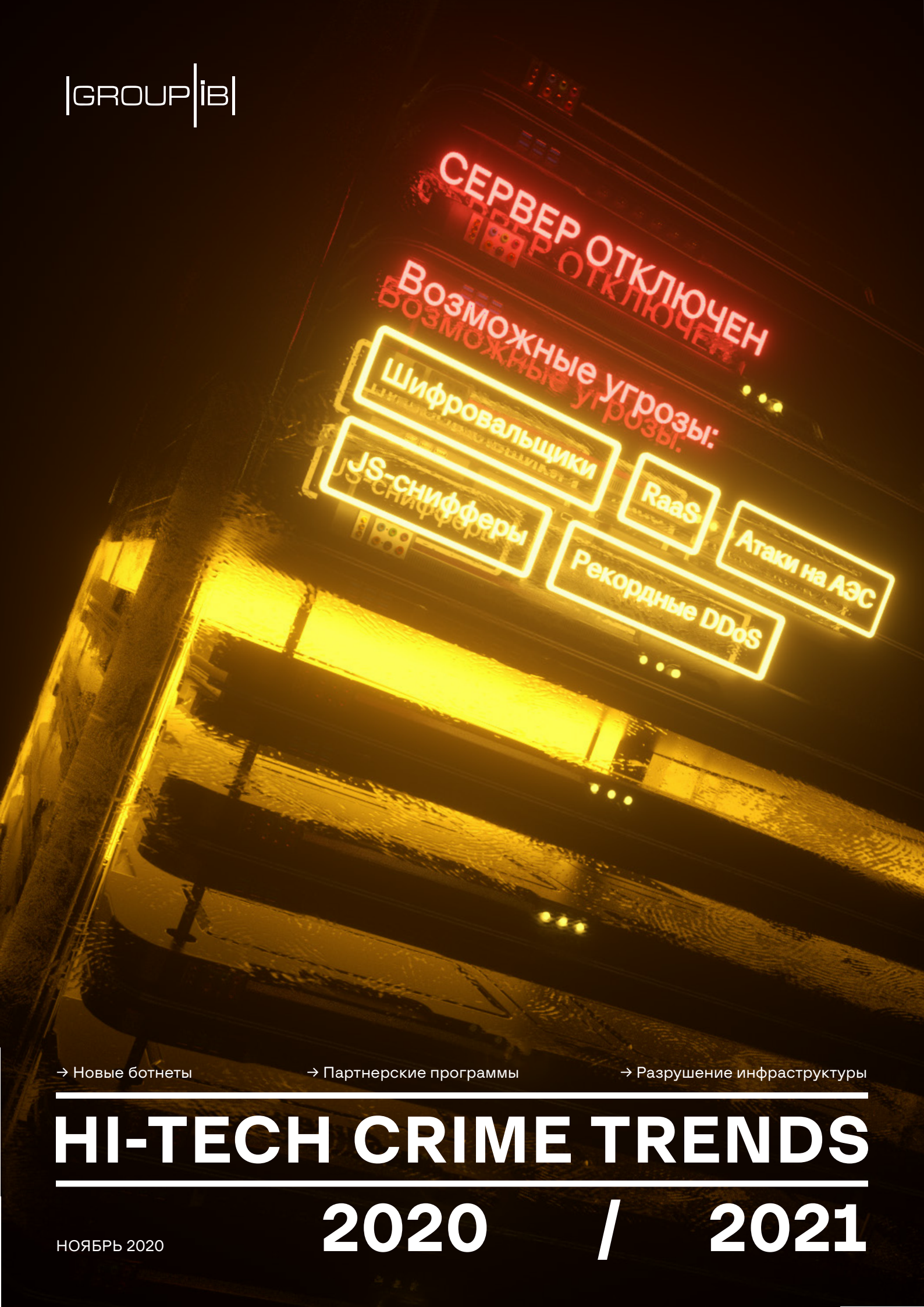


→ Новые ботнеты → Партнерские программы → Разрушение инфраструктуры

HI-TECH CRIME TRENDS 2020 / 2021

НОЯБРЬ 2020

1. Отчет подготовлен специалистами Group-IB без какого-либо финансирования третьими лицами.
2. Целью отчета является предоставление сведений о тактике, инструментах и особенностях инфраструктуры различных групп для минимизации риска дальнейшего совершения таких противоправных деяний, их своевременного пресечения и формирования у читателей должного уровня правосознания. В отчете приведены рекомендации от экспертов Group-IB по превентивным мерам защиты от атак групп. Описание деталей угроз в отчете приведено исключительно для ознакомления с ними специалистов по информационной безопасности с целью предотвращения возникновения подобных инцидентов в дальнейшем и минимизации возможного ущерба. Опубликованная в отчете информация об угрозах не является пропагандой мошенничества и/или иной противоправной деятельности в сфере высоких технологий и/или иных сферах.
3. Отчет подготовлен в информационных и ознакомительных целях, ограничен в распространении и не может использоваться читателем в коммерческих и иных, не связанных с образованием или личным некоммерческим использованием целях. Group-IB предоставляет читателям право использовать отчет на территории всего мира путем скачивания, ознакомления с отчетом, цитирования отчета в объеме, оправданном правомерной целью цитирования, при условии, что сам отчет, включая ссылку на сайт правообладателя, на котором он размещен, будет указан как источник цитаты.
4. Отчет и все его части являются объектами авторского права и охраняются нормами права в области интеллектуальной собственности. Запрещается его копирование, распространение полностью или в части, в том числе путем копирования на другие сайты и ресурсы в сети Интернет, или любое иное использование информации из отчета без предварительного письменного согласия правообладателя. В случае нарушения авторских прав на отчет Group-IB вправе обратиться за защитой своих прав и интересов в суд и иные государственные органы с применением к нарушителю предусмотренных законодательством мер ответственности, включая взыскание компенсации.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Когда мир сталкивается с неизвестной эпидемией, закрываются границы, бизнес балансирует на грани рентабельности, а политическое противостояние между странами приобретает все более острые формы, один показатель неизменно растет. Это уровень киберпреступности.

Начав исследовать эту область 17 лет назад, Group-IB все эти годы не только анализировала киберинциденты, отслеживала эволюцию тактик и инструментов атакующих, разрабатывала инновационные технологии для предотвращения киберугроз и охоты за киберпреступниками, но и обменивалась данными и делилась своими исследованиями с экспертным сообществом. Главной площадкой для презентации ежегодного аналитического отчета **Hi-Tech Crime Trends** стала международная конференция **CyberCrimeCon**.

В новом отчете **Hi-Tech Crime Trends 2020–2021** исследователи Group-IB назвали ключевые изменения, произошедшие в сфере высокотехнологичных преступлений, раскрыли аспекты функционирования киберкриминальной индустрии, связи между группами, развитие партнерских программ по продаже вредоносного ПО и различных сервисов. Традиционно Group-IB исследует атаки не только на коммерческий сектор, но и на объекты критической инфраструктуры, которые являются следствием скрытой деятельности спецслужб разных государств.

Именно этот отчет помогает получить ответы на главные вопросы: «Кто ваш противник в киберпространстве? Как он действует сегодня? Как будет развиваться его инструментарий для будущих атак? Как от них защититься?». Именно эти знания позволяют организациям во всем мире выстраивать эффективные стратегии кибербезопасности. **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 тем, кто может стать жертвой цифровых преступлений.

Паралич целых отраслей экономики, массовый перевод сотрудников на удаленный режим работы, массовые сокращения привели к всплеску компьютерной преступности, которая открыла для себя новые схемы и способы незаконного обогащения. Весной 2020 года эксперты Group-IB спрогнозировали рост числа финансовых мошенничеств и кибератак на компьютеры, оборудование (роутеры, видеокамеры) и незащищенные домашние сети сотрудников компаний. В группе риска в первую очередь оказались сотрудники финансовых учреждений, телеком-операторов и IT-компаний. Наши прогнозы, к сожалению, сбылись.

В период пандемии аналитики Group-IB отметили рост количества кибератак от прогосударственных хакерских групп и киберкриминала, эксплуатирующих тему COVID-19, с использованием шпионского ПО, шифровальщиков, бэкдоров. Злоумышленники искали способ проникновения в сети предприятий, адресно атакуя сотрудников, работающих удаленно, путем заражения их компьютеров вредоносными программами, через которые затем получали доступ в корпоративную сеть.

На фоне снижения количества успешных целевых атак на банки отмечен стремительный рост числа финансовых мошенничеств с использованием социальной инженерии (вишинга, фишинга), жертвами которых становились в основном клиенты банков. Основной мотив киберпреступников остался прежним — кража денег или информации, которую можно продать, но он приобрел новую «упаковку», адаптированную под актуальную повестку.

В этом году подавляющее большинство преступных групп переключилось на работу с шифровальщиками: с их помощью можно заработать не меньше, чем в случае успешной атаки на банк, а техническое исполнение — значительно проще. Набирает обороты Big Game Hunting — атаки на крупные компании с целью получения значительного выкупа, к которым присоединяются новые группировки, появляются коллаборации с другими представителями киберкриминального мира.

Активно развивался и рынок услуг Cybercrime-As-a-Service, связанный со сдачей в аренду компьютерных сетей, зараженных вредоносным программным обеспечением (ботнетов), используемых, например, при организации DDoS-атак, рассылке фишинговых писем и предоставлении прокси-серверов. Появляются новые продавцы доступов, которые вступают в партнерские отношения с операторами шифровальщиков; APT-группы, которые раньше занимались банковскими хищениями, теперь работают по приватным партнерским программам. Прогосударственные группировки также не игнорируют этот способ обогащения, открывая путь шифровальщикам к инфраструктуре крупных компаний. Эта угроза приобрела колоссальные масштабы и теперь актуальна для каждой компании, независимо от отрасли и географической принадлежности.

Мы уверены, что постоянный обмен данными, совместные усилия по поддержанию киберстабильности в мире, создание и развитие партнерских отношений между частными компаниями и международными правоохранительными органами — эффективный путь борьбы с киберпреступностью. Осознанное отношение мирового сообщества к кибербезопасности поможет сохранить и защитить глобальные возможности цифрового пространства и свободу коммуникаций.

КЛЮЧЕВЫЕ ВЫВОДЫ И ПРОГНОЗЫ

Атаки с использованием шифровальщиков

Существующие угрозы

Основная цель:

открыть доступ в корпоративные сети для шифровальщиков

Партнерские программы операторов шифровальщиков

формируют рынок по продаже доступов в корпоративные сети

— За последний год появилось 7 из 15 партнерских программ для атак на компании от операторов шифровальщиков, что сформировало рынок продажи доступов в корпоративные сети.
— В интервале H2 2019 — H1 2020 количество выставленных на продажу доступов увеличилось в 2,6 раза. Если за прошлый период было 138 подобных лотов, то за текущий — 362.
— Растет и количество злоумышленников, активно продающих доступы в корпоративные сети. В 2019 году было 50 активных продавцов, а в первой половине 2020 года их уже 63.
— Владельцы банковских бот-сетей TrickBot, Qbot, Silent Night, RTM начали использовать свои бот-сети для установки программ-шифровальщиков.
— Предположительно, группы Cobalt и Silence, которые ранее специализировались на целенаправленных атаках на банки, стали участниками приватных партнерских программ с шифровальщиками.
— В числе основных проблем для компаний — уязвимые версии программного обеспечения в публичных сервисах или слабые пароли. В случае компрометации цель атакующих состоит в нанесении максимального ущерба бизнесу с последующим вымогательством.
— 10 из 15 партнерских программ с шифровальщиками используют перебор паролей на RDP. Три из них также активно эксплуатируют уязвимости в VPN-сервисах.
— Появляются новые бот-сети, которые осуществляют распределенный перебор паролей к интерфейсам удаленного доступа (RDP, SSH, VPN) и другим сервисам.
— Одним из основных способов мотивировать жертву заплатить выкуп стала кража данных из сети и угрозы их последующей публикации в открытом доступе.
— Для увеличения прибыли некоторые группы не просто выкладывают данные, а проводят аукционы по их продаже.
— Шифровальщики стали настолько популярны, что в открытом доступе на GitHub стали публиковать готовые проекты Ransomware-As-A-Service для Linux, MacOS и Windows, например проект RAASNet.
— Для развития атак и получения контроля над корпоративной сетью используются два основных фреймворка для постэксплуатации: бесплатный Metasploit либо взломанная версия Cobalt Strike, значительно реже — фреймворки PoshC2 или Koadic. За H2 2019 — H1 2020 было обнаружено более 10 тыс. хостов с такими фреймворками против 6 тыс. за аналогичный период H2 2018 — H1 2019.
— Наиболее подверженными атакам странами стали США, Великобритания, Канада, Франция и Германия. На них пришлась 381 атака из 505, что составило 75%.
— Самой атакуемой отраслью стало производство. Половина всех атак пришлась на сферы торговли, здравоохранения, строительства, образования и государственные сервисы.
— Появились шифровальщики, нацеленные на остановку процессов, связанных с приложениями технологический сетей. Это позволяет им более эффективно шифровать ценные данные производственных предприятий.

Прогнозы

— Ожидается появление специализированных торговых площадок для выставления лотов с доступами в корпоративные сети, что может привести к еще большему росту инцидентов.
— Произойдет рост спроса на вредоносный код для Linux, необходимый для эффективного закрепления в сети и повышения привилегий.
— Владельцы IoT-ботнетов могут начать продавать доступ к устройствам, которые установлены в корпоративных сетях.
— Появятся новые бот-сети и криминальные сервисы на их основе для распределенного перебора паролей к интерфейсам удаленного управления.
— Произойдет кратковременный рост числа партнерских программ операторов шифровальщиков. Однако мы ожидаем, что уже в 2020 году рынок стабилизируется и их рост прекратится.
— Могут появиться случаи атак вымогателями именно почтовой системы компании. Они могут похищать данные локальных почтовых серверов и выводить систему из строя, поскольку работа электронной почты является критичной для ведения бизнеса. Это может привести к росту популярности облачных почтовых сервисов и отказу от модели on-prem хранения почты.
— Могут появиться группы, которые будут специализироваться на атаках именно на промышленные предприятия, получать доступ к SCADA-системам, чтобы манипулировать процессом производства.
— Спецслужбы могут заинтересоваться владельцами партнерских программ, чтобы использовать их для доступа к интересующим сетям.
— Спецслужбы для нанесения максимального урона своим жертвам и отвлечения внимания от своих атак могут начать действовать как криминальные структуры: активно выкладывать документы, подрывающие бизнес атакованной организации, продавать доступы в корпоративные сети.

Военные операции

Существующие угрозы

Все чаще шпионаж сменяется активными попытками уничтожения

объектов инфраструктуры

Среди значимых объектов атак:

ядерные объекты Ирана и Индии
и система водоснабжения Израиля

— Спецслужбы все чаще переводят атаки в более активные фазы, когда целью является не только шпионаж, но и вывод объектов критической инфраструктуры из строя.
— За текущий период было обнаружено семь новых APT-групп, а также выявлена активность шести ранее известных групп, которые оставались незамеченными последние несколько лет.
— В результате таких операций атакующим удавалось, например, добиться остановки энергоблоков на предприятиях атомной энергетики, физически уничтожить прилегающую инфраструктуру.
— Была зафиксирована атака на водоочистительные комплексы, предполагаемой целью которой было изменение уровня хлорирования воды, что могло привести к человеческим жертвам.
— Лидеры некоторых государств начали открыто заявлять об успешно проведенных атаках на территориях других стран.

Прогнозы

— Из-за обострения обстановки на Ближнем Востоке, возможно, будут проведены первые атаки на системы управления транспортными судами в Персидском заливе.
— Ожидается увеличение количества диверсионных операций на объектах критической инфраструктуры Ирана, особенно связанных с ядерной программой.
— Более активное развитие функции обнаружения закладок на уровне UEFI вендорами по безопасности может позволить обнаружить новые угрозы в UEFI, используемые в военных операциях.
— Новые успехи в космической отрасли компаний Илона Маска могут привлечь внимание спецслужб как в плане шпионажа, так и для получения контроля над системами управления спутниковой связи.

Угрозы в телекоммуникационном секторе

Существующие угрозы

Прогосударственные группировки

проявляют к телеком-сектору особый интерес, реализуя изощренные атаки

2,3 Тб/с и 809 млн пакетов в секунду

новые рекорды мощности DDoS-атак

— За анализируемый период в телекоммуникационном секторе проявляли активность 6 групп, связанных с спецслужбами.
— Китай наращивает свои возможности по шпионажу за операторами мобильной связи. Для этого был разработан специальный троян для Linux-серверов, который позволяет перехватывать SMS-сообщения по определенным критериям.
— Установлены новые рекорды мощности DDoS-атак: 2,3 Тб/с и 809 млн пакетов в секунду.
— Пока сети 5G не применяются широко, прогнозы по связанным с ними угрозами не оправдываются, однако они сохраняют потенциальную актуальность для последующего периода.
— Значительной проблемой остается перехват BGP или утечка BGP-маршрутов. За последний год было публично зафиксировано девять значимых случаев.

Прогнозы

— Учитывая нарастающие противостояния между государствами, ожидается, что будут зафиксированы первые атаки на операторов связи с целью вызова логической перегрузки сети, что приведет к каскадному эффекту и повлияет на множество секторов экономики.
— В связи с массовым переходом сотрудников компаний на удаленный режим работы, который, возможно, сохранится даже после пандемии, количество атак на домашние роутеры и системы хранения данных возрастает, поскольку они позволяют продвинутым и прогосударственным атакующим более эффективно получать доступ к корпоративным данным, не проникая в периметр организации.

Угрозы в энергетическом секторе

Существующие угрозы

Останавливать объекты и шифровать данные ради выкупа

готовы как спецслужбы, так и обычный криминал

Воздушный зазор (air gap) преодолен:

обнаружены новые инструменты атак на изолированные сети

— Арсенал атакующих активно пополняется инструментами для атак на физически изолированные сети. За последний год было обнаружено четыре инструмента, использующих USB-носители для преодоления воздушного зазора (air gap).

— Ядерная энергетика стала явной целью атакующих. Если в прошлом году в публичном пространстве не было зафиксировано ни одной атаки, то в этом на объекты ядерной энергетики Ирана нападали с целью саботажа, а в Индии — с целью шпионажа. Последняя привлекательна как страна, развивающая ядерную технологию и реакторы на основе тория.

— За год не было выявлено ни одного нового фреймворка, способного влиять на технологические процессы, что говорит о более тщательном сокрытии их использования в атаках.

— Обычный криминал начал активно проявлять интерес к энергетическим компаниям. Проводятся целенаправленные атаки с захватом контроля над всей сетью с целью заражения их инфраструктур программами-шифровальщиками.

— За анализируемый период активность в энергетическом секторе проявили 9 групп, связанных с спецслужбами, семь хакеров, продающих доступ в энергетические сети, а также известно об 11 случаях успешных атак с использованием шифровальщиков.

— В некоторые программы-шифровальщики добавлены функции обнаружения процессов, связанных с системами управления промышленными предприятиями, чтобы обеспечить потерю данных, с которыми они работают, и повысить цену за возможность восстановления доступа. Особенно это относится к данным Historian-серверов.

Прогнозы

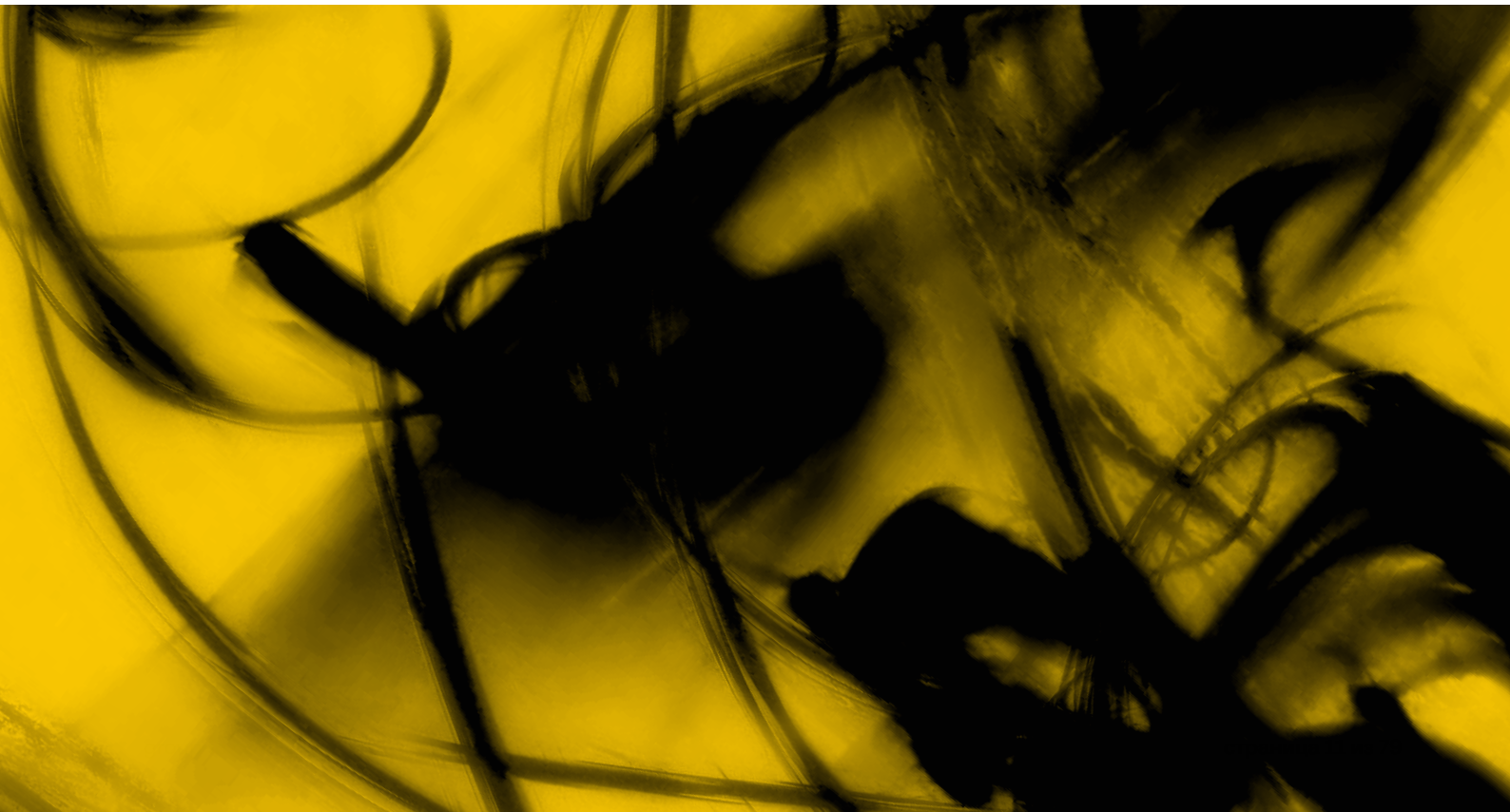
— Основной целью атакующих, спонсируемых государствами, останется шпионаж.

