приема оплаты для внедрения в сайт. В некоторых случаях единственным автором офферов является администратор площадки, но это скорее исключение.
- Партнёры выбирают оффер, получают реферальную ссылку для распространения и разными способами привлекают трафик на эту ссылку. Под способами распространения — подразумевается СМС-рассылка, почтовые письма, сообщения в социальных сетях и мессенджерах, реклама и т.д.

Схема работы мошеннических партнерских программ



Распределение оферов по индустриям (доли в %)

f6.ru



Самые популярные сценарии в партнерских программах в 2024 году.

- Розыгрыши от имени известных людей. Жертва переходила по ссылке и попадала на страницу, где ей предлагали открывать коробочки с призами. Обычно первые две попытки были безуспешными, а на третий раз попадался якобы крупный выигрыш. Чтобы получить деньги, жертве предлагалось ввести данные банковской карты, на которую можно зачислить выигрыш, и оплатить по реквизитам «комиссию». В итоге пользователи теряли деньги или как минимум компрометировали банковскую карту.
- Фейковые предложения от маркетплейсов и интернет-магазинов, в основном это псевдорозыгрыши от брендов известных маркетплейсов, в которых надо также оплатить комиссию, чтобы получить приз, либо трудоустройство с оценкой товаров, под предлогом которого необходимо заплатить.
- Фейковые лотереи, когда жертве сообщают, что бесплатно получен лотерейный билет. В итоге он, конечно же, выигрывает, но чтобы получить деньги, необходимо заплатить комиссию.

Инвестиционное мошенничество

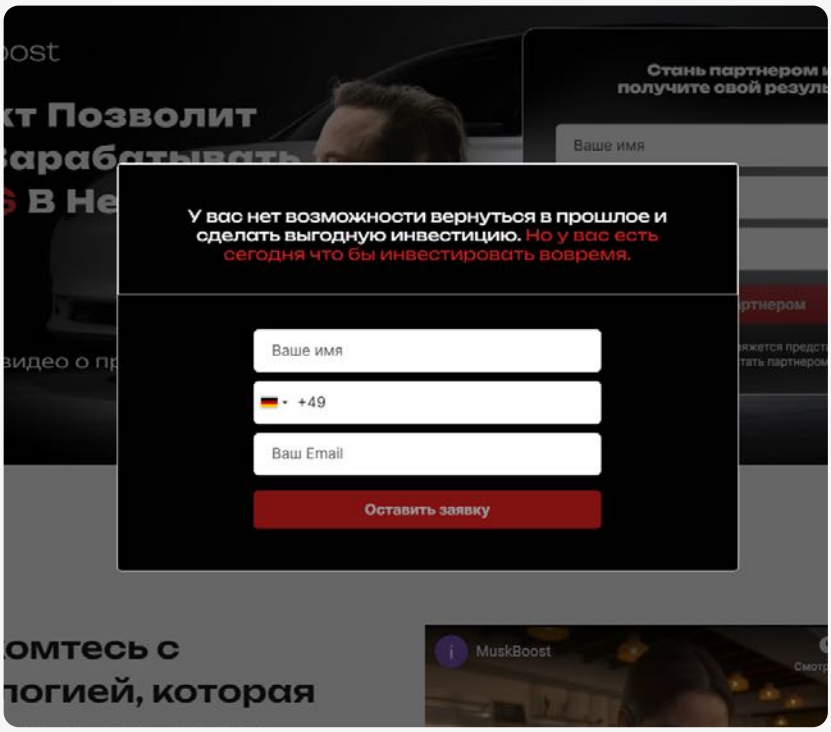


Рис. 49. Пример сайта инвестиционного мошенничества

Инвестскам (инвестиционное мошенничество) на киберпреступном поле уже давно и его активность не снижается среди других крупных схем, как по количеству создаваемых ресурсов и рекламных кампаний, так и по суммам ущерба.

Рис. 50. Пример интерфейса мошеннической инвестиционной платформы

Это вид финансового обмана с последующим требованием денежных средств под предлогом прибыльных инвестиционных вложений. В подобных схемах злоумышленники создают поддельные веб-ресурсы, аккаунты в социальных сетях и мессенджерах, разрабатывают приложения, имитируя инвестиционные проекты и биржи. После пополнения баланса в таком проекте первое время жертве могут «рисовать» красивые графики об успешном увеличении капитала. Но через какое-то время активы начнут искусственно уменьшаться, а мошенники будут настаивать на новом пополнении баланса под предлогом «гарантированного» приумножения денежных средств.

Как работает инвестскам

f6.ru

В своих рекламных кампаниях для повышения вовлеченности потенциальных жертв злоумышленники зачастую используют реальные бренды, в частности, из банковского сектора, нефти и газа, интернет-сервисов.

Отличительной чертой мошеннических схем с инвестициями в большинстве случаев является активное участие мошеннических колл-центров. Потенциальной жертве назначается личный «инвестиционный эксперт», задача которого — убеждать её вкладываться в проект и продолжать это делать до тех пор, пока не закончатся деньги. Перед попыткой вывода средств жертва всегда будет сталкиваться с различными препятствиями. Помимо хищения мошенниками денег, жертву будут вынуждать делиться конфиденциальными данными и персональными документами.

В первом полугодии 2024 года специалистами Digital Risk Protection было обнаружено более 10 мошеннических партнерских программ, а также 10 000 доменов, связанных с инфраструктурой мошеннических инвестиционных проектов. А за период с января 2023 года по май 2024-го мошенники опубликовали 17 969 соответствующих рекламных постов на русском языке в Instagram и Facebook (принадлежат корпорации Meta, которая признана экстремистской и запрещена в РФ), причем 98% из них были размещены только с августа 2023. Точные причины такого роста нам не известны, но предполагаем: это связано как раз с популяризацией мошеннических партнерских программ по этому направлению. Актуальность таких схем напрямую зависит от информационных поводов и, соответственно, от намерения людей заниматься инвестированием, чем активно пользуются киберпреступники.

FakeBoss

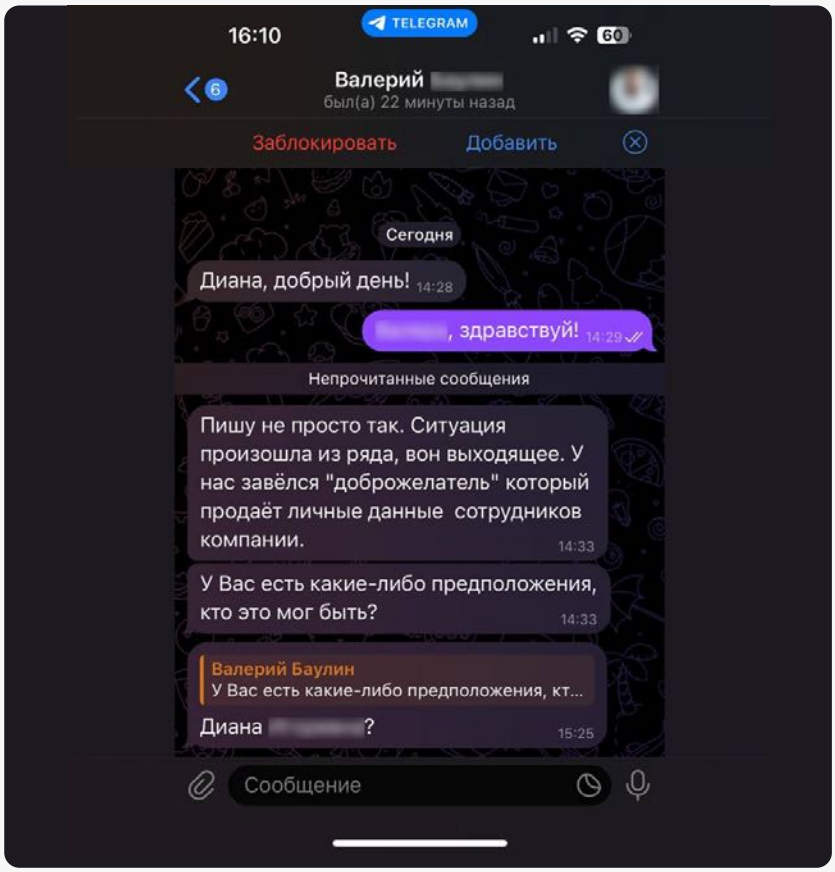


Рис. 51. Пример сообщения от фейкового аккаунта руководителя компании

Мошенническая схема, появившаяся осенью 2023 года как вариант классического телефонного мошенничествают лица руководителей частных и государственных организаций, с активным использованием ИИ-сервисов в 2024 году стала принимать характер эпидемии.