— Атаки на энергетический сектор с целью саботажа будут проводиться на Ближнем Востоке или в странах с новыми военными конфликтами.

— Для более эффективных атак злоумышленники будут нападать не только на крупные энергетические компании, но и на небольших операторов, обеспечивающих доставку электроэнергии на последней миле или оказывающих дополнительные услуги крупным энергетическим компаниям.

— Сети 5G подключат большое количество устройств, в т. ч. энергетических и промышленных предприятий, к глобальным сетям. В этом случае значительно увеличится поверхность атаки.

— Вектор проникновения через уязвимое сетевое оборудование будет использоваться чаще и в основном более продвинутыми атакующими. Злоумышленники с меньшим уровнем навыков будут использовать стандартные схемы с фишингом.



Угрозы в банковском секторе

Существующие угрозы

Целевые хищения становятся редким явлением,
актуальным для слабо защищенных банков

Получение доступа и шифрование данных ради крупного выкупа
является трендом для банковского сектора

— В 2020 году не было зафиксировано ни одного публичного сообщения о хищении через SWIFT, ATM Switch, платежные шлюзы или ATM, когда доступ к ним был получен через сеть банка.
— Однако известно, что группа Lazarus продолжала совершать попытки хищений через SWIFT, и для первоначального проникновения они использовали банковскую бот-сеть Trickbot, управляемую русскоговорящими киберпреступниками. Кроме того, были зафиксированы действия еще одной команды, использующей общедоступные трояны, кейлогеры и эксплойты без какой-либо модификации. Такой набор инструментов характерен только для атак на банки с минимальным уровнем безопасности, либо же их ошибочно определили специалисты, реагирующие на инцидент.
— Во второй половине 2019 года успешные хищения, не связанные со SWIFT, провела только группа Silence, но в 2020 году они перестали атаковать финансовую отрасль.
— В сентябре 2020 года был ограблен филиппинский банк United Coconut Planters Bank (UCPB), контролируемый государством. Атакующим удалось получить доступ к карточному процессингу и изменить лимиты, а также доступ к системе межбанковских переводов InstaPay. В результате они смогли вывести из банка 167 млн песо ($3,44 млн).
— Незначительное развитие получили инструменты целенаправленных атак на банкоматы. За отчетный период были выявлены ATMDtrack от Lazarus и новая модификация ATM-трояна от группы Silence, однако об их успешном применении в реальных хищениях ничего не известно.
— Предположительно, и Cobalt, и Silence стали участниками приватных партнерских программ операторов шифровальщиков, при этом банки перестали быть их основным фокусом.

Прогнозы

— В следующем году не ожидается большого количества традиционных атак на банки с целью хищений. Редкие инциденты возможны, но широкой практики, как раньше, не будет.
— Как и в других отраслях, большую угрозу будут представлять группы, занимающиеся шифрованием данных, что подтверждается участившимися случаями продаж доступов к корпоративным сетям финансовых учреждений.
— Более серьезной проблемой, чем шифрование данных, может стать хищение информации о финансовых транзакциях VIP-клиентов и появление таких сведений в открытом доступе. Это может нанести значительный финансовый ущерб и побудить пострадавшие банки более активно платить атакующим.
— Разглашение данных о финансовых транзакциях может запустить серию журналистских расследований по аналогии с «Панамской утечкой» (Mossack Fonseca) в 2015 году, в чем будут заинтересованы некоторые спецслужбы.
— Другим трендом могут стать оповещения атакующими финансовых регуляторов о том, что банк имеет проблемы с безопасностью. Подобные действия могут послужить стимулом для выплат вымогателям более высоких сумм.

Угрозы в ретейле

Существующие угрозы

96 семейств JS-сниффферов

отслеживают специалисты Group-IB на данный момент

На 156% больше дампов банковских карт,

полученных через POS-трояны, выставлено на продажу в этом году по сравнению с предыдущим

— Для ретейла можно выделить четыре основные угрозы, которые могут привести к потерям для бизнеса: атаки с помощью JS-сниффферов, атаки на POS-терминалы, credential stuffing и атаки с помощью шифровальщиков.

— Количество известных семейств JS-сниффферов выросло с 38 до 96 по сравнению с прошлым годом.

— Прогосударственная группа Lazarus также начала использовать JS-сниффферы. При этом используется модификация, которая позволяет им автоматически похищать денежные средства с Bitcoin-кошельков.

— Значительно улучшились техники, затрудняющие обнаружение JS-сниффферов на веб-ресурсах.

— Общий рынок кардинга вырос в два раза, с $880 млн до $1,9 млрд, по сравнению с прошлым годом. Количество предлагаемых к продаже текстовых данных банковских карт выросло с 12,5 до 28,3 млн.

— За отчетный период была обнаружена активность 14 POS-троянов, с помощью которых было скомпрометировано и впоследствии выставлено на продажу 63,7 млн дампов банковских карт, что на 156% больше, чем в прошлом году.

— За год удалось выявить 19 скомпрометированных сетей ретейлеров. В прошлом году их было 17.

— В основном целью мошенников являются банковские карты, выпущенные в США — на их долю приходится более 92% всех дампов, затем идут Индия и Южная Корея.

— Самым распространенным инструментом атак на ретейлеров являются боты без браузеров, открывающие новые возможности для обхода средств защиты и развития рынка киберпреступности в этом направлении.

Прогнозы

— Большое количество онлайн-ресурсов взламывается ежедневно, и одним из основных средств монетизации является продажа баз данных или размещение фишинговых страниц. Но потери для бизнеса и доходы злоумышленников могут значительно увеличиться, если последние станут активно сотрудничать с разработчиками шифровальщиков.

— Хакерские группы, использующие JS-сниффферы, будут представлять основную угрозу для онлайн-ретейла, особенно в США. При этом основные риски бизнеса будут связаны со штрафами за нарушение безопасности, а не с возмещением ущерба клиентам или репутационными потерями.

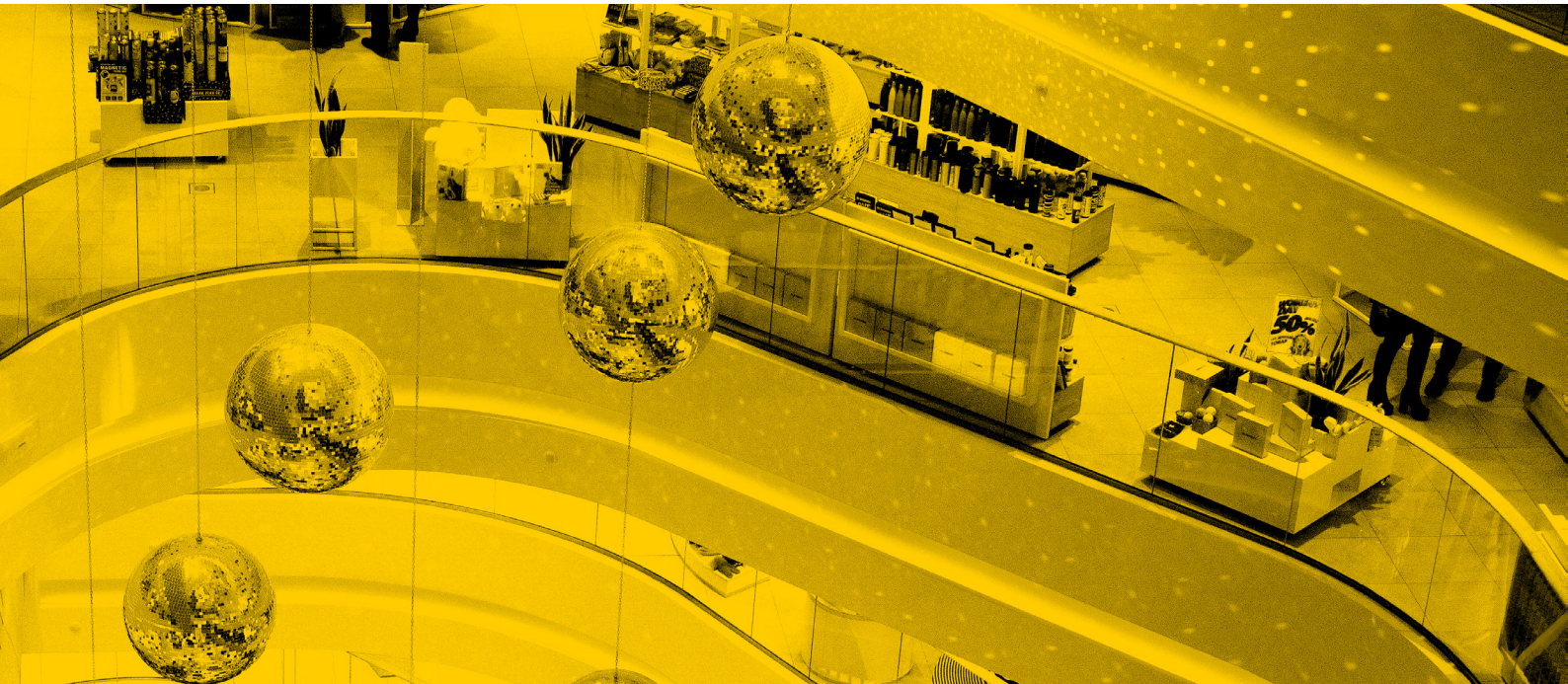
— Для США по-прежнему большой проблемой остается угроза атак на компьютеры с подключенными POS-терминалами для сбора дампов банковских карт.

— Уже есть отработанная схема, когда мошенники совершали финансовые операции в одном месте, а потом использовали доступ к POS-терминалам в других странах для отмены этих операций. Это восстанавливало баланс на карте, и атакующие могли продолжать совершать финансовые операции. Аналогичные схемы могут появиться и при использовании доступа к онлайн-ресурсам с подключенным приемом платежей.

— Несмотря на рост рынка кардинга, задержание основных его игроков может привести к остановке его развития и перераспределению активности между мошенниками.

— Основные схемы получения банковских карт и атакуемые страны (США, Индия, Южная Корея и др.) останутся без изменений.

— Новым регионом с растущей активностью кардеров может стать Латинская Америка, где уже достаточно сильно сообщество хакеров и накоплен опыт использования финансовых троянов.



Банковские трояны

Существующие угрозы

19 троянов для ПК и 10 для Android
были активны в этом году

Владельцы банковских бот-сетей
переключаются на шифровальщики

— Основной точкой роста банковских троянов стала Латинская Америка, и прежде всего Бразилия.
— Русскоговорящие владельцы крупнейших банковских бот-сетей (Trickbot, Dridex, Qbot, Silent Night) следуют основному тренду и переключаются на использование шифровальщиков.
— Всего в этом году активность проявляли 19 банковских троянов для ПК, 12 из которых разработаны русскоговорящими авторами, шесть — злоумышленниками из Латинской Америки и один не был атрибутирован.
— За отчетный период была зафиксирована активность десяти банковских Android-троянов, пять из которых являются новыми.

Прогнозы

— Русскоговорящие владельцы банковских бот-сетей под ПК и под Android еще больше снизят свою активность, и эти бот-сети перестанут существовать.
— В связи с растущей активностью банковских троянов в Латинской Америке мы ожидаем, что часть их владельцев будет арестована, что также повлечет минимизацию этой угрозы.
— Каждый год с рынка уходят 3–5 банковских бот-сетей для ПК. Такими темпами рынок банковских троянов для ПК может исчезнуть через 3–5 лет. Аналогичная ситуация ждет и рынок Android-троянов, эффективность которых снижается год за годом.

Веб-фишинг и социальная инженерия

Существующие угрозы

118% рост

фишинга в этом году по сравнению с предыдущим периодом

Новые тренды:

использование одноразовых ссылок на фишинговый сайт

— За год было выявлено и заблокировано на 118% больше фишинг-ресурсов по сравнению с предыдущим отчетным периодом.
— Пандемия спровоцировала вовлечение большего количества людей в исполнение фишинговых атак, что стало одной из причин роста этой угрозы.
— Во II квартале 2020 года было замечено увеличение фишинга, нацеленного на букмекерские конторы: 6% против 2% за предыдущий квартальный период.
— Еще одной категорией с 9%-ростом стал фишинг для сбора учетных записей различных онлайн-сервисов, например Microsoft, Netflix, Amazon, eBay, Valve Steam и т. п.
— Практически исчезли фишинг-ресурсы, нацеленные на криптовалютные проекты.
— Трендом этого года стало использование одноразовых ссылок: пользователь получает уникальную ссылку, которая становится неактивной после первого открытия. Так злоумышленники защищаются от обнаружения веб-фишинга.
— В России основной причиной значительного роста стали различные партнерские программы, объединявшие желающих заработать на фишинге вокруг тем, связанных с выплатой бонусов от банков, розыгрышей лотереи, прохождением платных опросов и т.п.
— Распространение и популярность в России проектов Phishing-as-a-Service.

Прогнозы

— Фишинговые партнерские программы, получившие популярность в России, будут более активно использоваться в других регионах.
— Автоматизация и увеличение продолжительности фишинговых атак благодаря появлению скам-проектов, распространяющихся по развивающейся модели Phishing-as-a-Service.
— Одной из самых больших проблем для ИБ-индустрии будет использование атакующими одноразовых ссылок на веб-фишинг.

ОСНОВНЫЕ ТЕНДЕНЦИИ

Получение доступа в корпоративные сети для шифровальщиков

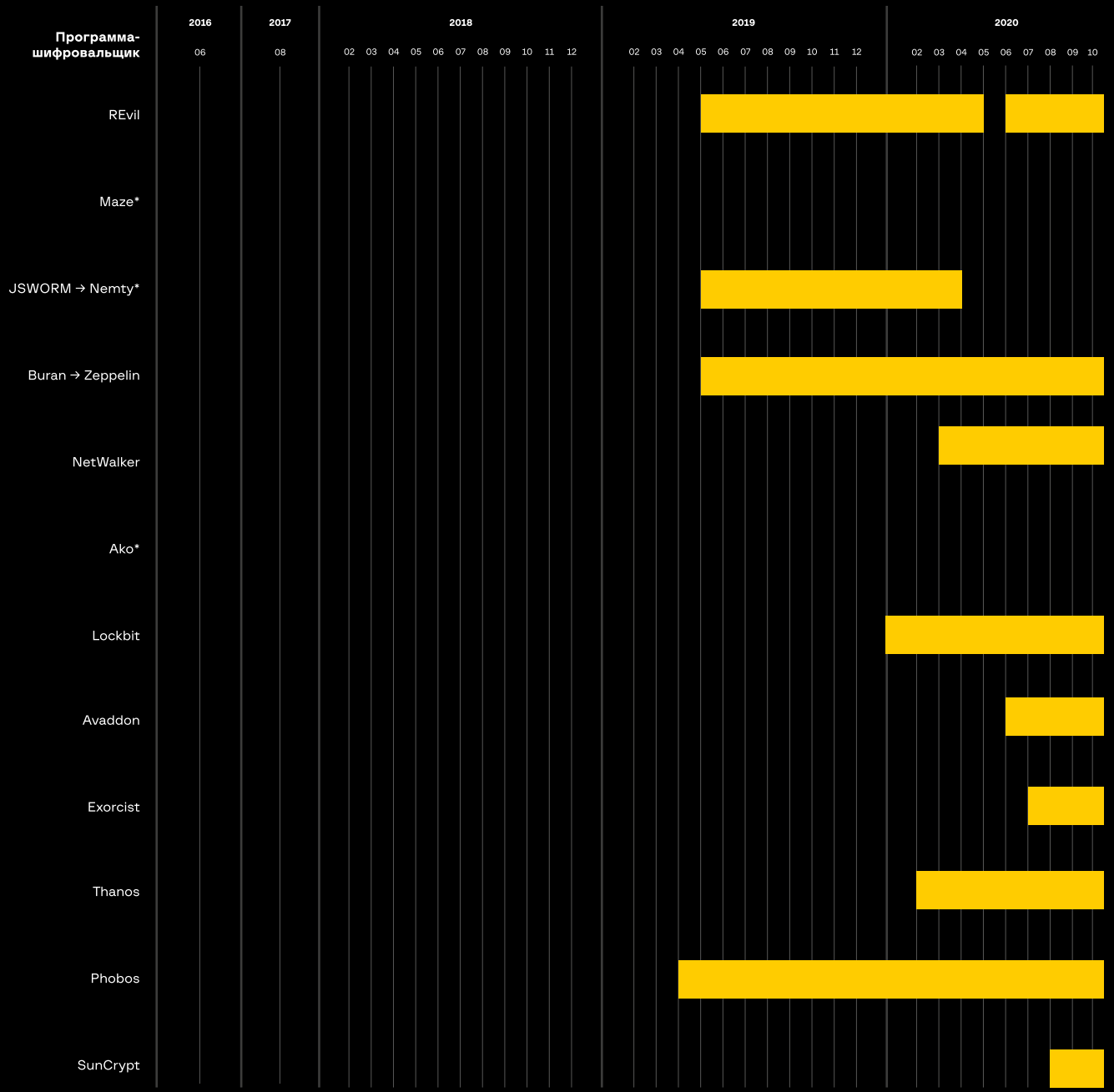
Появление партнерских программ шифровальщиков

В 2019 году многие операторы Ransomware отошли от атак на обычных пользователей и переключили свое внимание на компании из различных отраслей и государственные органы. Атаки на таких жертв сулят злоумышленникам куда большую выгоду.

Но не всегда у разработчиков шифровальщиков есть средства и возможности для проникновения в корпоративные сети. Для решения этой проблемы они начали открывать партнерские программы. Злоумышленники, которые специализируются на проникновении в корпоративные сети, могут монетизировать свои действия с помощью распространения шифровальщиков. После того как жертва выплачивает злоумышленникам выкуп, авторы шифровальщиков отправляют процент от этой суммы такому партнеру.

Существуют партнерские программы двух типов — публичные и приватные. Публичные программы начали появляться в середине 2019 года, и их отличительной особенностью является открытый поиск партнеров на андерграундных форумах. Приватные партнерские программы не афишируются и рассчитаны на сотрудничество с другими группами злоумышленников (например, APT-группами) и проверенными пользователями.

В таблице представлена информация о партнерских программах наиболее популярных шифровальщиков.

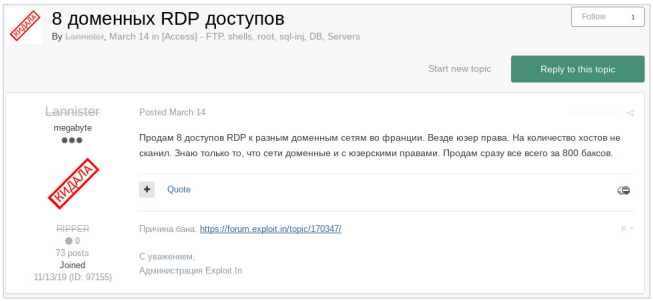


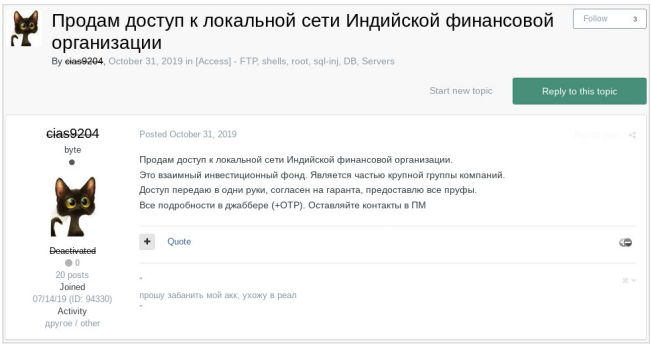
* Приватная партнерская программа

Многие партнеры предпочитают не афишировать свою деятельность, но анализ активности в хакерском сообществе, а также информации, полученной в результате реагирования на инциденты, позволяет обнаруживать некоторых из них. Часть из интересующихся партнерскими программами занимаются либо продажей доступов, либо работой с различным вредоносным ПО (в том числе стиллерами).

Скриншоты с примерами объявлений о продаже доступа приведены ниже (рис. 1-2).

Рисунок 1-2. Объявления с продажей доступа





Векторы компрометации

Обычно существует два изначальных вектора атаки:

- Вредоносные рассылки
- Получение доступа к внутренней сети через компрометацию аутентификационных данных к RDP
- Эксплуатация публично доступных приложений, связанных в том числе с VPN.

Помимо этого, для распространения шифровальщиков были обнаружены и другие методы: эксплойт-киты, VPN, ботнеты, другое вредоносное ПО (например, загрузчики).

Крайне редко встречается атака на цепочку поставок (supply chain), например, такая была замечена у REvil.

В целом данные способы доставки актуальны для любых шифровальщиков, в том числе для тех, которые распространяются без партнерских программ.

Ниже приведена таблица с партнерскими программами шифровальщиков и способами получения первоначального доступа, которые используют их операторы.

Шифровальщик	Phishing	Exploit Public-Facing Application	External Remote Services	Supply Chain Compromise
REvil	●	●	●	●
MegaCortex	●		●	
Maze	●	●	●	
Dharma			●	
JSWORM → Nemty	●	●	●	
Buran Zeppelin	●	●	●	
NetWalker	●		●	
Ako	●	●	●	
Lockbit			●	
Avaddon	●	●		
Thanos	●		●	

После компрометации

После изначальной компрометации многие операторы шифровальщиков сначала пытаются получить более высокие права доступа (с помощью эксплоитов или пост-эксплуатационных фреймворков), а после этого производят попытку получить доступ к другим учетным записям с помощью различного ПО (например, Mimikatz, LaZagne) или брутфорса.