FakeBoss. Как мошенники атакуют сотрудников компаний через мессенджеры

f6.ru

Разведка и поиск жертвы

Базы данных

Открытые источника

Поиск аккаунта руководителя в мессенджерах

Подготовка ресурсов

Заполнение профиля (ФИО, фото информация о себе)

Сокрытие номера телефона и username, отправителя при пересылкке сообщений

Использование статуса «верифицированного аккаунта»

Контакт с потенциальной жертвой

Рассылка по контактам, зарегистрированным в мессенджерах

Небольшая беседа с целью убедить жертву в легитимности следующего звонка

Телефонный звонок

Монетизация

Прямой перевод на карту мошенника

или

Просьба пройди до банкомата и перевести деньги на «безопасный» счёт

или

Вызов курьера к жертве для передачи наличных средств

Действуя по схеме, в качестве первого этапа захвата внимания, преступники используют сообщение в мессенджере с фейкового аккаунта руководителя жертвы с его ФИО и, иногда, фото. Расчет делается на то, что подчиненный не сможет отказать руководителю в просьбе пообщаться по телефону с «куратором от безопасности» или поставить под сомнение достоверность его информации.

Специалистами Digital Risk Protection было зафиксировано, что злоумышленники могут атаковать сотрудников компаний многократно, волнами в течение долгого периода.

Уже по телефону жертве будут рассказывать, например, что произошла утечка данных и денежные средства сотрудника находятся под угрозой, а для сохранения своих средств необходимо перевести часть суммы через банкоматы, часть передать курьеру. Либо, что счет жертвы задействован в противозаконных переводах, как, например, спонсирование запрещенных организаций. Когда жертва соглашается поговорить по телефону с куратором, последний запугивает и предлагает выход – раскрыть данные о предприятии, сотрудниках или перевести деньги на безопасный счет.

Еще одним сценарием может быть просьба фейкового руководителя сразу перевести денежные средства, без звонков, торопя жертву совершить перевод, чтобы она не успела разобраться в происходящем.

В начале 2024 года участники этой схемы начали использовать инструменты искусственного интеллекта для подделки голоса мошенника под руководителя.

В новом сценарии киберпреступники, выдающие себя за руководителя, не пишут сообщения подчиненному, а сразу звонят через мессенджер. Для подмены голоса с использованием ИИ злоумышленникам требуется заранее получить фрагмент речи, который будет использован для обучения нейросети. Для этого они могут, например, записать разговор, зная телефонный номер жертвы, или взломать аккаунт в мессенджере и получить доступ к голосовым сообщениям пользователя.

Фишинговые панели для кражи аккаунтов в мессенджерах

В первой половине 2024 года специалистам Digital Risk Protection было обнаружено 6 фишинговых панелей, используемых для создания фишинговых ресурсов, нацеленных на пользователей Telegram, и одна панель, работающая против пользователей WhatsApp.

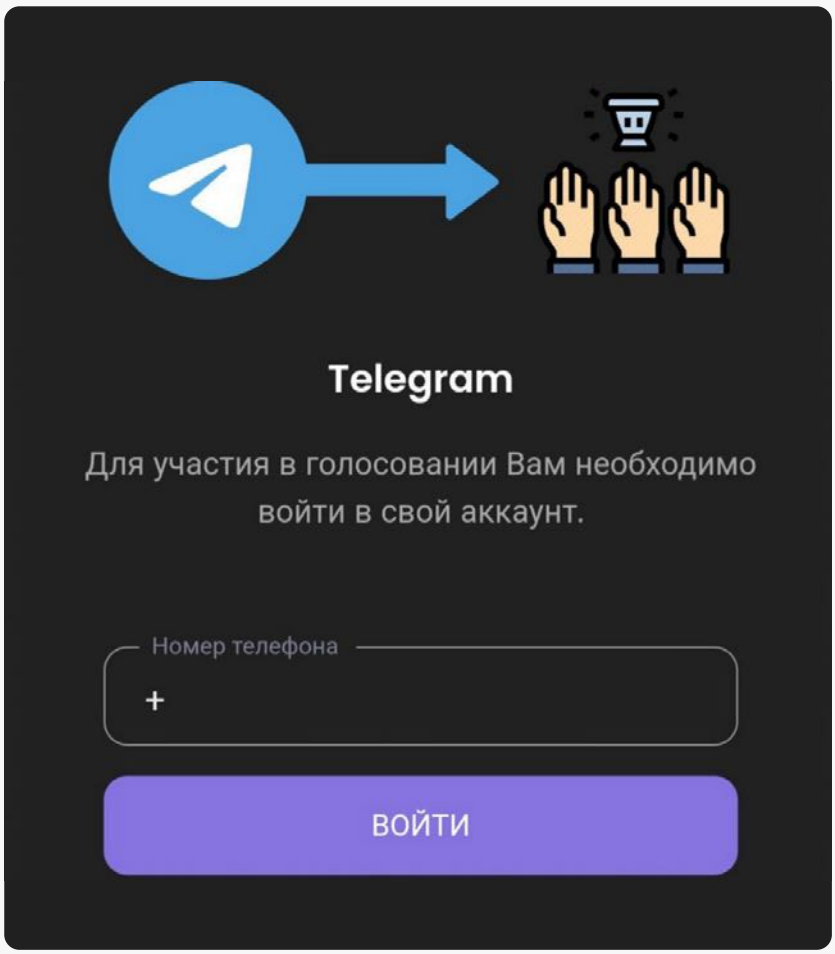


Рис. 52. Пример фишингового сайта для кражи учетных данных в Telegram

Платформы имеют схожие принципы работы и функциональность и способны поддерживать работу сотен пользователей. О количестве создаваемых таким образом ресурсов можно судить по тому, что с помощью только одной из платформ с января по июнь 2024 года было создано более 900 сайтов для кражи аккаунтов. Чаще всего фишинговые страницы были расположены в доменах .ru, .online, .shop, .site, .website.

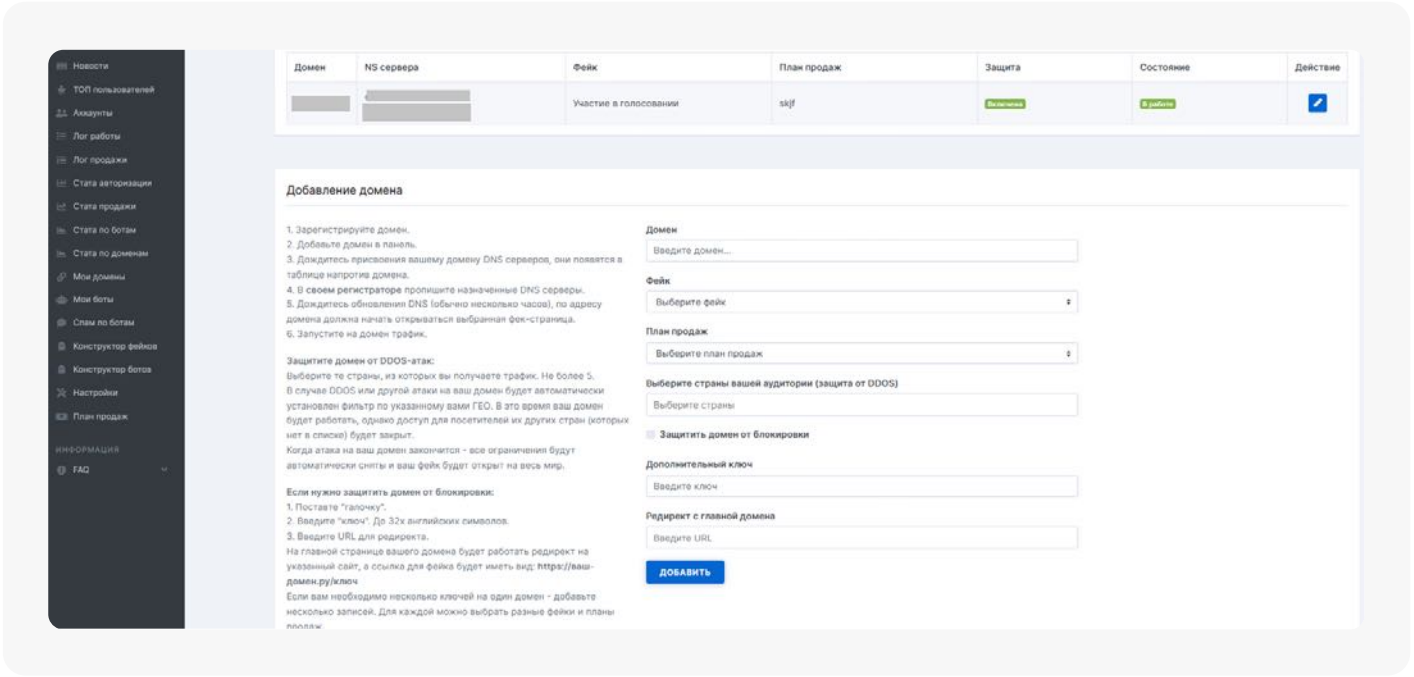


Рис. 53. Пример создания фишинга через панель

Злоумышленники стремятся использовать как новые поводы, например, вывод средств из игры Humster Kombat, фейковый сервис с нейросетью «Раздень подругу», так и проверенные временем уловки: денежные призы, бесплатные подписки, голосование, доступ в приватный канал и другие, побуждая пользователей вводить конфиденциальные данные на фейковых ресурсах. Украденные аккаунты продаются через маркеты в веб-панели или Telegram-ботов.