Также производится разведка сети с использованием вполне легитимных сканеров сети или фреймворков (например, Cobalt Strike, Metasploit). Это позволяет узнать информацию о системе, группах, сетевых ресурсах, политике паролей, domain trust relationships и т. п. Ниже представлена таблица использования различных фреймворков операторами шифровальщиков.

Шифровальщик	Cobalt Strike	Metasploit	CrackMapExec	PoshC2	Koadic	PowerShell Empire
Ryuk	●	●				●
REvil		●	●			
MegaCortex	●					
Maze	●					
DoppelPaymer				●	●	
Clop	●	●				
Lockbit			●			

Кража и публикация данных

Если поначалу злоумышленники только шифровали данные и требовали выкуп у пользователей, то с конца 2019 года у многих появилась новая техника: теперь перед шифрованием они копируют всю информацию на свои серверы с целью дальнейшего шантажа. Обычно для этого используются стандартные протоколы — HTTP, HTTPS, FTP, и легитимные облачные хранилища. В редких случаях задействуются электронная почта и мессенджеры.

Теперь, если жертва не заплатит выкуп, она не только потеряет данные: операторы шифровальщика еще и опубликуют их в свободном доступе. Для этого создаются специальные веб-сайты (обычно в onion-сети). Пример подобного сайта показан ниже (рисунок 3).

В июне 2020 года **REvil** начали проводить аукционы, где в качестве лотов выступали украденные данные (рисунок 4).

Рисунок 3. Потерянные данные отправляются в свободный доступ

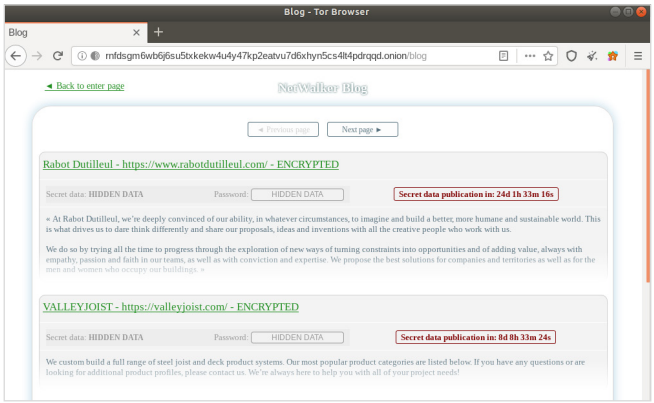
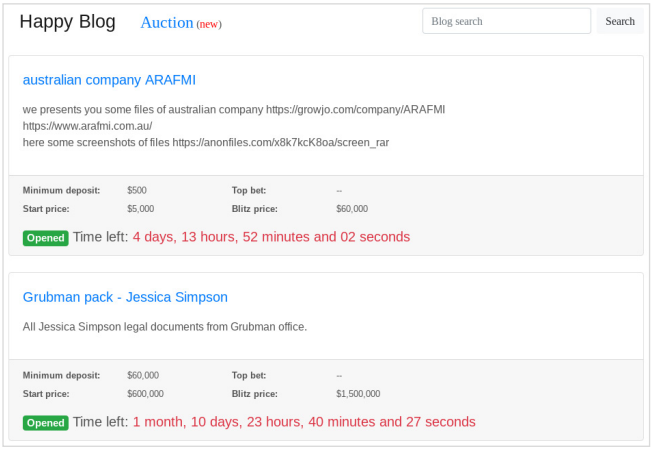


Рисунок 4. Аукцион REvil



Статистика атак

Среди жертв шифровальщиков есть как небольшие локальные компании, так и международные гиганты. Всего за последний год известно о более чем 500 успешных атаках известных шифровальщиков на компании в более чем 45 странах.

Общее количество успешных атак значительно больше, но пострадавшие компании предпочитают не рассказывать об инциденте, заплатив вымогателям, либо атака не сопровождалась публикацией данных из сети жертвы.

Наиболее популярными целями (около 60% от общего числа) были компании из США. На долю стран Европы пришлось всего около 20% от общего числа атак. Около 10% пришлось на страны Северной и Южной Америки (за исключением США) и Азии (7%).

СЕВЕРНАЯ И ЮЖНАЯ АМЕРИКА

ЕВРОПА

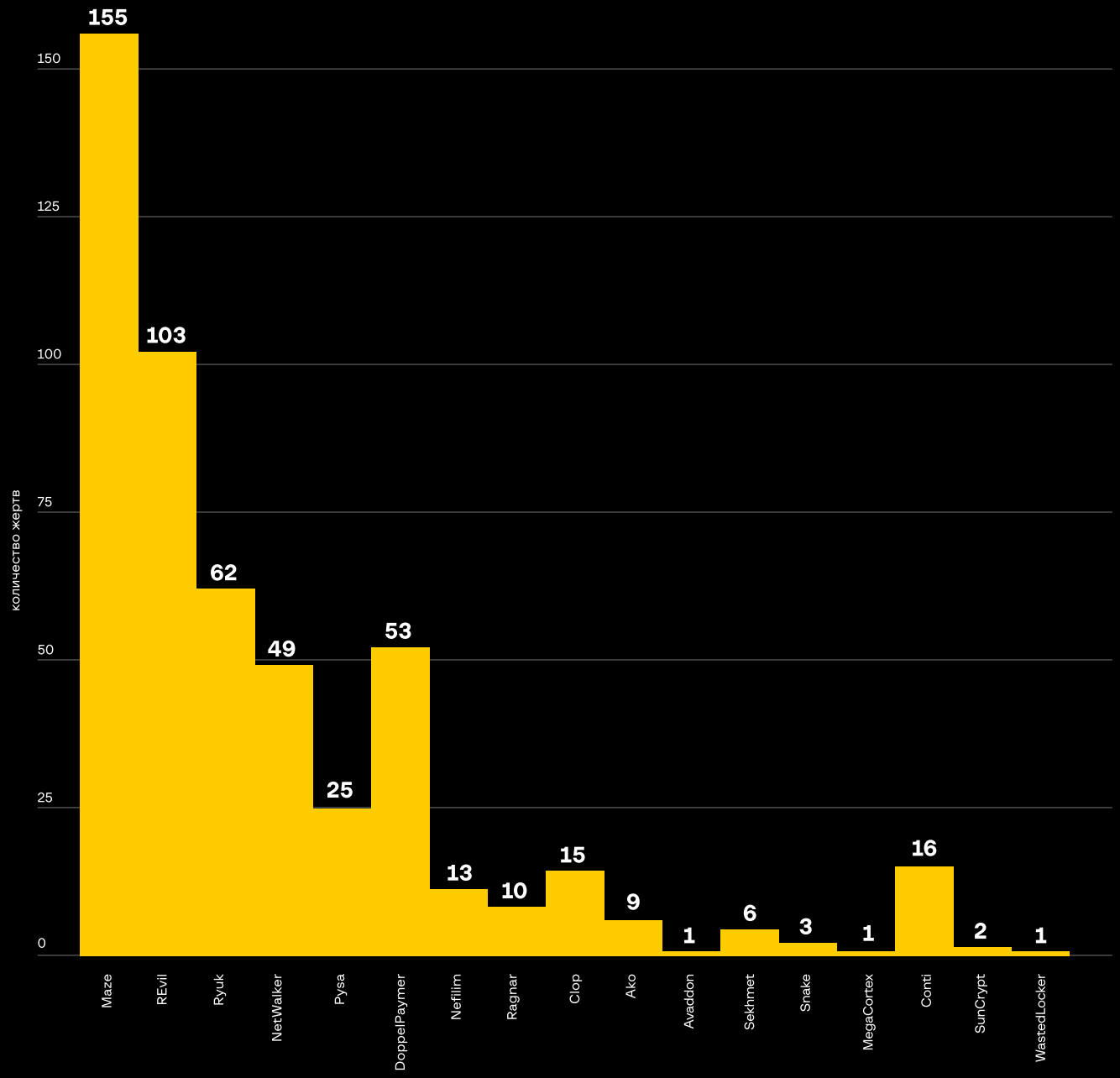
СРЕДНИЙ ВОСТОК И АФРИКА

ЮГО-ВОСТОЧНАЯ АЗИЯ И АВСТРАЛИЯ

Статистика по странам	
Страна	Количество жертв
США	313
Великобритания	25
Канада	24
Франция	20
Германия	17
Австралия	13
Испания	11
Бразилия	9
Италия	9
Швейцария	7
ОАЭ	6
Индия	6
ЮАР	5
Мексика	4
Китай	4
Колумбия	4
Бельгия	3
Саудовская Аравия	3
Коста-Рика	3
Таиланд	2
Австрия	2
Гонконг	2
Южная Корея	2
Япония	2
Аргентина	2
Оман	2
Косово	1
Сингапур	1
Катар	1
Филиппины	1
Португалия	1
Чили	1
Доминиканская Республика	1
Ямайка	1
Неизвестно	1
Швеция	1
Словения	1
Каймановы острова	1
Шри Ланка	1
Новая Зеландия	1
Кипр	1
Алжир	1
Нигерия	1
Пуэрто Рико	1
Люксембург	1
Македония	1
Хорватия	1
Нидерланды	1
Вьетнам	1
Итого	523

Статистика по индустриям	
Индустрия	Количество жертв
Производство	94
Торговля	51
Государственные учреждения	39
Здравоохранение	38
Строительство	30
Образовательные услуги	29
IT	28
Юридические услуги	20
Логистика и хранение	18
Административные и вспомогательные услуги, а также услуги по обращению с отходами и переработкой	14
Телекоммуникации	12
Бухгалтерские услуги	11
Группы компаний	3
Консалтинг	9
Инженерное дело	9
Обработка, хранение данных и связанные услуги	9
Дизайн	8
Агентства недвижимости	8
Научно-исследовательские	7
Страхование	7
Инвестиции	6
Кредитование	6
Добыча природных ресурсов	6
Другое	6
Сельское хозяйство	5
Энергетика	5
Банковское дело	4
Маркетинг	4
Некоммерческие организации	4
Издательства	3
Турагентства	3
Неизвестно	3
Гостеприимство	3
Искусство и развлечения	2
Вещание	2
Азартные игры	2
Авиация	2
Аукционные дома	1
Автопром	1
Продукты питания	1
Менеджмент	1
Транспорт	1
Профессиональные организации	1

Наиболее активными шифровальщиками с конца 2019 года являются Maze и REvil — на них приходится более 50% успешных атак. Во втором эшелоне идут Ryuk, NetWalker, DoppelPaymer.



155

ЦЕЛЕВЫХ АТАК

с использованием шифровальщика Maze зафиксировано

Самой атакуемой отраслью стало производство. В целом половина всех атак пришлась на производство, торговлю, государственные учреждения, систему здравоохранения, строительную отрасль и образовательные сервисы. При этом партнеры выбирают максимально доступные цели для своих атак, что объясняет большое распределение по разным отраслям.

Шифровальщик **Maze** — Жертв **155**

Топ-5 атакуемых стран

США	93
Канада	8
Франция	6
Италия	6
Великобритания	6

Топ-5 атакуемых индустрий

Производство	30
Торговля	19
Строительство	15
Административные и вспомогательные услуги, а также услуги по обращению с отходами и переработке	8
Здравоохранение	7

Шифровальщик **REvil** — Жертв **103**

Топ-5 атакуемых стран

США	63
Великобритания	7
Австралия	5
Швейцария	4
Канада	3

Топ-5 атакуемых индустрий

Производство	20
Торговля	17
IT	10
Юридические услуги	6
Государственные учреждения	4

Шифровальщик **Ryuk** — Жертв **62**

Топ-5 атакуемых стран

США	53
Испания	5
Австралия	1
Великобритания	1
Германия	1

Топ-5 атакуемых индустрий

Государственные учреждения	16
Образовательные услуги	14
Здравоохранение	14
Издательства	3
IT	3

Шифровальщик **NetWalker** — Жертв **49**

Топ-5 атакуемых стран

США	28
Франция	6
Канада	4
Великобритания	2
Австрия	1

Топ-5 атакуемых индустрий

Производство	14
Здравоохранение	6
Образовательные услуги	5
Торговля	4
Логистика и хранение	3

Шифровальщик **Pysa** — Жертв **25**

Топ-5 атакуемых стран

США	5
Великобритания	3
Канада	2
Франция	2
Мексика	2

Топ-5 атакуемых индустрий

Здравоохранение	5
Государственные учреждения	3
Производство	3
Строительство	2
Образовательные услуги	2

Шифровальщик **DoppelPaymer** — Жертв **53**

Топ-5 атакуемых стран

США	35
Франция	5
Канада	3
Саудовская Аравия	1
Катар	1

Топ-5 атакуемых индустрий

Trade	8
Государственные учреждения	7
Производство	6
Логистика и хранение	4
Строительство	3

Шифровальщик **Nefilim** — Жертв **13**

Топ-5 атакуемых стран

Бразилия	3
Индия	3
Германия	1
Франция	1
Швейцария	1

Топ-5 атакуемых индустрий

Производство	4
Строительство	2
Добыча природных ресурсов	2
Логистика и хранение	1
Административные и вспомогательные услуги, а также услуги по обращению с отходами и переработке	1

Шифровальщик **Ragnar** — Жертв **10**

Топ-5 атакуемых стран

США	7
Португалия	1
Германия	1
Сингапур	1
—	—

Топ-5 атакуемых индустрий

Маркетинг	2
Юридические услуги	2
IT	1
Производство	1
Строительство	1

Шифровальщик **Clop** — Жертв **15**

Топ-5 атакуемых стран

Германия	7
США	2
Испания	1
Австрия	1
Великобритания	1

Топ-5 атакуемых индустрий

Производство	6
IT	2
Логистика и хранение	2
Азартные игры	1
Государственные учреждения	1

Шифровальщик **Ako** — Жертв **9**

Топ-5 атакуемых стран

США	6
Великобритания	2
Канада	1
—	—
—	—

Топ-5 атакуемых индустрий

Строительство	2
Юридические услуги	1
Дизайн	1
Инженерное дело	1
Производство	1

Шифровальщик **Avaddon** — Жертв **1**

Топ-5 атакуемых стран

США	1
—	—
—	—
—	—
—	—

Топ-5 атакуемых индустрий

Строительство	1
—	—
—	—
—	—
—	—

Шифровальщик **Sekhmet** — Жертв **6**

Топ-5 атакуемых стран

США	3
Бразилия	1
Великобритания	1
Испания	1
—	—

Топ-5 атакуемых индустрий

Производство	2
Юридические услуги	1
IT	1
Страхование	1
Логистика и хранение	1

Шифровальщик **Snake** — Жертв **3**

Топ-5 атакуемых стран

Германия	1
Аргентина	1
Япония	1
—	—
—	—

Топ-5 атакуемых индустрий

Здравоохранение	1
Энергетика	1
Группы компаний	1
—	—
—	—

Шифровальщик **MegaCortex** — Жертв **1**

Топ-5 атакуемых стран

США	1
—	—
—	—
—	—
—	—

Топ-5 атакуемых индустрий

Обработка, хранение данных и связанные услуги	1
—	—
—	—
—	—
—	—

Шифровальщик **Conti** — Жертв **16**

Топ-5 атакуемых стран

США	13
Канада	2
Испания	1
—	—
—	—

Топ-5 атакуемых индустрий

Производство	3
Гостеприимство	2
IT	1
Страхование	1
Здравоохранение	1

Шифровальщик **SunCrypt** — Жертв **2**

Топ-5 атакуемых стран

США	1
Канада	1
—	—
—	—
—	—

Топ-5 атакуемых индустрий

Производство	1
Дизайн	1
—	—
—	—
—	—

Шифровальщик **WastedLocker** — Жертв **1**

Топ-5 атакуемых стран

США	1
—	—
—	—
—	—
—	—

Топ-5 атакуемых индустрий

Производство	1
—	—
—	—
—	—
—	—

Оценка потенциального ущерба

К сожалению, оценить реальный ущерб от действий групп, использующих шифровальщики, достаточно сложно. Оценка должна складываться из сумм, выплаченных жертвами, потерь в случае простоя, трат на восстановление нормального функционирования внутренних систем. Дополнительная сложность — получить информацию об атаках, так как многие компании платят злоумышленникам выкуп и не сообщают об этом.

Стоит отметить, что сумма выкупа может быть очень разной, например:

— Требования группы **REvil** варьируются в зависимости от количества зараженных хостов и размера компании. Если заражен только один компьютер в сети, злоумышленники потребуют около $48 тыс., в случае с несколькими зараженными машинами известно о сумме выкупа в $470 тыс., иногда она может превышать $1 млн. А в целом средняя сумма выкупа составляет $260 тыс.

— Группа **Maze** запрашивает обычно больше $1 млн. Средняя стоимость выкупа по известным инцидентам — $2 млн 420 тыс.

— Некоторые группы, такие как **WastedLocker**, совершали крайне мало атак, зато сумма выкупа превышала $10 млн.

— Аналогичная ситуация с шифровальщиком **MegaCortex**. Точное количество атак не известно, но есть данные, что сумма выкупа варьируется от $20 000 до $5 800 000.

Группа	Средняя сумма выкупа, $	Количество жертв	Потенциальный ущерб, $
Ako	300 000	9	1 800 000
Avaddon	7500	1	7500
Clop	400 000	15	6 000 000
Conti	200 000	16	3 200 000
DoppelPaymer	1 143 500	53	60 605 500
Maze	2 420 000	155	375 100 000
Nefilim	100 000	13	1 300 000
NetWalker	720 000	49	35 280 000
Pysa	None	25	None
Ragnar	7 750 000	10	77 500 000
REvil	300 000	103	30 900 000
Ryuk	1 451 500	62	89 993 000
Snake	None	3	None
SunCrypt	400 000	2	800 000

Таким образом, с учетом шифровальщиков, у которых публично известна сумма выкупа (см. в таблице выше), а также с учетом оценки потерь от WastedLocker и MegaCortex, суммарный потенциальный ущерб составляет около $1 млрд ($1 005 186 000).

Данные, приведенные выше, описывают только известные инциденты и показывают нижнюю границу ущерба. Но, как всегда, это лишь верхушка айсберга. Например, известно всего лишь о 62 инцидентах с использованием **Ryuk**, который активно распространялся с помощью банковского трояна **Trickbot**.

При этом, по нашим данным, владельцы бот-сети Trickbot за последний год успешно зашифровали более 2500 разных сетей, используя такие шифровальщики, как Ryuk (позже **Conti**), **Kraken**, **Thanos**. 62 известных инцидента — это лишь 2,5% от общего числа, а значит, и реальный ущерб гораздо больше.

Кроме этого можно рассмотреть другой пример с шифровальщиком Dharma. Его исходный код был выставлен на продажу в прошлом году, и его могли использовать самые разные группы - в этом случае сложно определить потенциальный ущерб.

1
МЛРД ДОЛЛАРОВ
суммарный потенциальный ущерб

Рынок продажи доступов к корпоративным сетям растет

Продажа различной аутентификационной информации является достаточно распространенной практикой на андерграундных форумах и существует с момента образования подобных сообществ.

Раньше, после нахождения каких-либо серверов и их компрометации, злоумышленники не проводили дополнительные исследования, не понимали, что они могут принадлежать крупным компаниям, а доступ к ним хорошо монетизируется.

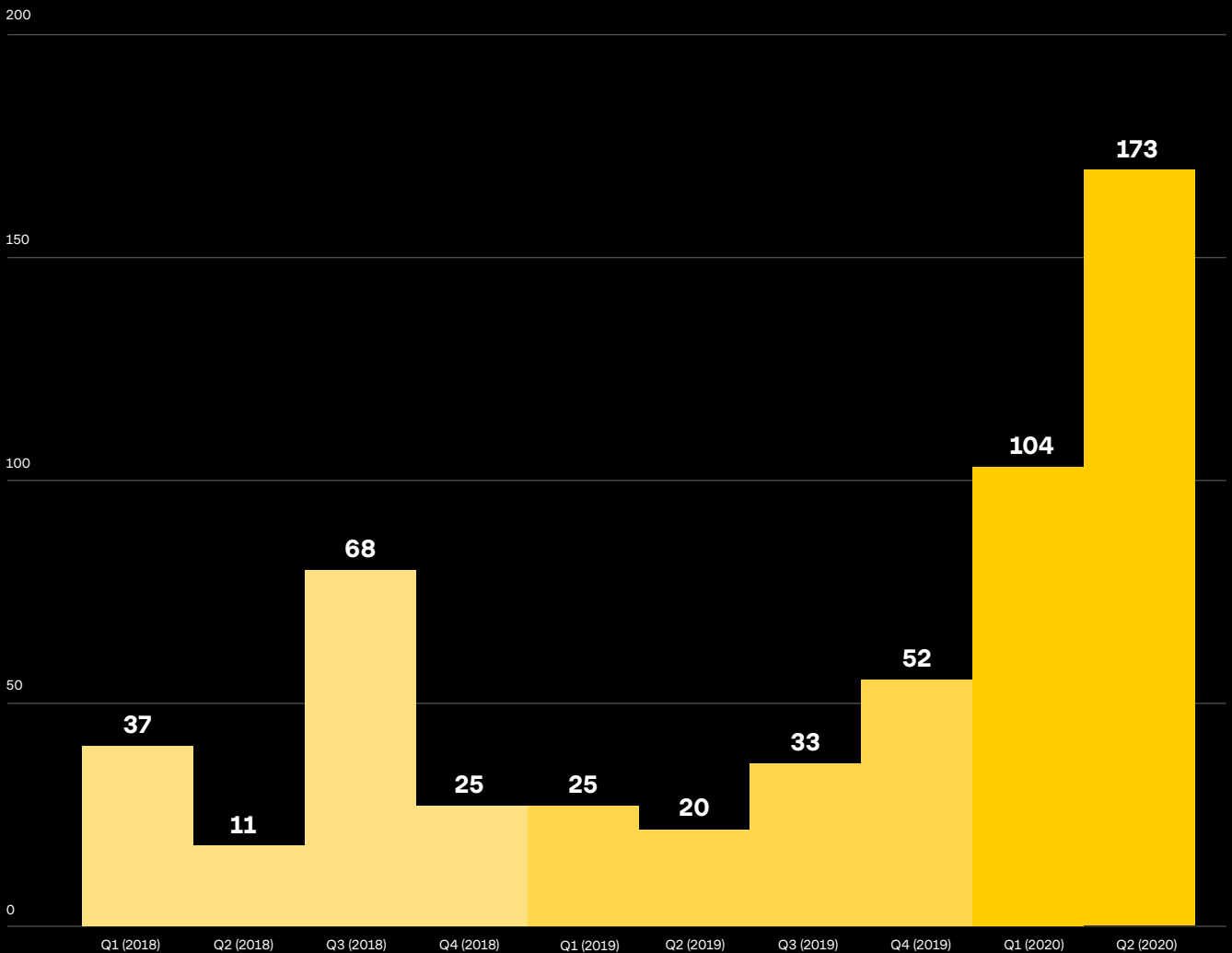
Количество продаваемых доступов к корпоративным сетям увеличивается из года в год, однако основной пик продаж пришелся на 2020 год, что связано с увеличением количества новых партнерских предложений по шифровальщикам.

Если сравнить периоды H2 2018 — H1 2019 и H2 2019 — H1 2020, то мы видим увеличение количества продаж в 2,6 раза: 138 предложений за первый период против 362 в текущем.

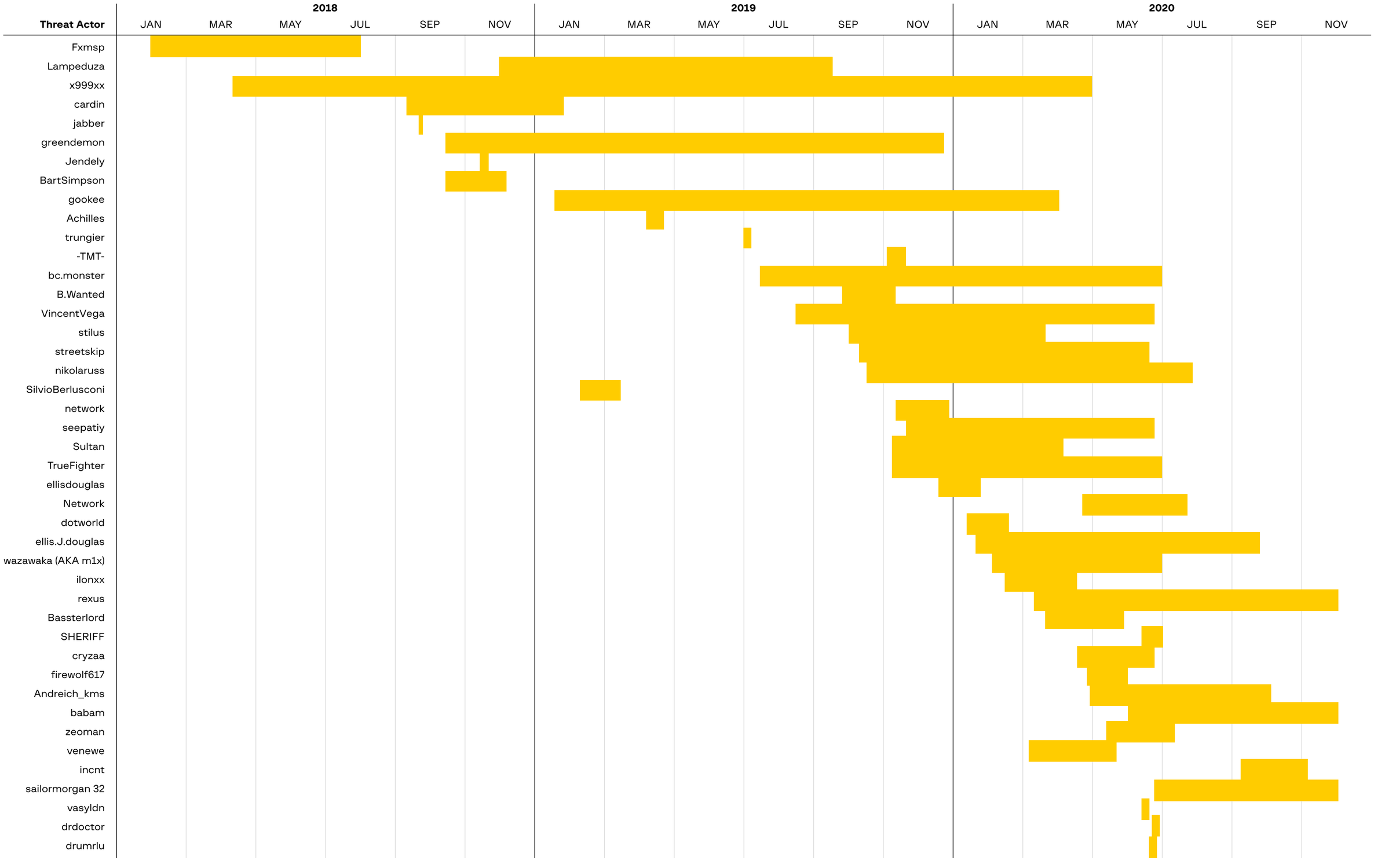
2018			
Q1	**Q2**	**Q3**	**Q4**
37	11	68	25
H1		**H2**	
48		93	
TOTAL			
141			

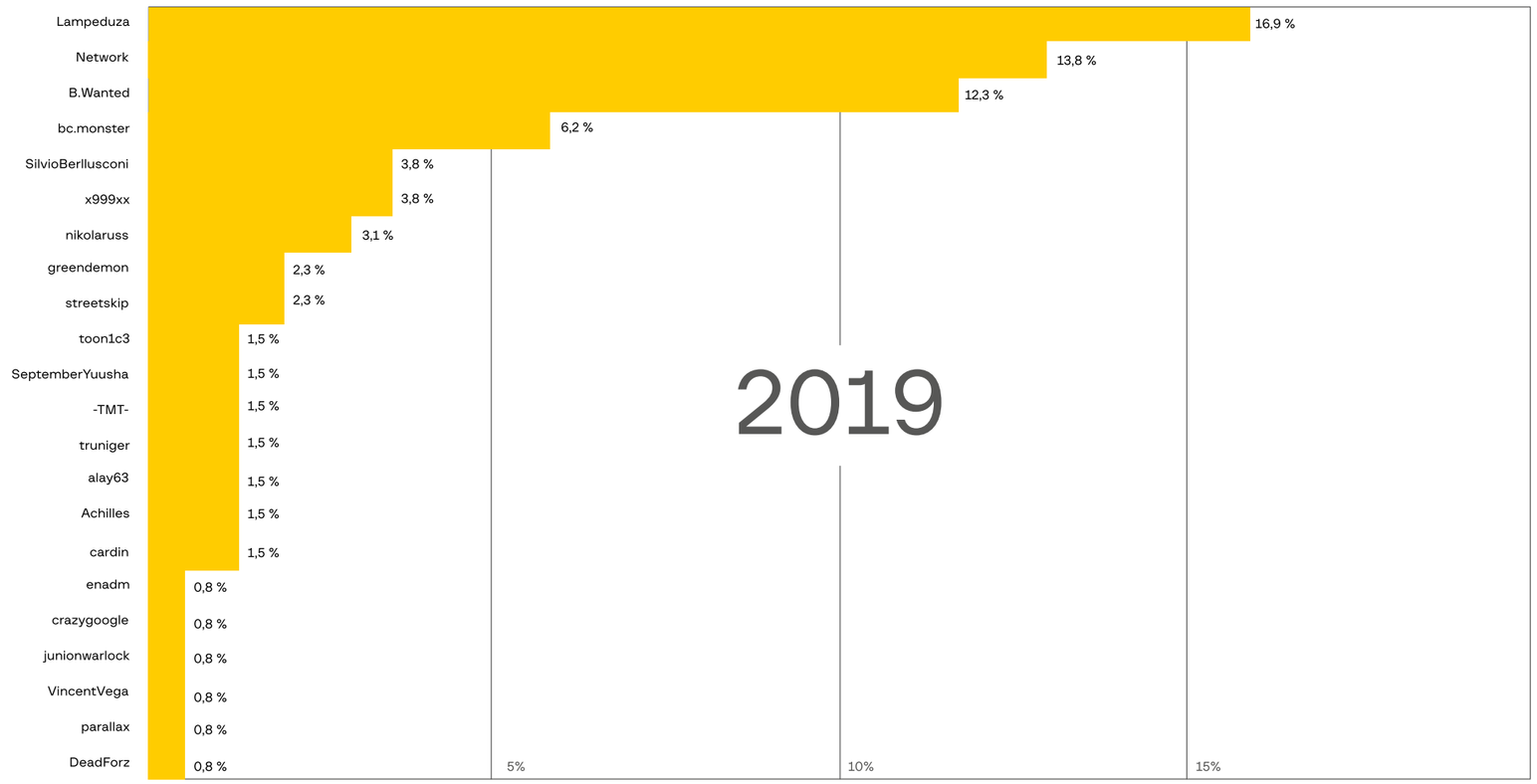
2019			
Q1	**Q2**	**Q3**	**Q4**
25	20	33	52
H1		**H2**	
45		85	
TOTAL			
130			

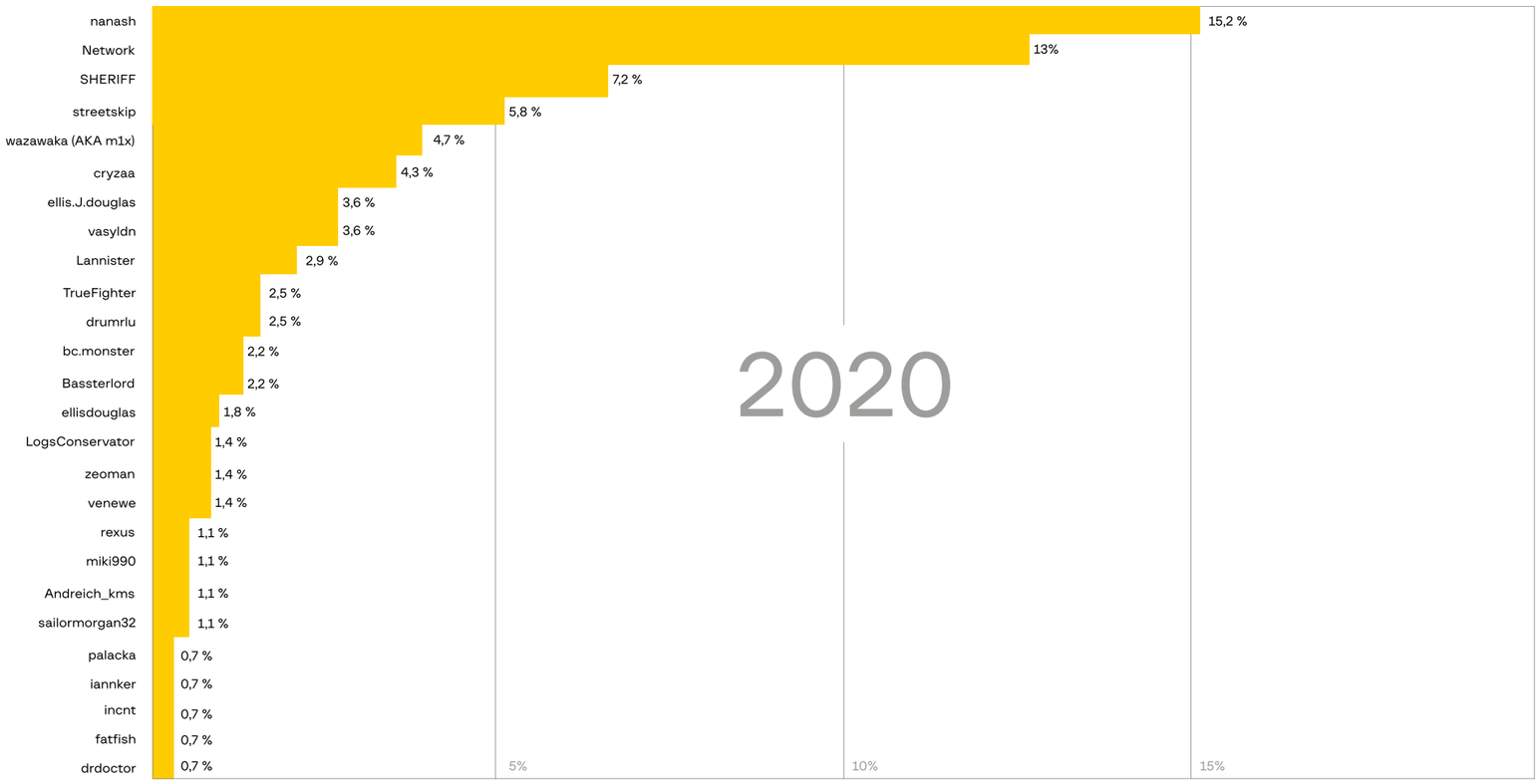
2020			
Q1	**Q2**	**Q3**	**Q4**
104	173	—	—
H1		**H2**	
277		—	
TOTAL			
277			



Активность продавцов доступов в андерграунде за 2018–2020 гг. (учитываются только те, у кого было несколько постов о продажах)







Количество продавцов доступов

37 продавцов доступов в 2018 году

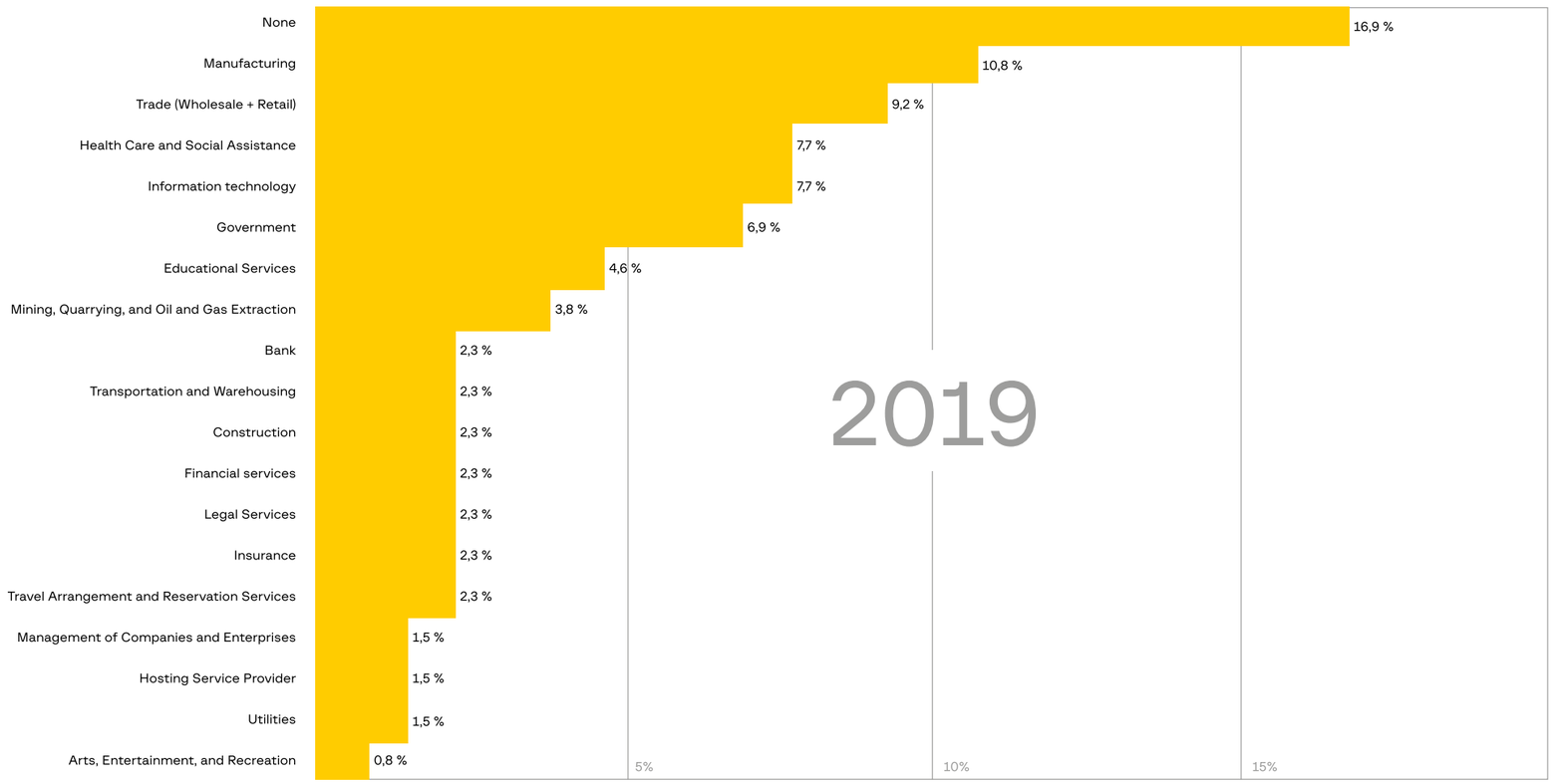
50 продавцов доступов в 2019 году

63 продавца доступов в 2020 году

В 2018 году активными были только 37 продавцов доступов.

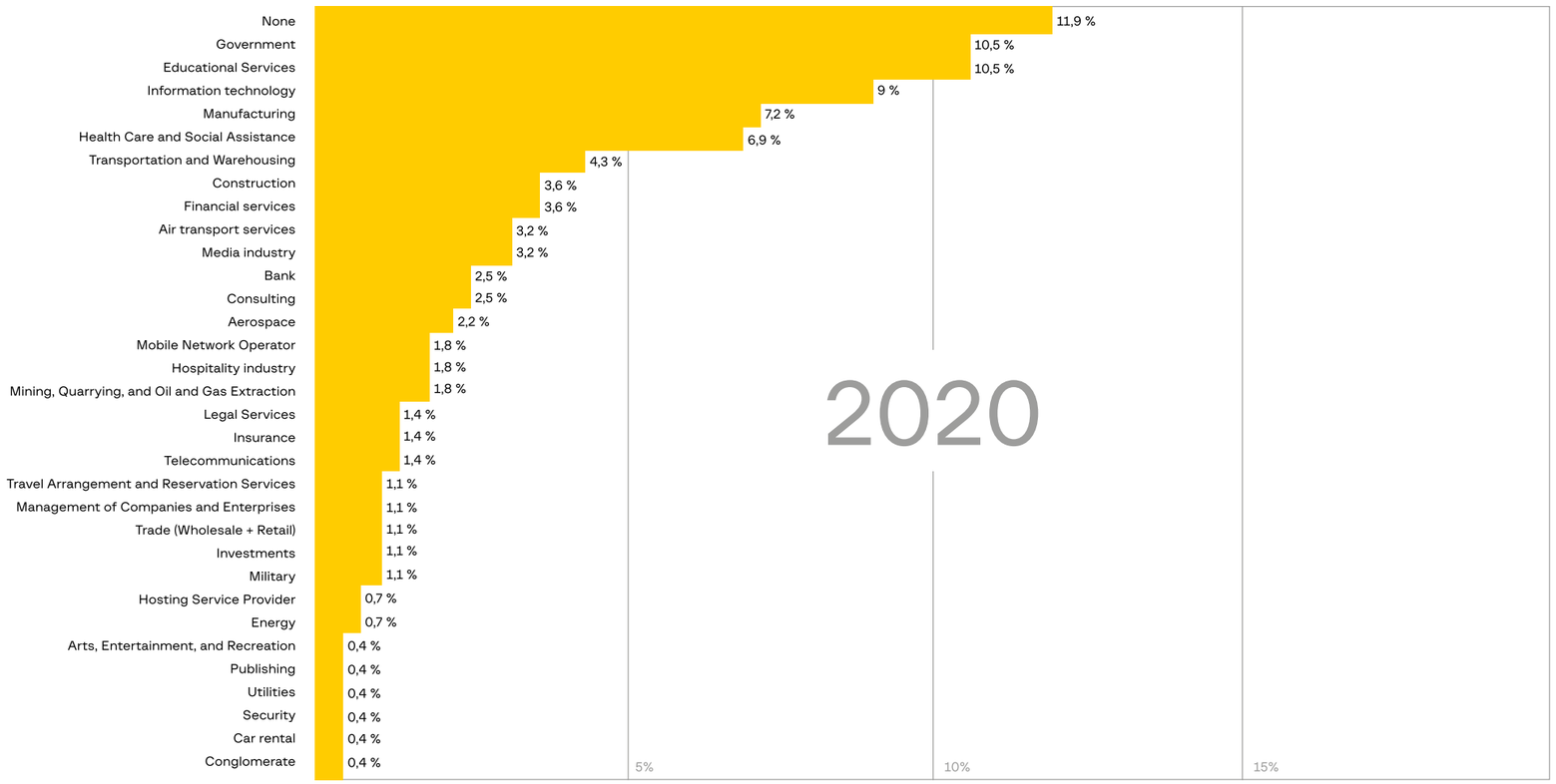
В 2019 году было выявлено 50 активных продавцов, которые выставили на продажу доступы к 130 компаниям. При этом 44 из них являются новыми, без истории активности в предыдущие годы.

Только за H1 2020 на андерграундных форумах было выставлено на продажу 277 доступов к корпоративным сетям различных компаний. Количество продавцов также выросло до 63 злоумышленников, 52 из которых начали свою активность в этом году.