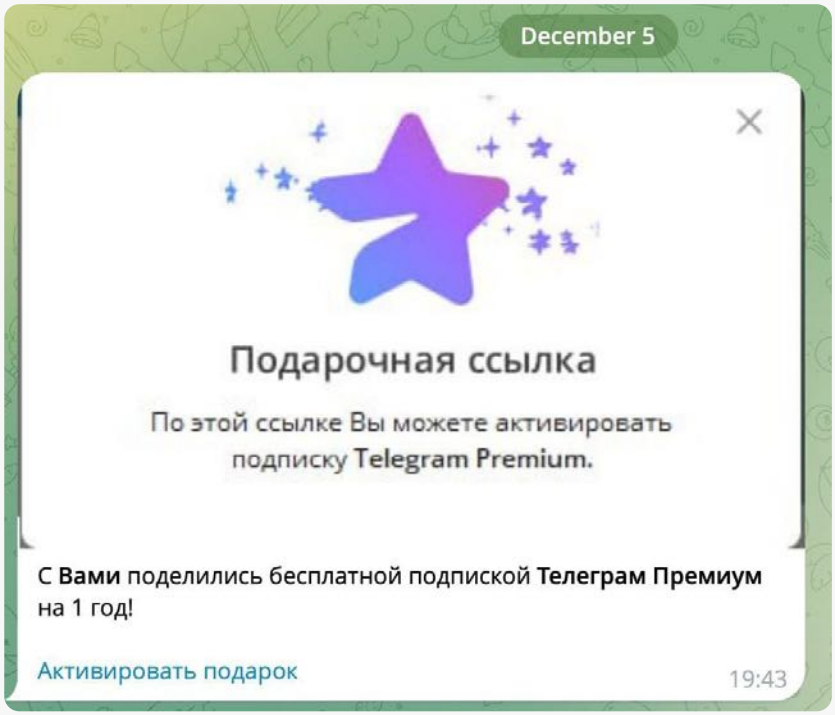


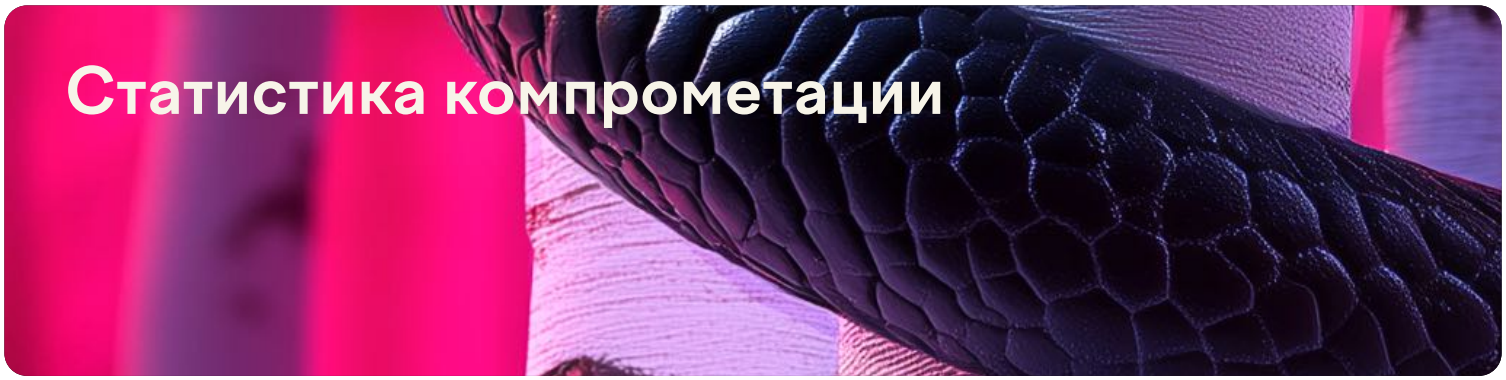
Рис. 54. Пример привлечения на фишинговый сайт под предлогом получения премиум подписки в Telegram

Средняя стоимость продажи логов на маркете форума составляет около 150 рублей. Цена украденного аккаунта зависит от того, есть ли подписка на premium, полномочия админа или владельца канала, количество диалогов, продолжительность «отлежки» (время с момента угона аккаунта, за которое он не был заблокирован или возвращен легитимному владельцу). Также на цене влияет «ситуация на рынке» — количество украденных аккаунтов на продажу.

Прибыль «топпера» — самого опытного и успешного участника группы по «угону» («тимы») — может составлять от 600 000 до 2 500 000 рублей в месяц, в зависимости от используемой панели.

Злоумышленники стремятся снизить трудозатраты на создание фишинговых ресурсов, пользуясь функциями фишинговых панелей и шаблонами. Это позволяет им концентрироваться на охвате большего количества жертв и оттачивать способы привлечения трафика. Фишинговые панели позволяют киберпреступникам не только пользоваться шаблонами, но и контролировать информацию об украденных аккаунтах, формировать планы продаж, отслеживать статистику и прочее.

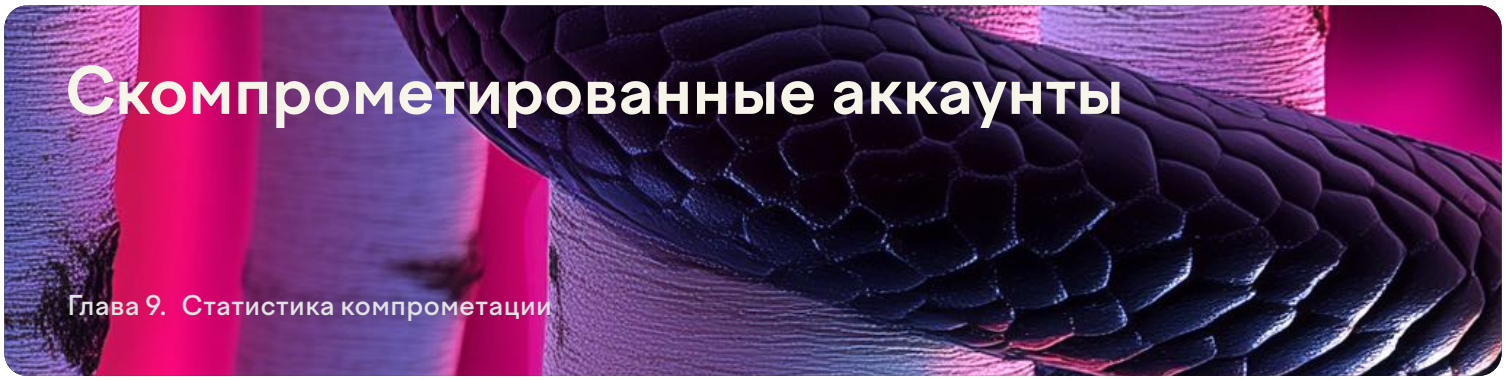
Статистика компрометации



Статистика компрометации

Приведем статистику по обнаруженным в 2024 году скомпрометированным данным, относящимся к пользователям из России и Беларуси. В настоящее время основным источником получения злоумышленниками скомпрометированных аккаунтов являются вредоносные программы-**стилеры**. В стилерах встроена функциональность невозможности работы в странах СНГ, однако, модифицируя код, злоумышленники могут отключать эту функцию. Впоследствии скомпрометированные данные злоумышленники используют или самостоятельно, или выставляют на продажу на **андеграундных маркетплейсах**, или такие данные попадают в продажу в **облака логов** от стилеров. Облака логов – это, как правило, закрытые Telegram-каналы или андеграундные форумы, зачастую платные, предоставляющие доступ к похищенной конфиденциальной информации.

В итоге скомпрометированная учетная запись может оказаться точкой входа для более серьезной атаки, особенно если был скомпрометирован корпоративный пользователь. Поэтому специалисты F6 настоятельно рекомендуют проводить мониторинг и реагирование на факты выявленных компрометаций. F6 Threat Intelligence позволяет получать информацию о скомпрометированных учетных записях из различных источников, что позволило нам получить следующую статистику за 2024 год.