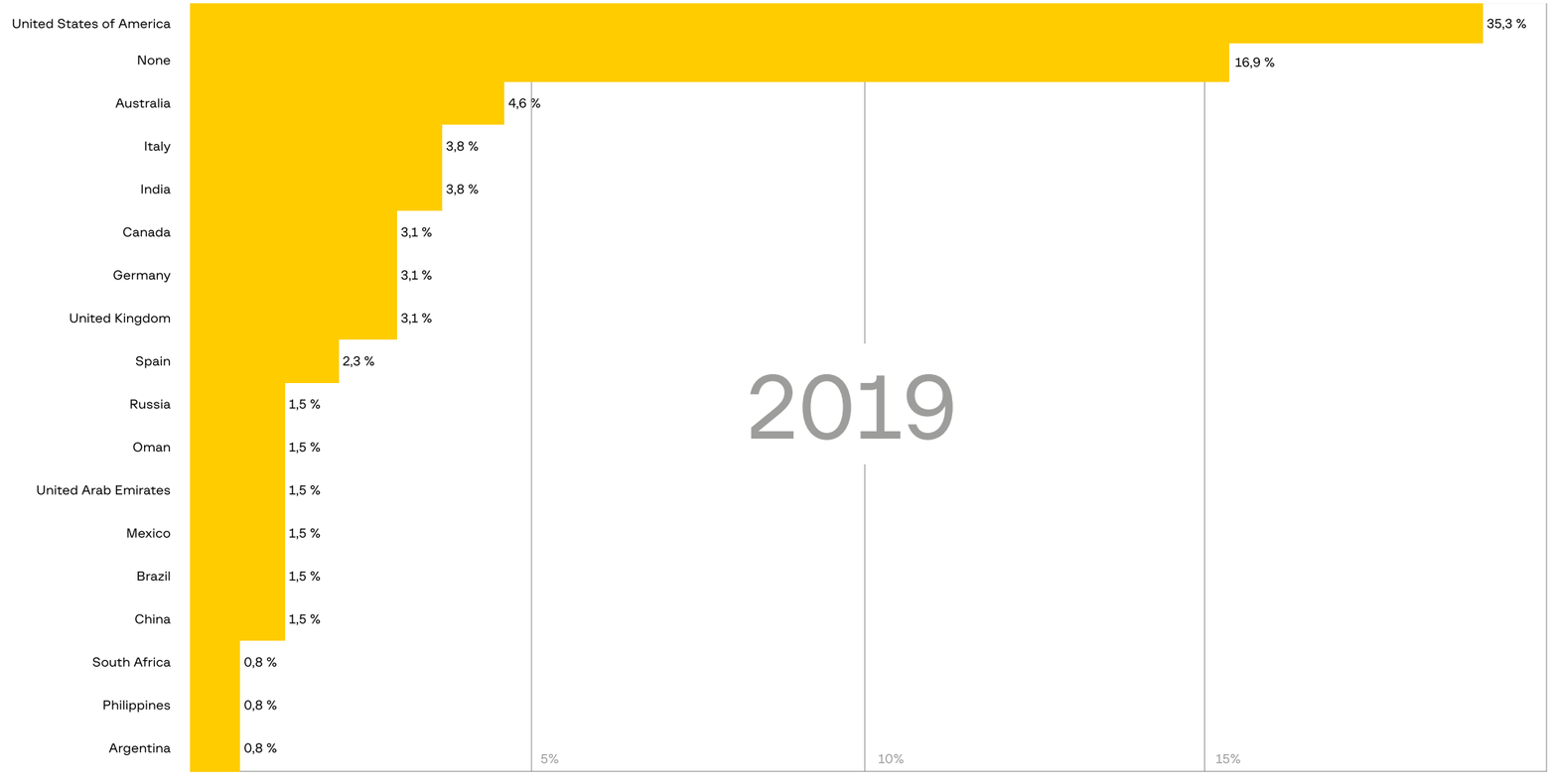
2019 фокус нападающих — производство

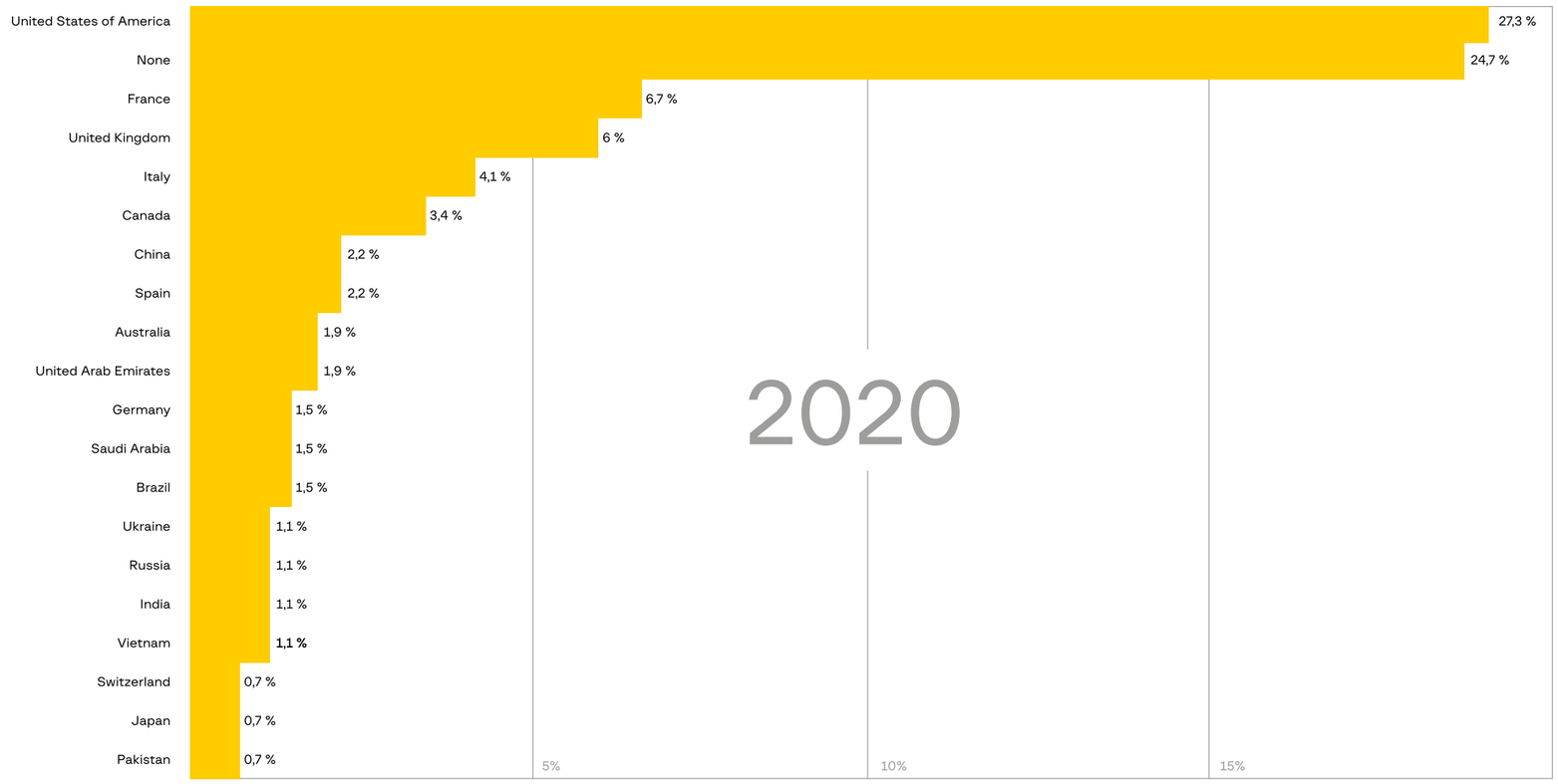
2020 фокус нападающих— государственные компании



В 2019-м основными жертвами были компании, связанные с производством, а также большое количество компаний из сферы здравоохранения, обычно больницы или клиники.

В 2020 году состав атакованных индустрий достаточно сильно меняется. На первые места выходят различные государственные компании и образовательные учреждения. Компании, связанные с производством, составляют лишь 7,2%.





США — один из самых атакуемых регионов

Что касается общего размера рынка продажи доступов, то проанализировать его точный объем достаточно сложно, так как злоумышленники часто не публикуют цены. Однако, по опубликованным на форумах ценам доступов:

$1 609 930

общий размер рынка в H2 2018 — H1 2019

$6 189 388

размер рынка в текущем периоде (H2 2019 — H1 2020) — четырехкратный рост

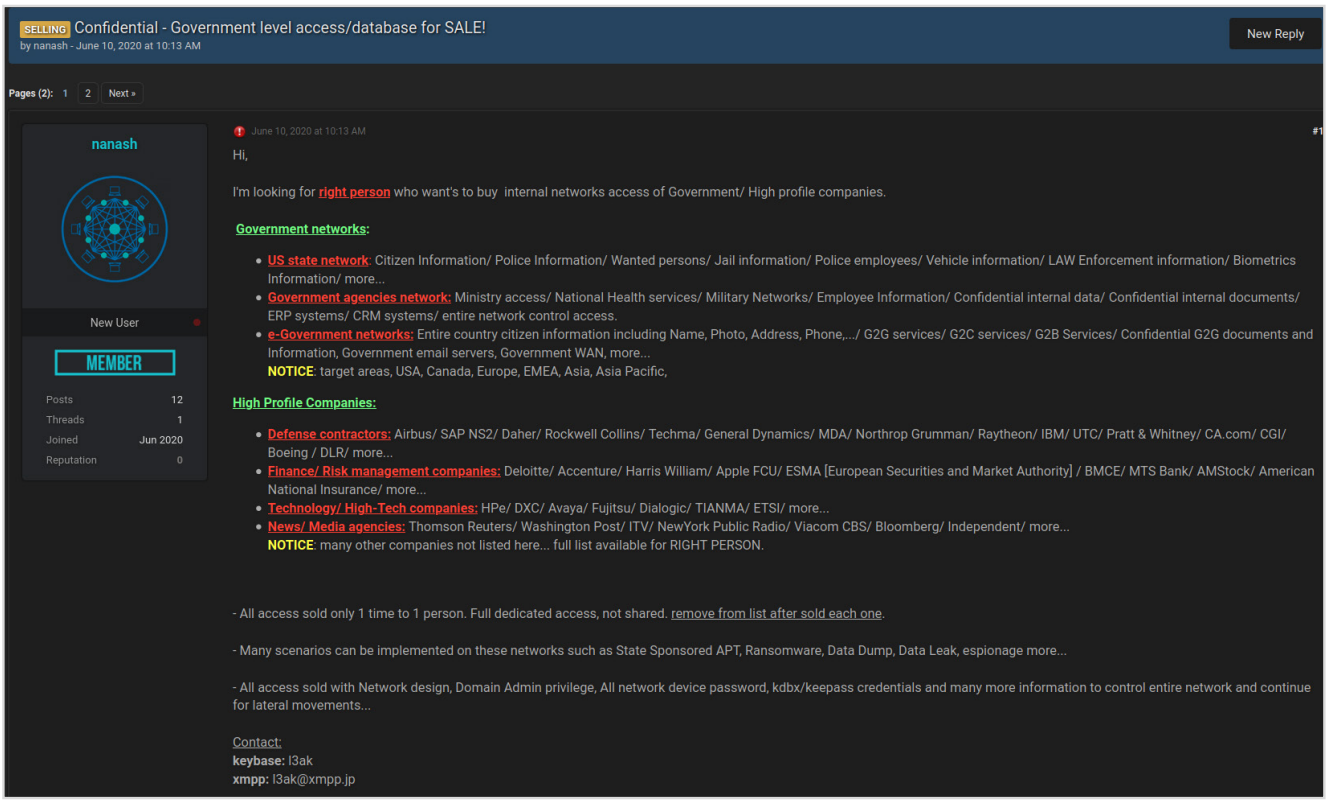
Основным атакуемым регионом остаются США, но стоит еще раз подчеркнуть, что установить название и локацию компаний, доступ к которым продается, все чаще невозможно без взаимодействия с атакующими.

Спецслужбы тоже продают доступ и используют шифровальщики

Некоторые прогосударственные группы пытаются найти дополнительное финансирование. Как и обычный криминал, они начинают продавать доступ в корпоративные сети или используют программы-шифровальщики.

Одним из ярких примеров является объявление пользователя с псевдонимом nanash в июне 2020 года о продаже доступов к большому количеству сетей, включая государственные ведомства США, оборонных подрядчиков (Airbus, Boeing и др.), ИТ-гигантов и медиакомпаний.

Рисунок 5. Продажа доступов к различным компаниям (nanash)



Данное сообщение выглядит крайне подозрительно, но в ходе дальнейшего расследования мы получили подтверждения, что его автор действительно имеет доступ как минимум к двум компаниям из данного списка. В качестве доказательств были получены скриншоты LDAP-доступа и видеодемонстрация.

Продавец отдельно отметил, что цена доступа к каждой из компаний составляет 11 BTC ($125 тыс.), продается он напрямую по частичной предоплате: после перевода 5 BTC злоумышленник предоставляет дополнительные доказательства, и лишь потом происходит конечная сделка.

В тексте сообщения перечислены не все компании, но стоимость доступа к явно указанным составляет около $5 млн.

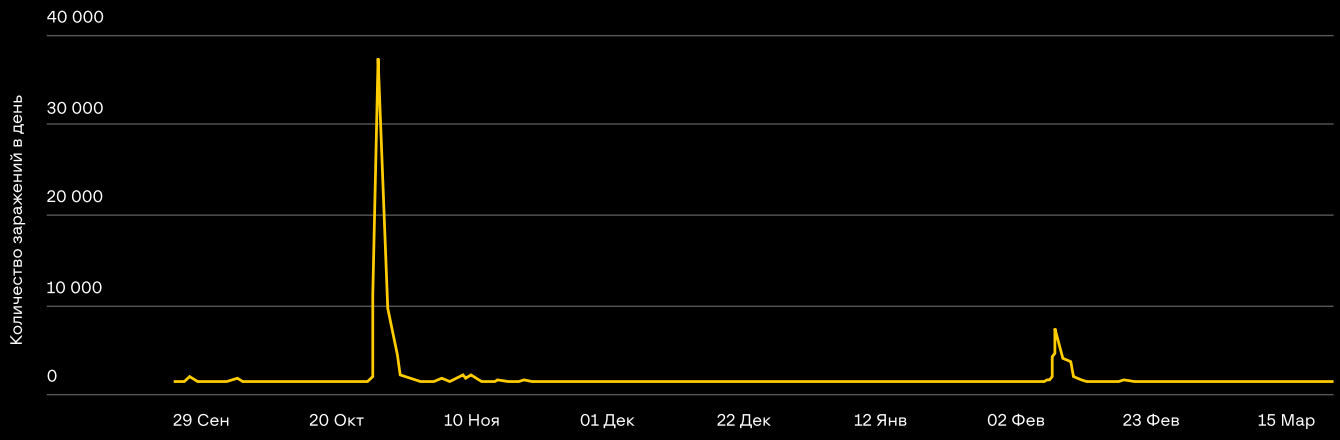
Еще одним способом заработать для прогосударственных групп является использование шифровальщиков, вот несколько примеров:

— Китайские хакеры из **APT41** по предположению тайваньских властей стояли за атакой вымогателей на энергетические и технологические компании острова в мае 2020 года. В уведомлении говорилось, что пострадала тайваньская компании CPC Corp., которая отвечает за доставку нефтепродуктов по всему Тайваню. Атака не повлияла на производственные процессы CPC, но помешала клиентам использовать платежные карты CPC Corp. для покупки газа. В ходе этой волны атак был задействован новый шифровальщик — **ColdLock**. Анализ указывает на сходство между ним и двумя ранее известными семействами вымогателей, в частности Freezing и «образовательным» набором вымогателей EDA2.

— Группа **Lazarus** вновь вернулась к разработке вымогателей и атаковала европейские компании шифровальщиком **VHD Ransomware**. Хакеры получали доступ с помощью уязвимого VPN-шлюза, повышали права до администратора и устанавливали бэкдор DacIs. Они перемещались по сети жертвы и шифровали файлы комбинацией AES-256 в режиме ECB и RSA-2048.

— Группа китайских хакеров **IronTiger** стояла за использованием шифровальщика **HybirdRansom** против компаний Азиатско-Тихоокеанского региона осенью 2019 года и весной 2020 года. Шифровальщик состоит из нескольких компонентов, последовательно запускающих друг друга для блокировки машины и шифрования файлов: Locker, Loader и Cryptor.

Количество атак с использованием шифровальщиков



Массовые взломы стали опаснее для крупных компаний

Ранее массовые атаки не наносили крупным компаниям серьезного ущерба. Подбор паролей или эксплуатация уязвимостей в распространенном программном обеспечении приводили к тому, что их инфраструктура использовалась для распространения или управления вредоносным кодом, майнинга криптовалют, проведения DDoS- атак или проксирования трафика.

С ростом рынка продаж доступов в корпоративные сети, увеличением количества атак с использованием шифровальщиков и активизацией APT-групп цена ошибки на внешнем периметре компании резко увеличивается.

10 из 15 партнерских программ операторов шифровальщиков используют перебор паролей на RDP. А три из них вдобавок активно эксплуатируют уязвимости в VPN-сервисах.

Подобные действия совершают APT-группы:

APT29 (aka Cozy Bear) активно эксплуатировала следующие уязвимости с публичными эксплойтами:

— CVE-2019-19781 (Citrix)
— CVE-2019-11510 (Pulse Secure)
— CVE-2018-13379 (FortiGate)
— CVE-2019-9670 (Zimbra)

APT-группа **BlackEnergy** (aka Sandworm) пользовалась уязвимостью почтового сервера Exim CVE-2019-10149 для установки SSH-бэкдора.

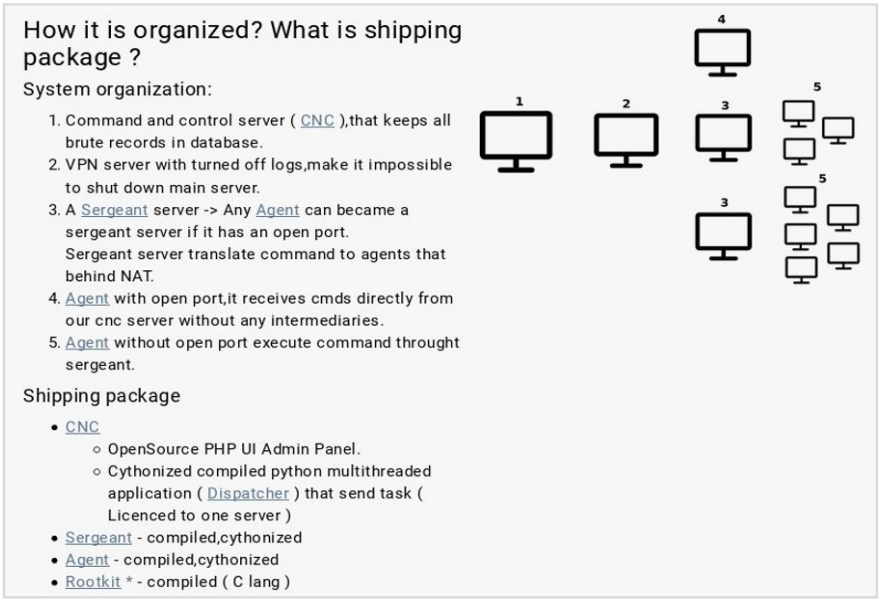
Отмечено участие и обычного криминала:

Например, группа **Clownz**, ответственная за утечки из GoDaddy и 247.ai, тоже использовала CVE-2019-10149 (Exim) для установки SSH-бэкдора. За несколько месяцев работы им удалось заразить 80 тыс. серверов.

Как мы уже писали выше, одним из основных способов получения доступа в корпоративные сети является подбор паролей к интерфейсам удаленного доступа (RDP, SSH, VPN). От эффективности подбора зависит, сколько компаний будет в итоге скомпрометировано и сколько заработают мошенники.

Другим важным изменением является появление новых типов бот-сетей. Их основное назначение — распределенный подбор паролей с большого количества зараженных устройств, в том числе серверов.

Рисунок 6. Пример продажи услуги на основе брутфорсера — распределенного сканера для подбора паролей



Фреймворки для постэксплуатации используются чаще

Для успешной реализации атаки в корпоративной сети нужны инструменты для горизонтального перемещения, повышения привилегий после компрометации. Рост рынка продаж доступа привел к росту использования post exploitation фреймворков.

Такие фреймворки используются повсеместно и операторами/партнерами шифровальщиков, и обычными криминальными группами, и прогосударственными атакующими. Мы постоянно наблюдаем за появлением новой инфраструктуры различных постэксплуатационых фреймворков. За H2 2019 — H1 2020 было обнаружено, что они используют более 10 тыс. хостов. За аналогичный период прошлого года таких хостов было обнаружено 6 тыс.

	Атакующий	Cobalt Strike	Metasploit	Covenant	CrackMapExec	PoshC2	Koadic
Ransomware	Ryuk	●	●				
	REvil		●		●		
	MegaCortex	●					
	Maze	●					
	DoppelPaymer					●	●
	Clop	●	●				
	Lockbit				●		
Cybercrime	Cobalt	●					
	Silence		●				
	Fxmsp		●				
	FIN6	●	●				
APT	Lazarus	●					
	OilRig	●	●	●			
	APT41	●	●				
	APT32	●					
	Gamaredon		●				
	Chimera	●					
	Mustang Panda	●					
	Chafer		●				
	APT10	●					
	APT33					●	

10 000 ХОСТОВ

под фреймворки постэксплуатации было обнаружено за период H2 2019 — H1 2020

ВОЕННЫЕ ОПЕРАЦИИ

Семь новых APT-групп обнаружено за текущий период

И шесть уже известных, но ранее ушедших с радаров, возобновили атаки

Новые инструменты и разрушительные последствия

Остановка энергоблоков, физическое уничтожение инфраструктуры, атаки на air-gapped сети

Страны АТР становятся одной из ключевых арен

и привлекают внимание киберпреступников из Китая, Северной Кореи, Ирана и Пакистана

Изменение ландшафта угроз

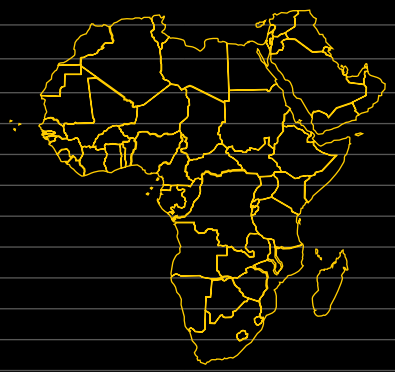
Данный год стал очень плодотворным по количеству атак на Азиатско-Тихоокеанский регион, к которому проявляли интерес активные группы из Китая, Северной Кореи, Ирана и Пакистана.

За текущий период было обнаружено семь новых APT-групп, а также выявлена новая активность шести ранее известных групп, которые оставались незамеченными последние несколько лет.

АТР

APT10	China
DarkHotel	North Korea
OceanLotus	Vietnam
TA428	China
Kimsuky	North Korea
APT37	North Korea
FruityArmor	UAE
BITTER	India
Patchwork	India
Emissary Panda	China
Poison Carp	China
Rancor	China
Lazarus	North Korea
IronTiger	China
APT41	China
Mustang Panda	China
Higaisa	South Korea
APT33	Iran
Platinum	China
APT-C-35	Unknown
APT20	China
BlackTech	China
Tick	China
SideWinder	India
APT40	China
Transparent Tribe	Pakistan
Cycldek	China
Tonto Team	China
TwoSail Junk	China
Naikon	China
Tropic Trooper	China
Chimera	Unknown
APT30	China
Orangeworm	Unknown

СРЕДНИЙ ВОСТОК И АФРИКА

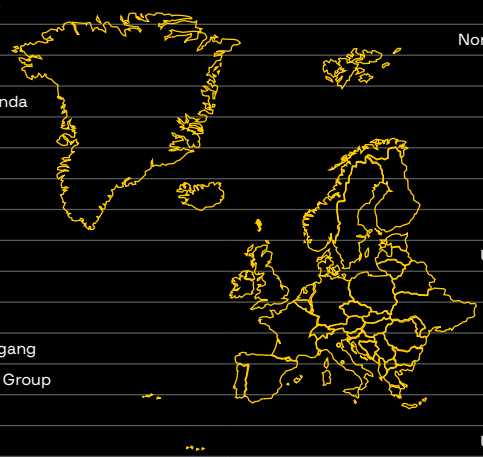


APT10	China
Oilrig	Iran
MuddyWater	Iran
Gorgon Group	Pakistan
FruityArmor	UAE
Tortoiseshell	Iran
APT41	China
Mustang Panda	China
APT33	Iran
APT-C-37	Unknown
Domestic Kitten	Iran
APT35	Iran
APT-C-23	Gaza
Gaza Cybergang	Gaza
Chafer	Iran
StrongPity	Turkey
WildPressure	Unknown
Orangeworm	Unknown

АМЕРИКА

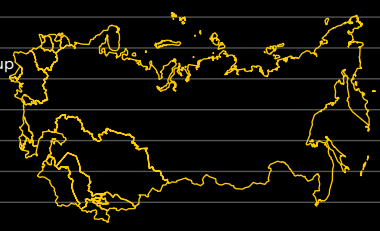
Gorgon Group	Pakistan
Kimsuky	North Korea
IronTiger	China
APT41	China
APT35	Iran
Oilrig	Iran
APT33	Iran
APT20	China
APT37	North Korea
Gaza Cybergang	Gaza
TA410	China
APT5	China
Tortoiseshell	Iran
Orangeworm	Unknown
Transparent Tribe	Pakistan

ЕВРОПА



APT 10	China
APT15	China
Gorgon Group	Pakistan
Kimsuky	North Korea
FruityArmor	UAE
Lazarus	North Korea
APT41	China
Mustang Panda	China
APT29	Russia
Turla	Russia
Oilrig	Iran
Avivore	China
APT-C-35	Unknown
APT20	China
APT35	Iran
Gaza Cybergang	Gaza
Gamaredon Group	Russia
APT33	Iran
InvisiMole	Unknown
APT5	China
Orangeworm	Unknown
Transparent Tribe	Pakistan

ПОСТСОВЕТСКОЕ ПРОСТРАНСТВО



APT28	Russia
MuddyWater	Iran
Gamaredon Group	Russia
IronTiger	China
Turla	Russia
Golden Falcon	Kazakhstan
APT37	North Korea
Kimsuky	North Korea
Tonto Team	China

Новые APT-группы

Tortoiseshell

География	Вектор первичной компрометации	Инструменты
Америка Средний Восток	Фишинг Drive-by-атаки	Backdoor.Syskit Infostealer

Группа **Tortoiseshell** оставалась незамеченной с июля 2018 года и за это время атаковала по меньшей мере 11 ИТ-компаний, большинство из которых расположены в Саудовской Аравии.

Как минимум в двух организациях есть свидетельства того, что получение злоумышленниками доступа на уровне администратора домена привело к заражению нескольких сотен компьютеров в сети. Возможно, это была вынужденная мера и так они искали наиболее интересные цели. Ведь заражение ИТ-провайдера открывает большие возможности для доступа к клиентским машинам.

Для этих атак группа создала уникальный вредонос под названием **Backdoor.Syskit**, разработанный в версиях на языках Delphi и .NET. С его помощью преступники могут загружать дополнительные инструменты и выполнять команды. Позже он был замечен в фишинговой атаке на бывших американских военных.

Poison Carp

География	Вектор первичной компрометации	Инструменты
Америка Средний Восток	Drive-by-атаки Эксплуатация публичных приложений Целевой фишинг	MOONSHINE INSOMNIA IRONSQUIRREL

Незамеченной с 2018 года оставалась и группа **Poison Carp**. В связи со специфическими целями атак — высокопоставленными членами тибетских и уйгурских групп — ее в настоящий момент относят к Китаю. Poison Carp использует в общей сложности восемь эксплойтов для Android-браузера, одну цепочку эксплойтов для iOS, а также комплект шпионских программ для Android и iOS.

Представляясь журналистами или чиновниками высокого ранга и начиная переписку в WhatsApp, хакеры завоевывали доверие жертвы и отправляли ей ссылку. При переходе на смартфон устанавливалось шпионское программное обеспечение.

Вредоносный софт MOONSHINE позволял хакерам получать доступ к звонкам, сообщениям, включая сообщения в установленных на гаджете мессенджерах, информацию о геолокации, контролировать микрофон и камеру смартфона, а также устанавливать на телефон программы.

Higaisa

География	Вектор первичной компрометации	Инструменты
APT Европа Россия	Целевой фишинг	GHOST RAT Keylogger InfoStealer

С 2016 года оставалась без внимания группа **Higaisa**. Она проводит фишинговые рассылки с исполняемым файлом внутри, который чаще всего отправляется под видом легитимного установщика или изображения/документа.

В качестве приманок группа использует поздравительные тексты или важные новости. Были обнаружены следующие инструменты злоумышленников:

— модифицированная версия GHOST RAT;
— кейлоггер;
— вредоносная программа для кражи паролей из Outlook;
— Android-трояны (поддерживающие функции по созданию скриншотов, получению GPS-локации, SMS, записей разговоров, телефонной книги, загрузке файлов).

AVIVORE

География	Вектор первичной компрометации	Инструменты
Европа Великобритания	Supply Chain	Mimikatz PlugX Living-off-the-land

Ранее считалось, что это такие хакерские группы, как, например, китайская APT10, организовывали атаки на европейские транснациональные корпорации в аэрокосмической и оборонной отраслях. Но как выяснилось, угроза исходит от неизвестных ранее хакеров — **AVIVORE**.

Группа была активна с 2015 года, но основная часть их деятельности пришлась на 2019 год.

Предположительно, AVIVORE является источником четырех атак 2019 года на европейский аэрокосмический гигант Airbus. Последняя из них произошла в сентябре.

Злоумышленники вторглись в глобальную сеть поставщиков Airbus через британского производителя Rolls-Royce (поставляет двигатели для самолетов) и французскую фирму Expleo (оказывает услуги технологического консультирования).

Кроме того, были скомпрометированы два неустановленных подрядчика, работающих на аэрокосмическую компанию.

Основной вредоносный инструмент группы — **PlugX**.

Nuo Chong Lions

География	Вектор первичной компрометации	Инструменты
Средний Восток	Целевой фишинг Атака типа «водопой» (watering hole)	AndroRat SandroRat Droidjack SpyNote MobiHok

Nuo Chong Lions (aka **SilencerLion**) не отмечена в 2019–2020 гг., но после того, как в группе сменился глава, можно прогнозировать новый рост ее активности.

Речь идет о волне атак группы в 2013–2018 гг. Они проводились с целью наблюдения и чтобы «заставить замолчать» критиков как внутри страны, так и за рубежом.

Группа, возможно, обучила (подкупила) двух сотрудников соцсети Twitter, чтобы попытаться получить доступ к личной информации диссидентов и радикалов, включая номера телефонов и IP-адреса. Так, 11 ноября 2015 года компанияTwitter выпустила уведомление о безопасности для десятков владельцев учетных записей, которые посещал один из ее бывших сотрудников.

Считается, что в этой деятельности усмотрели участие Сауд аль-Кахтани, бывшего советника наследного принца Саудовской Аравии — якобы именно он отдавал заказы израильской NSO Group на слежку за активистами и журналистами, критически настроенными к Эр-Рияду (столица Саудовской Аравии).

В своих атаках хакеры использовали методы watering hole и целевого фишинга. Nuo Chong Lions использовала четыре мобильных RAT, включая RAT с открытым исходным кодом (AndroRat), и три коммерческих RAT — SandroRat, SpyNote и MobiHok.

Chimera

География	Вектор первичной компрометации	Инструменты
Тайвань	Внешние удаленные сервисы	SkeletonKeyInjector Cobalt Strike ChimeRAR

Стало известно о хакерской группе, которая в 2018–2019 гг. атаковала несколько компаний сверхпроводниковой промышленности Тайваня. Во время расследования специалисты назвали эту угрозу **Chimera**.

Основной целью атак была эксфильтрация интеллектуальной собственности: документов по интегральным схемам (ИС), комплектов для разработки программного обеспечения (SDK), проектов ИС, исходного кода и т.д.

Причиной этих атак, вероятно, является конкуренция или борьба между государствами, о чем может свидетельствовать их продвинутый характер. Первой точкой входа был VPN-сервер, где использовалась действительная учетная запись. Скорее всего, пароль для входа в VPN совпадал с паролем из скомпрометированной учетной записи. Группа известна использованием вредоносной программы «с отмычками» (Skeleton Key), которая позволяла войти в систему жертвы без действительных учетных данных.

WildPressure

География	Вектор первичной компрометации	Инструменты
Средний Восток	Unknown	Milum

У группы **WildPressure** нет пересечений с другими APT-группами. Она проводила атаки на организации Ближнего Востока, часть из которых связана с промышленным сектором.

Хакеры распространяют полноценный троян **Milum**, написанный на C++. Анализ зашифрованных сообщений в запросах HTTP POST показал версию вредоносного ПО — 1.0.1. Такой номер указывает на раннюю стадию разработки. Другие поля указывают на существование как минимум планов для версий не на C++, из чего можно сделать вывод, что о группе мы еще услышим.

Возвращение давно знакомых APT-групп

Описываемый в данном отчете период знаменателен тем, что стало известно о длительных и скрытных атаках давно известных групп, которые, казалось, совсем ушли с радаров.

С одной стороны, это лишний раз показывает нам, что не стоит недооценивать APT-группы и их изощренность. С другой — обучение систем раннего обнаружения вредоносной инфраструктуры и ПО вносит существенный вклад в эффективность превентивных мер. Все больше атак удается обнаружить и отследить, в том числе потому, что большинство этих групп имеют свой уникальный стиль или используют свои собственные разработки.

Golden Falcon

Неожиданное открытие 2019 года — деятельность группы Golden Falcon (или APT-C-34), о которой стало известно после получения доступа к одному из их управляющих серверов.

Группа проводила хакерскую операцию против частных компаний и государственных организаций Казахстана. Двумя основными инструментами оказались:

— Вариация RCS (Remote Control System) — шпионский набор, продаваемый итальянским разработчиком HackingTeam;
— Бэкдор-троян Harpoon (CTC «Гарпун»).

Русскоязычная документация о последнем была обнаружена на управляющем сервере, что навевает мысль о том, что данный вредонос был заказан группировкой по собственному техническому заданию у сторонних разработчиков.

Действия Golden Falcon очень похожи на активность группы DustSquad, известной с 2017 года. Те также проводили кампании по шпионажу против Казахстана, но с трояном Octopus. Вполне возможно, что за группой стоят спецслужбы Казахстана или лица, заинтересованные в мониторинге обстановки внутри государства.

Naikon

Призом за «одну из самых незаметных и длительных кампаний» можно наградить китайскую группировку Naikon. Она провела пятилетнюю кампанию против правительственных учреждений высшего звена целевых стран в Азиатско-Тихоокеанском регионе.

Naikon использовала новый бэкдор под названием Aria-body, способный создавать и удалять файлы и каталоги, делать скриншоты, выполнять поиск файлов, собирать метаданные файлов, информацию о системе и местоположении. Несмотря на распространенный вектор атаки (отправка электронных писем с вредоносными вложениями), группа проводит их очень эффективно.

APT20

Два года оставалась незамеченной группа APT20, которая атаковала коммерческие организации и правительственные учреждения, похищая пароли и обходя двухфакторную аутентификацию для сбора данных.

Их кампания Operation Wocao оказалась масштабной и затронула следующие отрасли: авиацию, строительство, финансовую сферу, здравоохранение, страхование, азартные игры и энергетику. Преступники эффективно заметали следы, регулярно удаляли инструменты для кражи данных с зараженных компьютеров.

APT5

Еще одно неожиданное возвращение — APT5 (она же Manganese). Группа действует с 2007 года и состоит из нескольких подгрупп с определенной тактикой и инфраструктурой.

Преступники атакуют и взламывают организации в разных отраслях, но в первую очередь уделяют внимание телекоммуникационным и технологическим компаниям. Особый интерес для них представляют фирмы, занимающиеся спутниковой связью.

На этот раз APT5 создала инфраструктуру для интернет-сканирования и поиска корпоративных VPN-серверов Fortinet и Pulse Secure. Затем преступники попытались воспользоваться уязвимостями в VPN-серверах (CVE-2018-13379 в Fortinet и CVE-2019-11510 в Pulse Secure), которые связаны с «предварительным считыванием файлов». Их эксплуатация позволяет неавторизованному злоумышленнику извлекать файлы с VPN-сервера.

APT30

Оказалось, что группа APT30 поддерживает свои инструменты десятилетней давности (BACKSPACE и NETEAGLE) и использует их в атаках на Юго-Восточную Азию. Кроме того, хакеры продолжают придерживаться известных подходов к организации сетевых ресурсов и тестируют свежее программное обеспечение — RHttpCtrl и RCtrl.

Cycldek

Отметились и хакеры из Cycldek. Обнаружено использование этой группой трояна USBCulprit, который предназначен для кражи данных из корпоративных сетей и дает злоумышленникам возможность проникнуть на отключенные от сети и физически изолированные устройства.

По данным специалистов, вредонос оставался незамеченным с 2014 года и новые образцы появлялись в 2019 году. Вся активность группы была сосредоточена на правительственных организациях в нескольких странах Юго-Восточной Азии.

Значимые операции

Атаки на ядерные объекты

2019, Индия

В сентябре 2019 года специалисты Group-IB обнаружили архив, содержащий **Dtrack** — инструмент удаленного администрирования, который атрибутируется к северокорейским хакерам Lazarus.

Как показало наше исследование, логи содержат данные со скомпрометированной машины под управлением ОС Windows, которая принадлежит работнику Индийской корпорации по атомной энергии (Nuclear Power Corporation of India Limited, NPCIL).

Все файлы в архиве скомпилированы в разное время, однако стоит отметить, что основной файл со скомпрометированными данными датируется 30 января 2019 года, более чем за полгода до обнаружения. Можно предположить, что хакеры долго оставались незамеченными в сети жертвы.

Вскоре стало известно, что в результате атаки была скомпрометирована АЭС «Куданкулам» — атомная электростанция в Индии, расположенная на юге индийского штата Тамилнад. 19 октября 2019 года второй энергоблок АЭС был отключен. Мы предполагаем, что данные события могут быть связаны.

По официальным заявлениям, причина остановки энергоблока: SG level low.

Second nuclear plant at TN's Kudankulam stops operation

The second 1,000 MW nuclear power unit at Kudankulam, owned by the Nuclear Power Corporation of India Ltd (NPCIL) stopped power generation on Saturday.

IANS | Oct 19, 2019, 01.48 PM IST

A+

CHENNAI: The second 1,000 MW nuclear power unit at Kudankulam, owned by the Nuclear Power Corporation of India Ltd NSE -0.46 % (NPCIL) stopped power generation on Saturday, said Power System Operation Corporation Ltd (POSOCO).

The atomic power plant stopped generation about 12.30 a.m. on Saturday owing to "SG level low", the company added.

The expected date of the unit's revival is not known.

Другими словами, давление в парогенераторе, который отвечает за передачу тепла от активной зоны до турбины электрогенератора, было низким. Это могло привести к перегреву активной зоны.

После того как ИБ-исследователь Пухрадж Сингх опубликовал информацию об атаке в Twitter, администрация АЭС отрицала, что «Куданкулам» подверглась какому-либо заражению, выпустив заявление, в котором его слова были названы «ложной информацией», а кибератака «невозможной».

Но позже Индийская корпорация по атомной энергии сообщила, что заявления представителей АЭС не совсем соответствовали истине и кибератака все же имела место. Официальная версия NPCIL гласит, что троян проник в административную сеть АЭС, заразив один компьютер, но не достиг критически важной внутренней сети, которая используется для управления ядерными реакторами.

2020, Южная Корея

В апреле 2020 Lazarus отправила вредоносные рассылки в сторону одной компании в сфере энергетики Южной Кореи. Темой стали приглашения на работу в KHNP (Korea Hydro & Nuclear Power Co., Ltd.). KHNP является дочерней компанией Korea Electric Power Corporation. Она управляет крупными атомными и гидроэлектростанциями в Южной Корее, которые обеспечивают около 30% поставок электроэнергии в стране.

Кроме того, начиная с октября 2019 года северокорейские группировки Lazarus и Kimsuky активно атакуют оборонные предприятия в Южной Корее, и с апреля 2020 года эти атаки только усиливаются.

2020, Иран

3 июля 2020 года стало известно, что власти Израиля под подозрением в осуществлении кибератаки на один из ядерных объектов Ирана. Инцидент произошел 2 июля и повлек за собой пожар и взрыв на подземном объекте по обогащению урана в Натанзе.

До того как стало известно о пожаре в Натанзе, на электронную почту персидской службы BBC пришло письмо, в котором группа под названием «Гепарды родины» (Cheetahs of the Homeland) взяла на себя ответственность за нападение. Она якобы состоит из «бывших сотрудников иранских сил безопасности, решивших бороться против властей».

Как сообщили власти Ирана, взрыв нанес значительный ущерб и может сказаться на производстве центрифуг для обогащенного урана.

Атаки на объекты водоснабжения Израиля

В апреле 2020 года Национальный кибердиректорат Израиля (Israeli National Cyber-Directorate, INCD) выпустил предупреждение для компаний, работающих в сфере энергетики и водоснабжения, где просил как можно скорее сменить пароли для всех подключенных к интернету систем.

В предупреждении сказано, что INCD получает сообщения о попытках атак на водоочистные сооружения, водонасосные станции и канализационные сети, которые подтвердили власти Израиля. Подробности атак не раскрываются, но глава INCD Игаль Унна заявил, что они могли привести к серьезной нехватке воды и потерям среди гражданского населения. Как сообщили власти, преступники атаковали автоматизированные системы управления технологическим процессом (АСУ ТП), но атаку удалось отразить.

Хотя исходные сообщения гласили, что атака злоумышленников вообще не увенчалась успехом, позже издание The Financial Times, ссылаясь на свои источники, сообщило, что хакеры получили доступ к системам очистки и пытались изменить уровень содержания хлора. Если бы эта диверсия удалась, злоумышленники могли бы спровоцировать волну отравлений среди местного населения.

Кроме того, израильское Управление по водным ресурсам предупредило, что в июне текущего года системы водоснабжения и очистки воды вновь подверглись атакам. Сообщается, что эти инциденты не нанесли никакого ущерба атакованным предприятиям.

По информации местных СМИ, первая атака была направлена на сельскохозяйственные водяные насосы в Верхней Галилее, а вторая — на водяные насосы в центральной провинции Матех-Иегуда.

«Это были специальные небольшие дренажные сооружения в сельскохозяйственном секторе, которые были немедленно и независимо отремонтированы местными жителями, атаки не причинили никакого вреда или каких-либо реальных последствий», — говорится в заявлении Управления водного хозяйства Израиля.

Атаки на критические объекты Ирана

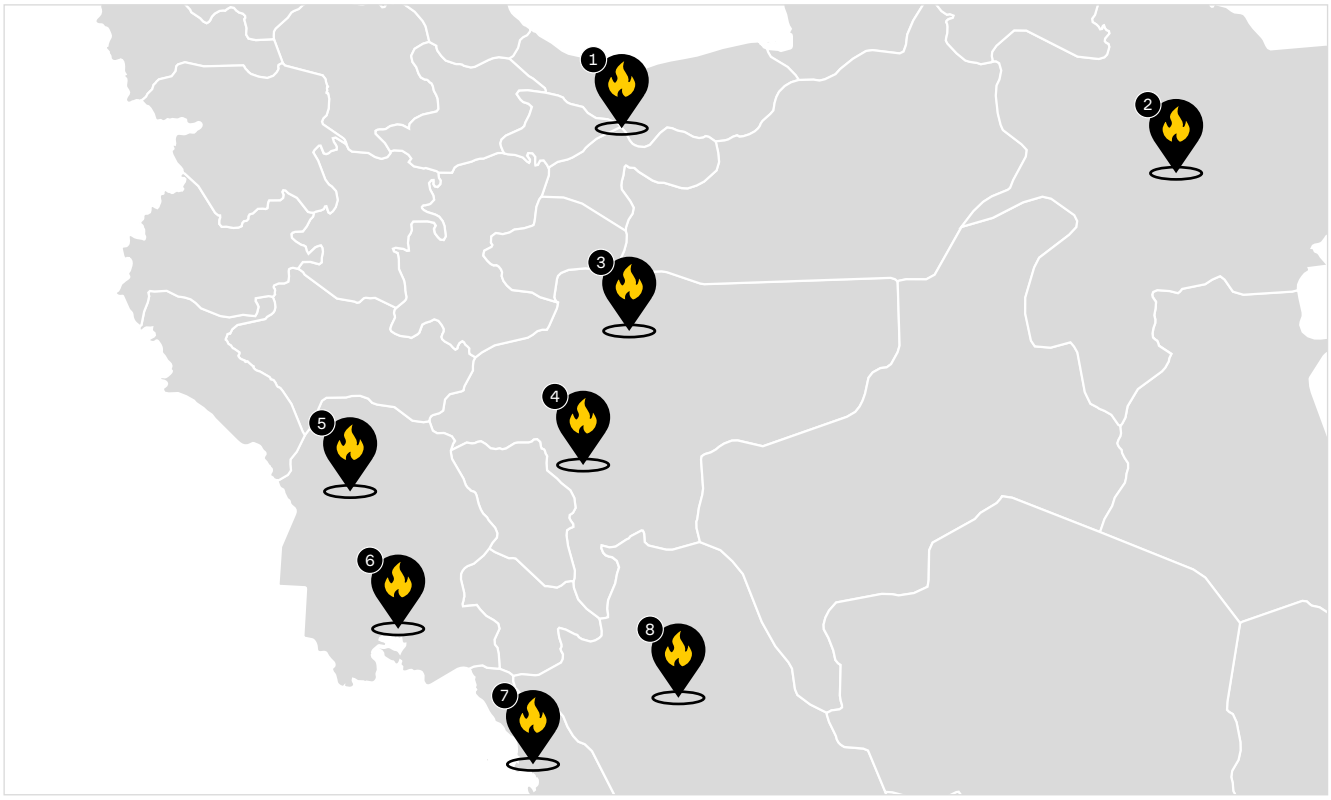
9 мая 2020 года была совершена кибератака на системы морского порта Шахид-Раджаи города Бендер-Аббас, находящегося на юге Ирана.