Скомпрометированные аккаунты

За 2024 год Threat Intelligence было обнаружено следующее количество уникальных скомпрометированных учетных записей пользователей из России и Беларуси:

Количество уникальных скомпрометированных учетных записей пользователей из России и Беларуси

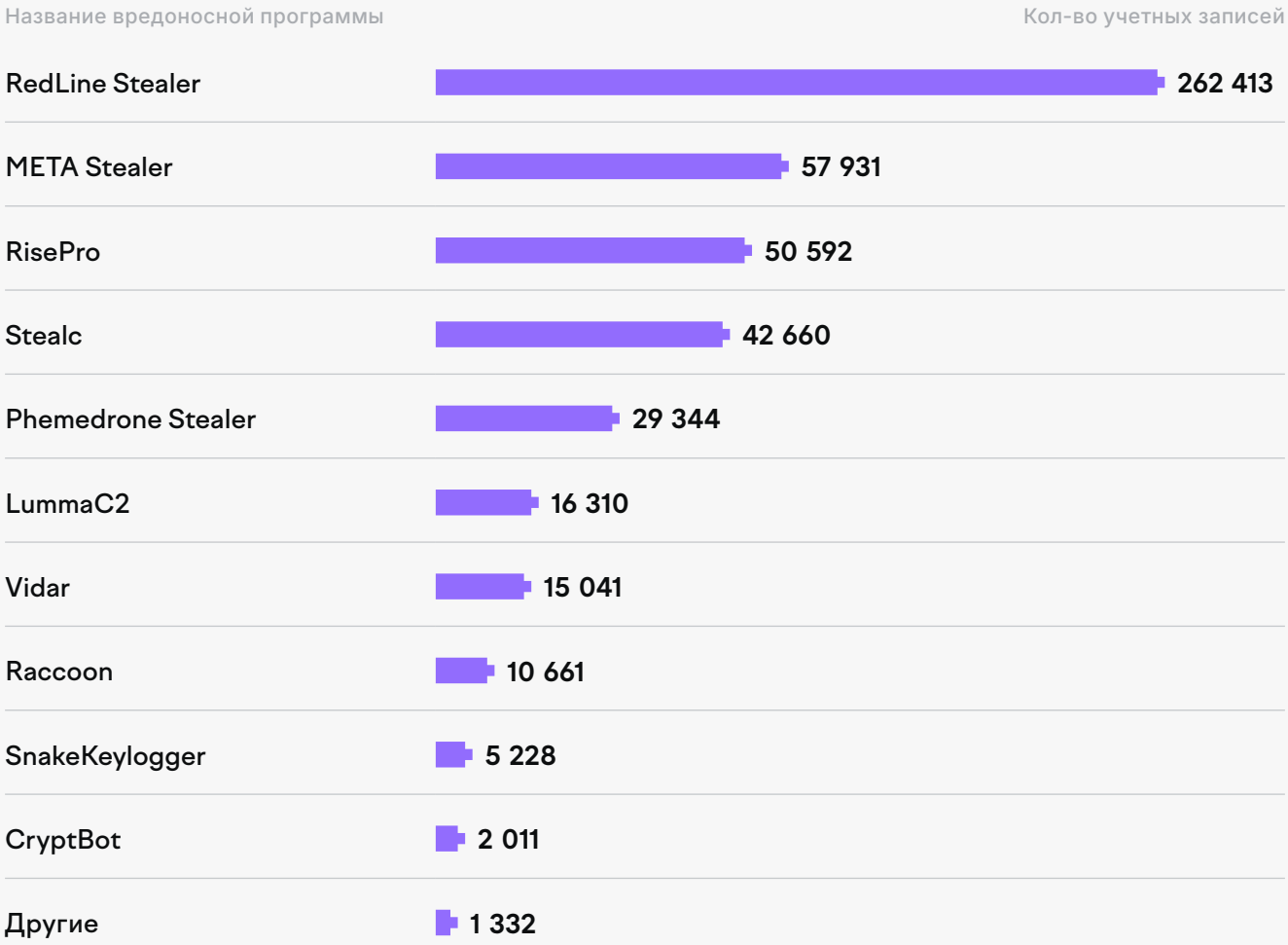
f6.ru

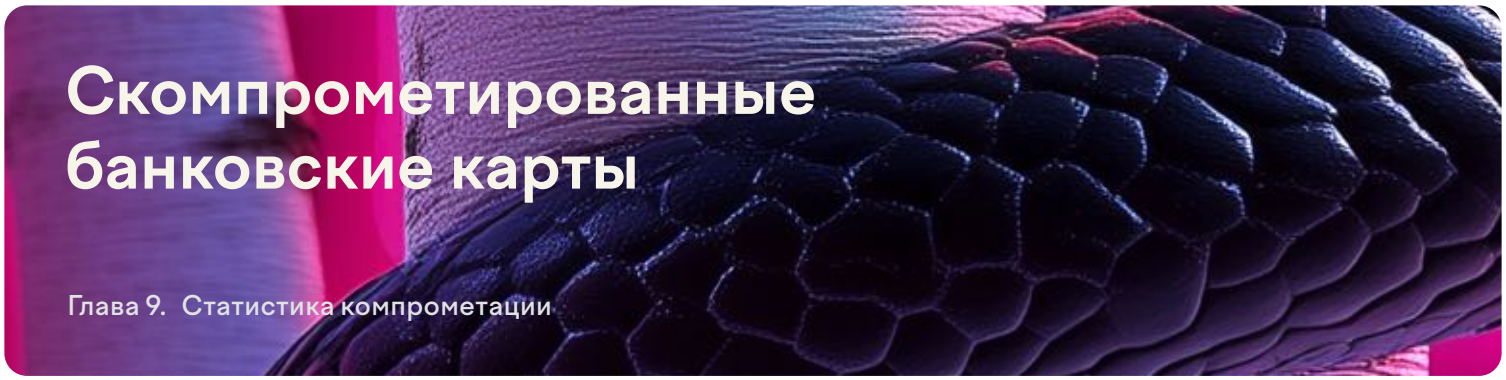
Страна	Кол-во учетных записей
Россия	322 930
Беларусь	91 865

Статистика по основным вредоносным программам, используемым для компрометаций в России и Беларуси 2024 году:

Статистика по основным вредоносным программам

f6.ru





Скомпрометированные банковские карты

Для компрометации банковских карт злоумышленники используют различные методы: фишинг, вредоносное программное обеспечение на устройстве жертвы (те же стилеры), JS-скрипты на сайтах, позволяющих совершать онлайн-платежи. Третий способ не является распространенным в России и странах СНГ, однако первые два активно применяются.

Скомпрометированные банковские карты затем зачастую публикуются злоумышленниками на андеграундных форумах, в Telegram-каналах, продаются в специализированных андеграундных магазинах (так называемых «кардшопах»). Система Threat Intelligence позволяет автоматизированно мониторить ряд источников и извлекать оттуда данные о скомпрометированных картах.

В 2024 году с помощью Threat Intelligence было выявлено **28 192** уникальных скомпрометированных карты клиентов банков из России и Беларуси.

Несмотря на то, что скомпрометированные данные российских и белорусских карт — это не самый популярный и «ходовой» материал на кардшопах, они встречаются в продаже в данных андеграундных магазинах.

Киберугрозы в России и СНГ.
Аналитика и прогнозы 2024/25

Рекомендации на 2025

Рекомендации на 2025

Для защиты от актуальных киберугроз рекомендуем неукоснительно выполнять приведенные ниже рекомендации:

- Проводить своевременное и регулярное обновление программного обеспечения, которое позволяет закрывать обнаруженные уязвимости.