Согласно Министерству дорог и городского развития Ирана, она затронула ограниченное количество частных операционных ресурсов в порту и не нанесла существенного ущерба. Однако, как стало известно, произошел сбой в работе компьютерных систем, регулирующих потоки судов, грузового транспорта и товаров, что создало заторы на водных путях и дорогах, ведущих к объекту.

Взлом может быть ответом на попытку иранских хакеров атаковать израильскую водную инфраструктуру.

За этой атакой последовала череда различных аварий и взрывов, которые фиксировались на различных критических объектах Ирана, включая нефтехимические заводы, центры обогащения урана, электростанции, порты и т. д.

Рисунок 7. Карта аварий и взрывов в Иране



1. **June 26 →** Khojir SSM facility
   June 30 → Sina Athar Clinic in Shariati Avenue
   July 13 → Shian forest
   July 9 → Garnadareg explosion
   July 12 → Enghelab fire
2. **July 13 →** Kavian Friman industrial complex
3. **July 2 →** Natanz nuclear enrichment facility
4. **July 13 →** Najafabad fire
   July 19 → Isfahan power plant
5. **July 4 →** Zargan power plant
   July 4 → Karoon petrochemicals plant
6. **July 12 →** Shahid Tondgooyan petrochemical plant in Khyzestan province
7. **July 15 →** Bushehr ships fire
8. **July 3 →** Shiraz fire

26 июня в районе Тегерана произошел сильный взрыв. Иранское правительство поспешило объяснить этот эпизода взрывом газа на военной базе Парчин. Но спутниковые снимки показывают, что на самом деле взрыв произошел на базе ракетно-производственного комплекса Ходжир (входит в Shahid Hemmat Industrial Group). Здесь проложены подземные тоннели и, по предположениям экспертов, хранится растущий ракетный арсенал Ирана.

В Иране связали эту атаку с новостями об отключении электроэнергии в Ширазе, почти в 600 милях к югу. В Ширазе также есть крупные военные объекты, а взрыв и отключение электричества произошли в тот же час в пятницу. Представители американских и израильских спецслужб настаивают, что они не имеют к этому никакого отношения.

Рисунок 8. Спутниковый снимок места взрыва в горах на востоке Тегерана

УГРОЗЫ ДЛЯ ТЕЛЕКОММУНИКАЦИЙ

6 групп, связанных со спецслужбами,

атаковали телеком-сектор в этом году

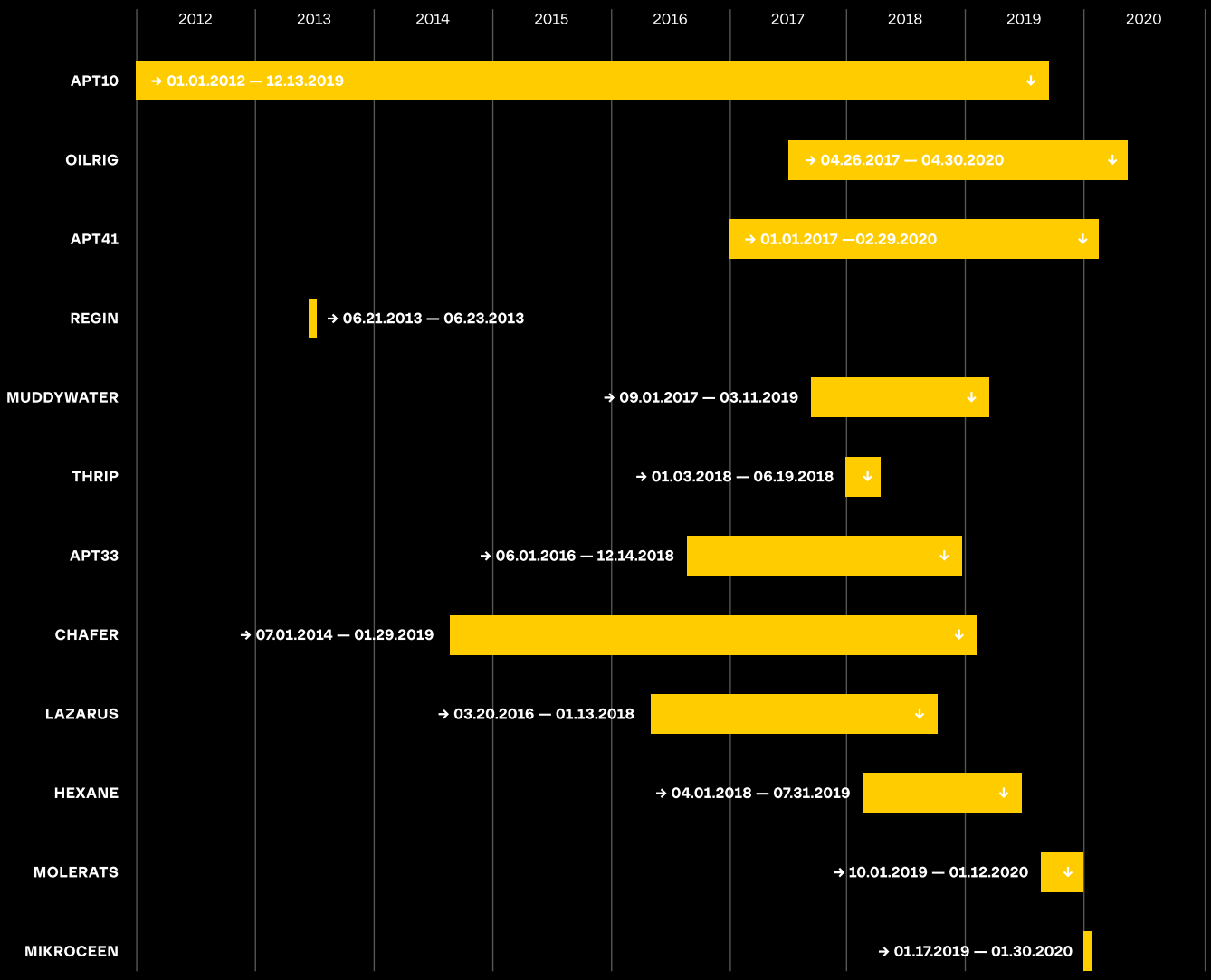
2,3 Тб/с и 809 млн пакетов в секунду (Mpps) —

зафиксированы новые, рекордные по своей силе атаки

Основной угрозой для телеком-компаний являются атаки спецслужб, и за анализируемый период активность в телекоммуникационном секторе проявили 6 таких групп, атаковавших как обычных, так и мобильных операторов связи.

Традиционными проблемами, с которыми сталкиваются операторы, являются утечки BGP-маршрутов и DDoS-атаки, мощность которых непрерывно растет и ставит новые рекорды.

Спецслужбы, атакующие телеком-сектор



95 МЕСЯЦЕВ

вела свою деятельность одна из группировок, направленная на телеком-сектор

APT41

Группировка APT41 организовала целый ряд атак. В феврале 2020 года хакеры скомпрометировали маршрутизатор Cisco RV320 телекоммуникационной организации. Неизвестно, какой именно эксплойт использовался, но существует модуль Metasploit, объединяющий уязвимости CVE-2019-1653 и CVE-2019-1652 и позволяющий удаленно выполнять код на подобных маршрутизаторах. Для размещения определенной полезной нагрузки он использует wget.

Преступники также эксплуатировали уязвимость (CVE-2020-10189) в Zoho ManageEngine, позволяющую удаленно выполнять код без авторизации с правами суперпользователя или SYSTEM.

На следующий день после исправления уязвимости CVE-2020-10189 преступники атаковали более десятка систем и смогли скомпрометировать как минимум пять из них. Затем злоумышленники разместили пробную версию загрузчика Cobalt Strike BEACON и внедрили еще один бэкдор для загрузки VMProtected Meterpreter.

OilRig

Иранская группа OilRig причастна сразу к двум кампаниям, затрагивающим телекоммуникационный сектор.

Первая кампания, как оказалось, была активна на протяжении последних трех лет. В публичном пространстве ее окрестили **Fox Kitten**. В ходе этой операции злоумышленникам удалось получить доступ и закрепиться в сетях многочисленных компаний и организаций из разных секторов, в том числе и секторе телекоммуникаций.

Первоначальное проникновение в целевые организации было выполнено в большинстве случаев с использованием 1-day уязвимостей в различных VPN-сервисах, таких как Pulse Secure VPN, Fortinet VPN и Global Protect от Palo Alto Networks. Получив точку входа, злоумышленники пытались сохранить доступ к сетям, открыв множество средств коммуникаций, включая каналы связи по RDP через туннелирование по SSH. На последнем этапе после успешного проникновения в организацию злоумышленники выполняли процесс идентификации, проверки и фильтрации конфиденциальной и ценной информации от каждой целевой организации.

Вторая кампания затронула телеком-провайдеров Южной Азии и была обнаружена в апреле 2020 года. В ходе этой кампании злоумышленники использовали такие фреймворки и инструменты для постэксплуатации, как Covenant, Cobalt Stike, Metasploit и Mimikatz, а также легитимные инструменты Plink, Bitvise и Bitsadmin. Для получения первоначального доступа злоумышленники использовали фишинговые письма. Основной целью данной кампании является кража данных учетных записей пользователей с последующим получением доступа к серверам баз данных.

Атака была длительной, так как злоумышленники могли присутствовать в сети одной организации начиная с октября 2019 года. Первые вредоносные действия были замечены 11 октября 2019 года, когда была выполнена PowerShell-команда для установки модуля CobaltStrike Beacon. Затем злоумышленники выполнили PowerShell-команду, запускающую загруженный файл, который представляет собой Metasploit, для закрепления в системе.

Следующие действия начались 6 февраля 2020 года, когда была выполнена очередная PowerShell-команда для поиска файлов, похожих на web.config. Из каждого найденного файла по возможности извлекается информация об имени пользователя и пароле. Эти учетные данные могут использоваться для доступа к ресурсам организации, таким как SQL-серверы.

11 марта злоумышленники попытались подключиться к серверу базы данных через PowerShell, предположительно с использованием украденных учетных данных. Они также использовали команду SQL для получения информации о версии сервера базы данных, возможно, для проверки учетных данных и подключения.

Molerats

В период с октября по начало декабря 2019 года специалисты наблюдали фишинговые атаки, которые, вероятно, связаны с группой Molerats (AKA Gaza Hackers Team и Gaza Cybergang). Целями стали восемь организаций в шести различных странах, в том числе правительственные структуры, телекоммуникационные, страховые компании и предприятия розничной торговли.

Все атаки включали фишинговые электронные письма для доставки вредоносных документов, которые требовали от получателя выполнения определенных действий. Методы социальной инженерии включали заманчивые изображения, чтобы пользователь позволил контенту запустить макрос. Кроме того, пользователям угрожали выпустить компрометирующие изображения в СМИ, чтобы они перешли по ссылке для получения вредоносной полезной нагрузки. В большинстве атак это был бэкдор Spark, позволяющий субъектам угроз открывать приложения и запускать команды командной строки в скомпрометированной системе.

Mikroceen

Аналитики дали название Mikroceen кампании неизвестной китайской APT-группировки, шпионившей с помощью трояна за неназванными телекоммуникационной и газовой компаниями, а также правительственным учреждением в Центральной Азии.

В своих операциях группа использовала бэкдоры, чтобы получить постоянный доступ к корпоративным сетям своих жертв. Основываясь на полученных данных, исследователи предполагают, что ранее эта группа была активна как минимум с 2017 года и причастна к другим атакам: Microcin — против российских военнослужащих, BYEBY — против правительства Беларуси и Vicious Panda — против государственного сектора Монголии. Данная теория подкрепляется тем, что, во-первых, использовался троян Gh0st RAT, который давно и часто применяется китайскими APT-группами, во-вторых, аналитики обнаружили явные сходства в коде использованных вредоносных программ.

Атаки на мобильных операторов

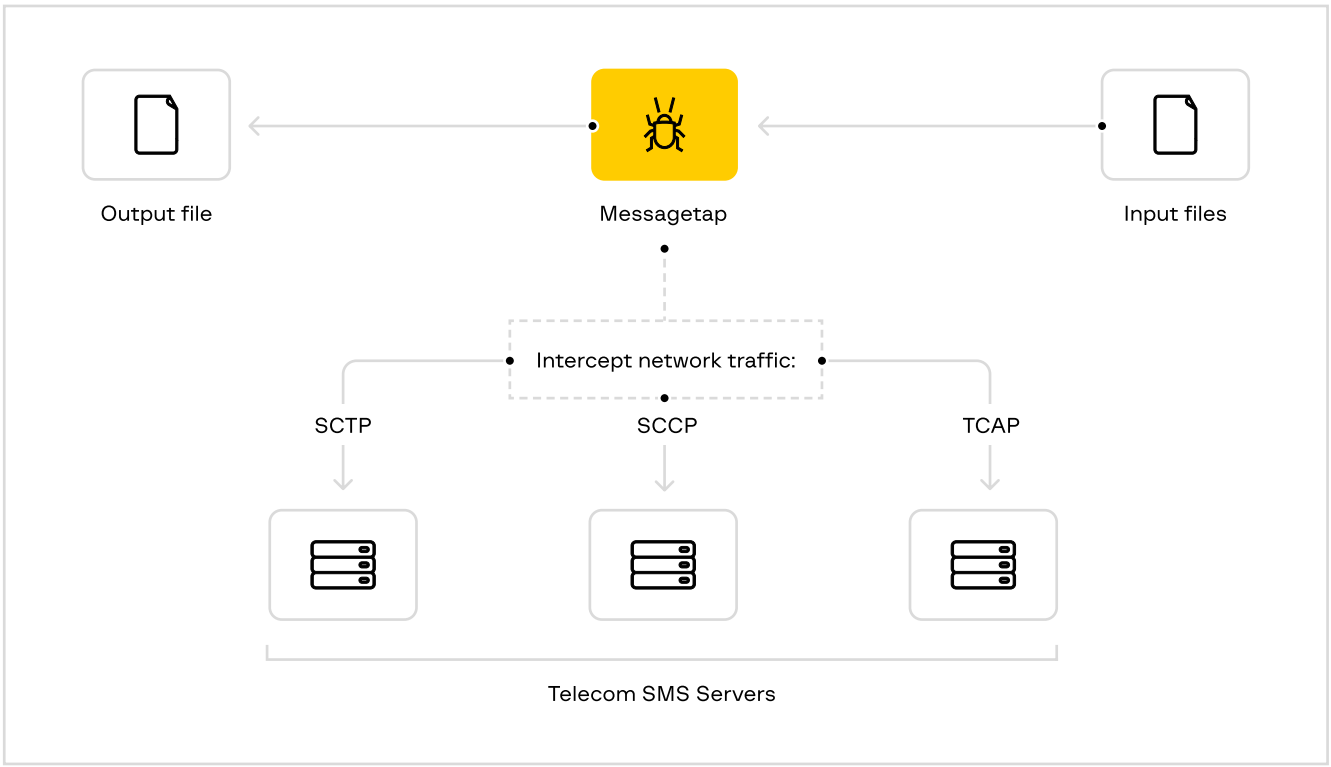
Спонсируемые китайским государством хакеры из APT41 были очень активны в этот период, и одним из значимых инструментов в их арсенале стал **Messagetap.**

Вредонос предназначен для Linux-машин и создан для размещения на серверах SMSC (Short Message Service Center), отвечающих за работу службы коротких сообщений в сетях операторов связи. Так группировка скомпрометировала кластер серверов Linux неназванного телеком-провайдера, в результате чего могла перехватывать сообщения лиц, представляющих интерес для китайского правительства. Они искали сообщения через ключевые слова, составляющие геополитический интерес для китайских спецслужб, в том числе имена политических лидеров, названия военных и разведывательных организаций, а также политических движений.

Помимо этого, MESSAGETAP интересуется сообщениями, отправленными на определенные номера или с этих номеров, а также конкретными устройствами, опираясь на их International Mobile Subscriber Identity (IMSI). В момент обнаружения группа отслеживала тысячи телефонных номеров и IMSI одновременно.

В ходе атаки группировка APT41 также искала базы данных с логами работы телекоммуникационного оборудования (Call Detail Record) отдельных лиц, включающие информацию о времени, когда были совершены звонки, используемые телефонные номера и продолжительность разговоров.

Рисунок 9. Схема работы Messagetap



MESSAGETAP представляет собой 64-битный ELF-анализатор данных, изначально загружаемый установочным скриптом. После установки вредонос проверяет наличие конфигурационных файлов keyword_parm.txt и parm.txt, содержащих инструкции по выбору целей, а также какие текстовые сообщения нужно извлечь. После прочтения и загрузки в память оба конфигурационных файла удаляются с диска, далее инструмент загружает списки с ключевыми словами и IMSI-номерами и приступает к мониторингу всех сетевых соединений от и к серверу. Он использует библиотеку libpcap для просмотра трафика и извлекает метаданные SMS-сообщений, включая содержание SMS-сообщения, номер IMSI, а также телефонные номера отправителя и получателя.

Исходя из вышеперечисленного, организациям и конечным пользователям стоит учитывать риск компрометации данных на нескольких уровнях выше в их цепочке сотовой связи. Лица, представляющие особый интерес для геополитики других стран, такие как активисты, диссиденты, журналисты, работники государственных предприятий, работающие с конфиденциальной информацией, должны осознавать риски передачи конфиденциальных данных по SMS.

BGP Hijacking

Проблема BGP Hijacking в мире остается актуальной. Зачастую происходят и преднамеренные атаки, и сбои по вине компаний с некорректно настроенными конфигурациями или префикс-фильтрами.

Дата	Название	Краткое описание
21.07.2020	AS 264462 Comercial Conecte Sem Fio Ltda me, Бразилия	Компрометация 13 046 префиксов. Пострадавшие ISP принадлежат Индии, России, Южной Корее, Вьетнаму
09.06.2020	IBM Cloud	Сбой в работе IBM Cloud (облачный дата-центр), вызванный тем, что внешний провайдер направил туда некорректные маршруты
23.04.2020	AS205310 Beiersdorf Shared Services GmbH, Германия	Компрометация 90 000 префиксов — маршруты были перенаправлены в AS15943 вместо AS8220
22.04.2020	AS263444 Open X Tecnologia Ltda, Бразилия	Утечка 9328 префиксов из 1250 AS, включая Akamai, Cloudflare, Vodafone, NTT, Amazon, NVIDIA
05.04.2020	AS7552 Viettel, Вьетнам	Утечка 4825 префиксов 326 операторов
01.04.2020	AS12389 Rostelecom, Россия	Утечка 8870 префиксов из почти 200 AS, включая Akamai, Cloudflare, Hetzner, Digital Ocean, Amazon AWS
31.03.2020	AS50048 NEWREAL-AS, Россия	Утечка 2658 префиксов в Tier-2 ISP Transtelecom, префиксы принадлежали Orange, Akamai, Rostelecom и др
16.02.2020	AS139070 Google Asia Pacific Pte. Ltd., Сингапур	—
07.02.2020	AS8359 MTS, Россия	Утечка 225 префиксов из 36 AS

Изменение мощности DDoS-атак

Увеличение количества устройств интернета вещей (IoT) привело к росту количества хостов в популярных бот-сетях (например, Mirai), а также появлению новых бот-сетей.

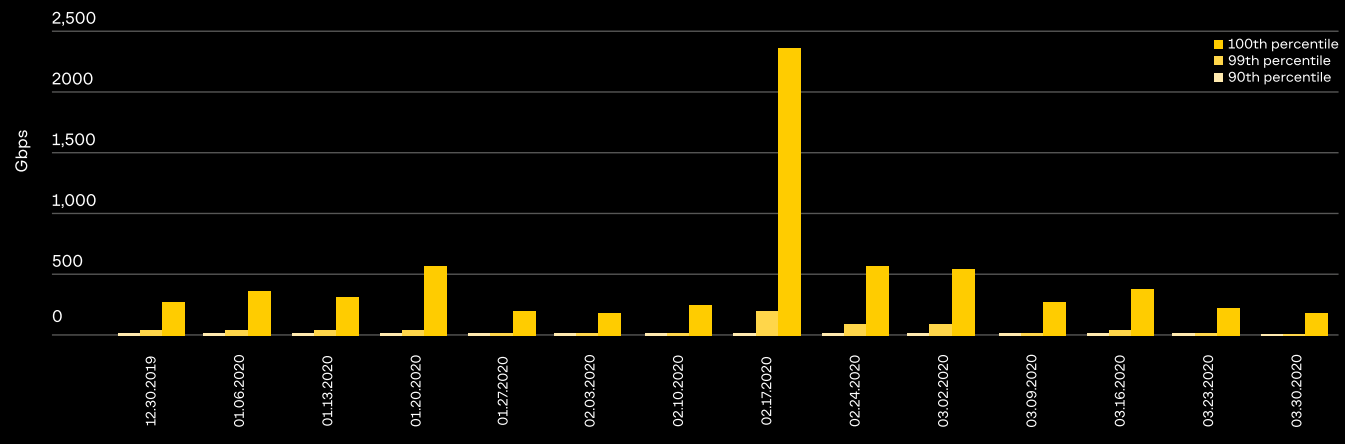
Касательно техник проведения DDoS-атак, SYN-флуд по-прежнему остается самым популярным типом атаки. ICMP-флуд атаки вышли с последнего на второе место по популярности, а на последнем месте оказался HTTP-флуд с минимальными показателями с января 2019-го.

В 2020 году наблюдается рост мощности атак типа отказа в обслуживании. Именно на первую половину года приходится рекордное количество зафиксированных атак.