- Настраивать многофакторную аутентификацию для учетных записей удаленных сервисов. Это ограничивает возможности использовать скомпрометированные учетные данные.
- Использовать для защиты конечных устройств решения класса EDR или XDR, например, F6 Managed Extended Detection and Response (MXDR), а также антивирусное программное обеспечение. Своевременно реагировать на все алерты — срабатывания и оповещения 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 для локальных и доменных учетных записей.
- 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 безопасности 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 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 осуществляется 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.
- Использовать минимальные привилегии для учетных записей служб — это ограничивает права, получаемые процессом, уязвимость в котором может быть использована.
- Осуществлять непрерывную идентификацию теневых ИТ для управления поверхностью атаки (теневые ИТ — системы и устройства, развернутые сотрудниками без ведома или одобрения ИТ-подразделений компании).
- 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.
- 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.
- Запретить пользователям регистрироваться на сторонних сервисах с использованием корпоративной почты.
- Отслеживать трафик DNS: некоторые разновидности вредоносного программного обеспечения требуют связи с сервером или C&C, вредоносное соединение может маскироваться под легитимный, трафик, в том числе по протоколу HTTP.
- Использовать различные пароли для локальных администраторов на всех хостах инфраструктуры. При компрометации отдельной машины это позволит не считать скомпрометированным весь задействованный сегмент.
- Проводить аудит нелегитимных сессий пользователей в Telegram.
- Ограничить возможность использования личных устройств 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 ритейнер 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.