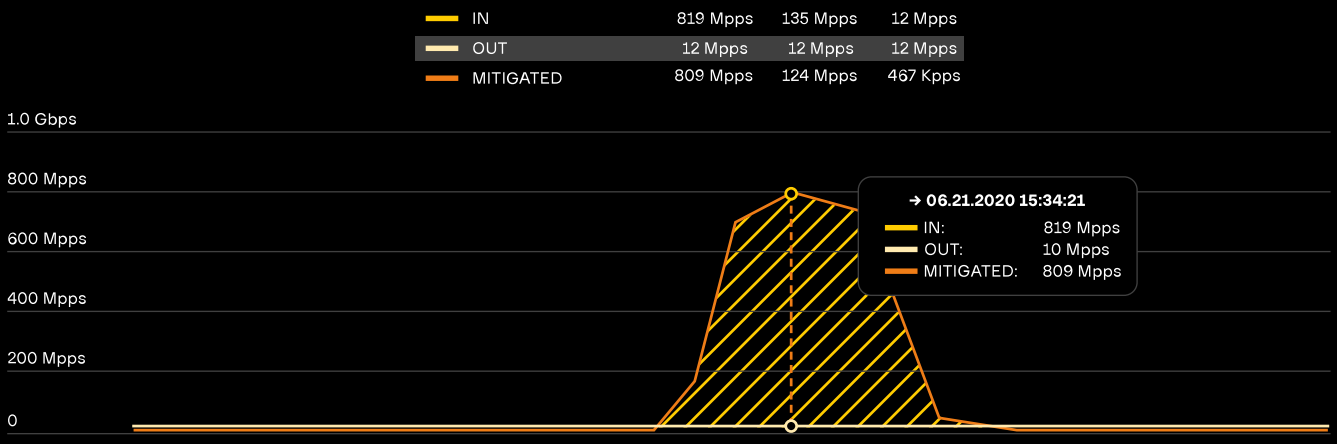
Крупнейшая DDoS-атака в Gbps

Согласно отчету Amazon за I квартал 2020 года, служба AWS Shield в середине февраля отразила самую крупную DDoS-атаку из когда-либо зафиксированных, объем которой достигал **2,3 Тб/с**. Компания не раскрывает ни источника, ни цели атаки. Она была проведена с использованием взломанных CLDAP веб-серверов и продолжалась в течение трех дней. CLDAP (Connectionless Lightweight Directory Access Protocol) — это альтернатива более старому протоколу LDAP, которая используется для проведения DDoS-атак начиная с 2016 года. Используя CLDAP-сервера, злоумышленники способны отразить и приумножить DDoS-трафик в 76 раз от его первоначального объема, что делает их востребованным для киберпреступников, предоставляющих сервисы осуществления заказных DDoS-атак.

Предыдущий рекорд крупнейшей из DDoS-атак объемом 1,7 Тб/с был зафиксирован в марте 2018 года. Данная атака была отражена компанией NETSCOUT Arbor. При проведении атаки были использованы взломанные веб-сервера с технологией Memcached для амплификации DDoS-трафика.



Крупнейшая DDoS-атака в MPPS



Графики из отчета Akamai (https://blogs.akamai.com/2020/06/largest-ever-recorded-packet-per-secondbased-ddos-attack-mitigated-by-akamai.html)

Крупнейшая DDoS-атака в MPPS

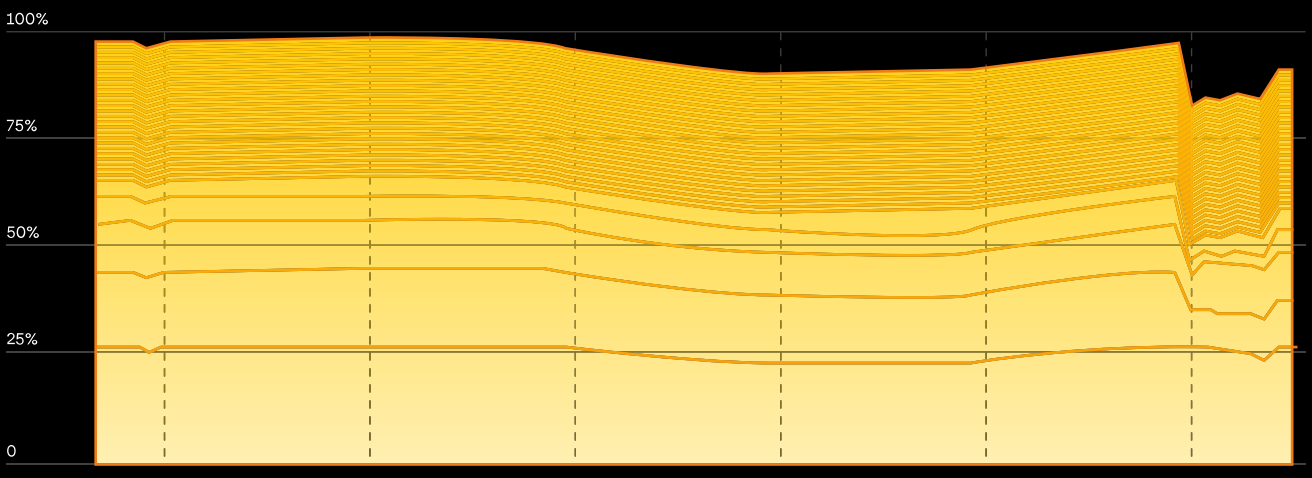
Атака, о которой сообщили специалисты компании Akamai, была произведена 21 июня 2020 года на европейскую финансовую организацию (банк), название которой не было раскрыто. Объем атаки составил 809 млн пакетов в секунду (MPPS). Важной особенностью является то, что подавляющее большинство трафика атаки (96,2%) было получено от IP-адресов, которые не были зарегистрированы в предыдущих атаках 2020 года, что указывает на появление новой бот-сети. Атака 21 июня была примечательна не только своими размерами, но и скоростью, с которой она достигла своего пика. Атака выросла с обычного уровня трафика до 418 Гбит/с за считаные секунды, а затем достигла своего пика в 809 Mpps примерно за две минуты. В общей сложности атака длилась чуть менее 10 минут.

Проблемы доступности на уровне страны

В начале февраля 2020 года инфраструктура Ирана подверглась масштабной DDoS-атаке, в результате которой без доступа к сети оказались 25% иранских интернет-пользователей. Как сообщает интернет-обсерватория NetBlocks, осуществляющая мониторинг безопасности и свободы интернета, сбои в работе сети начались в субботу, 8 февраля, в 11:45 по местному времени (11:15 МСК).

Проблемы с доступом к интернету затрагивали крупнейших иранских операторов связи. Частично возобновить подключение удалось в течение одного часа после отключения, однако некоторые сети не могли восстановить связь на протяжении семи часов.

Проблемы доступности на уровне страны



Netblocks.org: Network Connectivity, Iran: → 02.07.2020 — 02.08.2020 UTC

УГРОЗЫ ДЛЯ ЭНЕРГЕТИЧЕСКОГО СЕКТОРА

Объекты ядерной энергетики Индии и Ирана

пострадали от успешных атак в этом году

Обход «воздушного зазора»

появились новые инструменты для атак на физически изолированные сети

Для энергетического сектора этот год стал насыщенным с точки зрения угроз. самое интересное происходило в атомной энергетике, о чем мы писали в разделе «Военные операции» данного отчета. Атакующие успешно останавливали энергоблоки, физически разрушали прилегающую инфраструктуру.

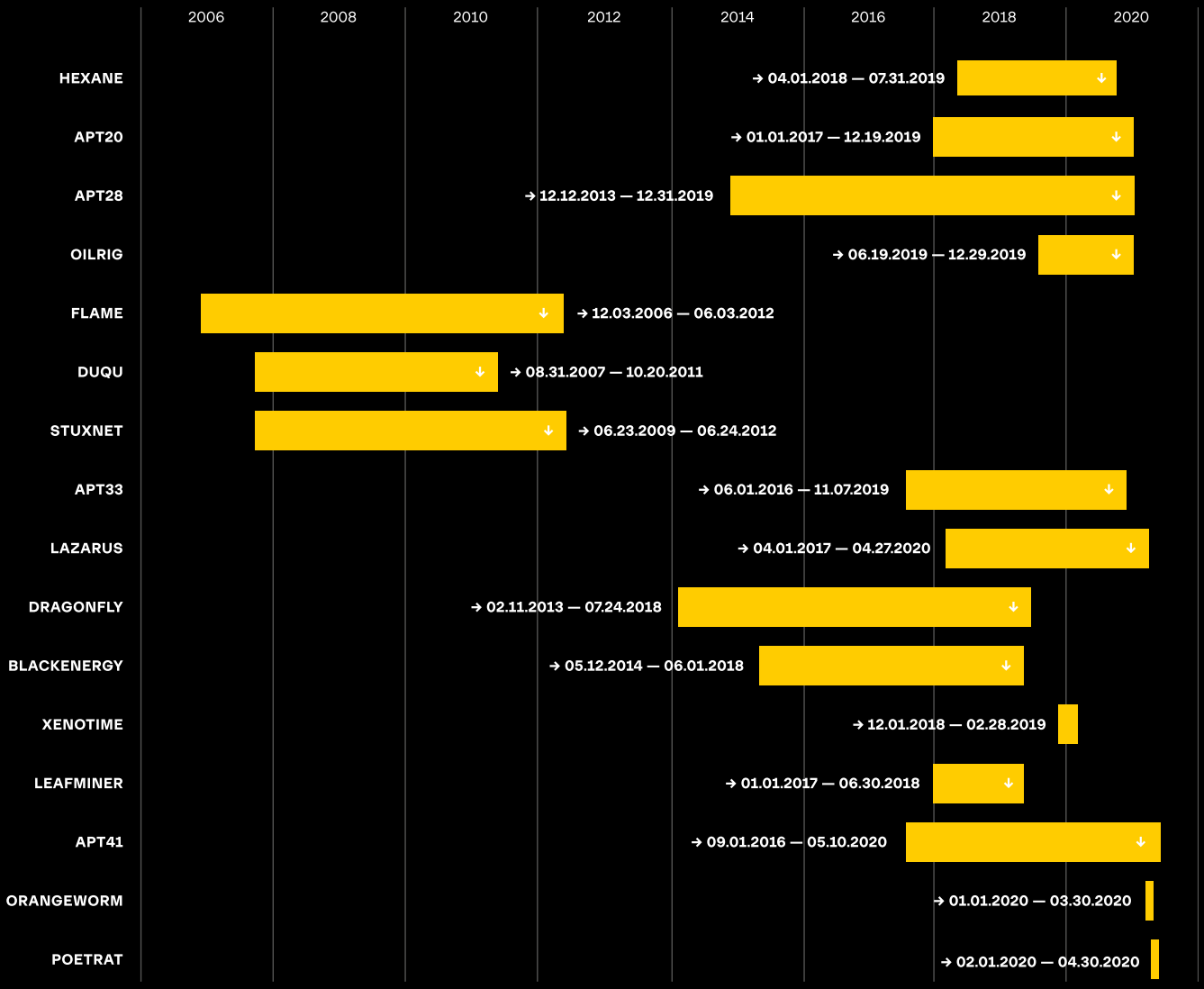
В этом году структуры ядерной энергетики Ирана стали объектом нападений с целью саботажа, а в Индии — с целью шпионажа. Индия представляет интерес, так как развивает ядерную технологию и реакторы на основе тория.

Серьезной угрозой для энергетических компаний являются не только спецслужбы, но и обычная организованная преступность, при этом и те, и те готовы останавливать производство, используя программы-шифровальщики для получения выкупа.

За анализируемый период активность в энергетическом секторе проявили 9 групп, связанных с спецслужбами.

При этом некоторые из них, например APT41 (Китай), активно применяли программы-шифровальщики для вывода сетей из строя.

Спецслужбы, атакующие энергетический сектор



9 ГРУПП,

связанных со спецслужбами, проявляли интерес к энергетическому сектору в период H2 2019 — H1 2020

Исследуя уже проведенные атаки, можно утверждать, что в случае с энергетическим сектором атакующие используют следующие методы:

Вектор атаки	Принцип работы
Разведка через OPC	Для сбора информации об используемом оборудовании, а также обнаружения его топологии злоумышленники применяют протокол OPC.
Доступ к SCADA HMI	Поскольку рабочие места с HMI имеют маленькую поверхность атаки, то, помимо стандартных способов получения доступа к компьютерам под управлением ОС Windows, атакующие активно исследуют уязвимости в HMI, эксплуатация которых позволит выполнить вредоносный код.
Управление контроллерами	Фреймворки атакующих (например, Idustroyer) пополняются модулями, которые позволяют управлять контроллерами по их стандартным протоколам, например IEC 60870-5-101, IEC 60870-5-104, IEC 61850.
Управление противоаварийной защитой	Для контроля над системами противоаварийной защиты, позволяющими останавливать производства, злоумышленники разработали соответствующие модули управления ими. Например, фреймворк Triton.
Проникновение через домашние роутеры и NAS	Для обнаружения промышленных сетей на сетевые устройства загружаются модули для анализа трафика и обнаружения протокола Modbus. Например, фреймворк VPNFilter.

APT20

Китайские хакеры из APT20 атаковали организации в десяти странах в рамках кампании Operation Wocao, которая в том числе затронула отрасль энергетики.

Преступники обычно получают доступ к системам, эксплуатируя уязвимость в веб-серверах, которыми управляет компания или государственное учреждение. Затем они продвигаются дальше по сети в поисках учетных данных системных администраторов с привилегированным доступом к наиболее важным частям инфраструктуры.

APT20 загружали кейлоггеры на компьютерные системы администраторов для записи нажатий клавиш и хищения паролей. В ходе кампании они использовали следующие инструменты:

— веб-шеллы для загрузки файлов и выполнения команд;
— скрипт для сканирования системы на предмет необходимой группе информации;
— кастомный бэкдор XServer;
— CheckAdmin для определения авторизованных администраторов и другие.

APT28

Группу APT28 (aka Fancy Bear) подозревают в проведении атаки на украинский нефтегазовый холдинг Burisma в начале ноября 2019 года. Злоумышленники зарегистрировали поддельные домены, замаскированные под легитимные сайты дочерних и партнерских для Burisma организаций — KUB-Gas LLC, Esko-Pivnich и CUB Energy Inc.

Злоумышленники рассылали сотрудникам компании письма, внешне похожие на легитимные, за исключением того, что записи аутентификации отправителя были настроены посредством SPF и DKIM. Полученные таким образом данные нескольких работников позволили атакующим скрытно действовать внутри сети организации и получать необходимую информацию.

APT41

В ходе волны атак на цели на Тайване группировка APT41 использовала новый шифровальщик — ColdLock. По всей видимости, его прямыми предшественниками являются такие семейства вымогателей, как Freezing и «образовательный» набор вымогателей EDA2. Например, от первого он перенял аналогичный способ распространения в сетях (скомпрометированные серверы AD), методы отражающей инъекции и внутреннюю модульную архитектуру.

ColdLock останавливает некоторые службы перед шифрованием их файлов:

— mariadb
— msexchangeis
— mssql
— mysql
— oracleservice

Также он завершает процесс Outlook и проверяет версию Windows. Шифровальщик выполняет несколько специфических подпрограмм для версии ОС Windows 10, отключая защитник Windows, push-уведомления и отправку отзывов/образцов вредоносных программ в Microsoft.

Стало известно, что эта атака зацепила CPC Corp., которая отвечает за доставку нефтепродуктов по всему Тайваню. Как сообщают источники, атака не повлияла на производство, но помешала попыткам некоторых клиентов использовать платежные карты CPC Corp. для покупки газа.

PoetRAT

Действия ранее неизвестного трояна удаленного доступа PoetRAT были обнаружены в феврале 2020 года. Атаки затронули государственный сектор и промышленные компании Азербайджана, главным образом энергетические. В рамках расследования было установлено, что особенный интерес злоумышленники проявляют к SCADA-системам, связанным с ветряными турбинами.

RAT написан на Python и имеет все стандартные функции этого типа вредоносного ПО, обеспечивая полный контроль над скомпрометированной системой в процессе работы.

Злоумышленники рассылали вредоносные документы Microsoft Word, некоторые якобы от правительственных учреждений Азербайджана или от Организации оборонных исследований и разработок Индии. Названия ряда файлов содержали отсылку к COVID-19.

Злоумышленники следили за конкретными каталогами, чтобы украсть определенную информацию о жертвах, используя кейлоггер, стиллер учетных данных браузера, а также Mimikatz и pypykatz для дальнейшего сбора учетных данных.

OilRig

Иранские хакеры вновь были замечены за использованием вайперов, но на этот раз атаки приписывают группе OilRig (aka APT34). Новый троян получил название ZeroCleare и участвовал в недавно обнаруженной целенаправленной атаке на нефтегазовую компанию.

Атака началась осенью 2018 года с разведывательного сканирования различных дешевых/бесплатных провайдеров VPN и получения доступа к одной из учетных записей, которая впоследствии была задействована в атаке. Летом 2019 года злоумышленники получили доступ к дополнительным учетным записям, чтобы установить веб-оболочки ASPX и получить права администратора домена.

После компрометации устройства через уязвимый драйвер вайпер распространялся на другие устройства в локальной сети для дальнейшей деструктивной атаки. Вредонос загружал EldoS RawDisk, легитимный инструмент для работы с файлами, дисками и разделами. Он и использовался, чтобы стереть MBR и повредить разделы диска. Точное число пострадавших организаций неизвестно, но по крайней мере

1400 хостов были заражены ZeroCleare.

Позже стало известно о новом витке развития трояна ZeroCleare, получившем название Dustman. Он был замечен в сети национальной нефтяной компании Бахрейна — Bapco. Общим компонентом обоих вредоносов является все тот же EldoS RawDisk. Отличие Dustman от других вайперов в том, что необходимые драйверы и загрузчики поставляются в одном исполняемом файле, а не в двух, как в случае с ZeroCleare. Также Dustman перезаписывает том, тогда как ZeroCleare стирает его, перезаписывая мусорными данными (0x55).

В этой атаке OilRig, скорее всего, пытались замести следы, так как ранее допустили ряд ошибок, которые и выявили их присутствие в сети.

Orangeworm

Начиная с января 2020 года отмечается волна атак с применением трояна Kwampirs. Этот вредонос связывают с группой Orangeworm, которая использовала его для атак на цепочки поставок сектора здравоохранения, в частности на поставщиков программного обеспечения.

Проникнув в систему, троян Kwampirs собирал базовые данные об устройстве и передавал на удаленный сервер. Также на зараженной машине открывался бэкдор, позволяющий злоумышленникам получить доступ к конфиденциальным данным. Если скомпрометированную систему определяли как потенциально интересную, производилось хищение данных, а также «агрессивное копирование» вредоноса на любые доступные машины и сетевые ресурсы организации.

В этом году интерес группы поменялся. В настоящий момент компании — поставщики ПО являются мишенью для атак с целью получения доступа к организациям, поддерживающим системы промышленного контроля (ICS) для глобального производства, передачи и распределения энергии.

Orangeworm официально не связывают с какой-либо страной. Однако, по словам ФБР, изучение исходных кодов Kwampirs позволяет предположить, что троян весьма похож на известный вайпер Shamoon, разработанный иранскими хакерами APT33, хоть и не имеет компонента-вайпера.

Атаки на физически изолированные сети

Несмотря на широкое применение сетевой изоляции, атаки на промышленные сети проходят успешно даже в тех случаях, когда для их разделения применяется «воздушный зазор».

Для его обхода атакующие применяют следующие основные методы:

— доверенные USB-устройства;
— подключенные Raspberry Pi устройства;
— атаки на цепочку поставок (supply chain).

В этот период отмечается появление новых инструментов, разработанных специально для проникновения в системы с воздушным зазором:

Группировка	Троян	Принцип работы
Cycldek (Китай)	USBCulprit	USBCulprit доставлялся с помощью другого трояна — NewCore RAT, который изначально попадал к пользователям через спирфишинговые письма на политические темы. Оказавшись в системе, USBCulprit изучал пути к исполняемым файлам и собирал документы с определенными расширениями, а затем переносил их на подключаемые USB-устройства. При подключении к компьютеру зараженных флешек троян либо загружал на них украденные данные, либо, наоборот, забирал записанную информацию на отключенном от сети компьютере.
Tropic Trooper (Китай)	USBferry	Установщик вредоносного ПО размещается через USB в физически изолированном хосте. Вредонос проверяет подключение к сети и, если обнаруживает, что сеть недоступна, пытается собрать информацию с целевой машины и скопировать собранные данные на USB-накопитель. После сбора данных троян пытается связаться с командным сервером для эксфильтрации данных.
DarkHotel (Южная Корея)	Ramsay 1 (сентябрь 2019); Ramsay 2.a (начало марта 2020); Ramsay 2.b (конец марта 2020)	Все версии вредоноса отличаются друг от друга и заражают жертв разными способами: Ramsay 1 и 2.b используют уязвимость в .doc (CVE-2017-0199), .rtf (CVE-2017-11882) и механизмы Visual Basic, интегрированные в Word. Версия 2.a рассчитана на применение «отвлекающего инсталлятора» в виде 7zip. Механизм закрепления в системе тоже зависит от используемой версии Ramsay. Некоторые из них имеют специальный модуль распространения spreader, который добавляет копии Ramsay ко всем файлам PE, обнаруженным на съемных дисках и среди сетевых ресурсов, чтобы в конечном итоге добраться до изолированных систем. Эксфильтрация собранных данных осуществляется внешним компонентом, который в настоящее время не удалось обнаружить.
Turla	COMpfun	Хакеры обновили классический троян удаленного доступа COMpfun и дополнили его возможностью отслеживать подключение съемных USB-устройств к зараженному хосту . Как предполагают эксперты, данный механизм используется Turla для заражения физически изолированных систем и автоматического распространения трояна.
Transparent Tribe	Компонент USBWorm трояна Crimson	USBWorm разработан для кражи файлов со съемных дисков и распространяется по системам, заражая съемные носители. Кража данных происходит путем перечисления всех файлов, хранящихся на устройстве, и копирования файлов с расширением, соответствующим заранее определенному списку. В процедуре заражения перечисляются все каталоги. USBWorm скрывает все фактические каталоги и заменяет их вредоносной копией с тем же именем. Более того, USBWorm использует значок, имитирующий каталог Windows, заставляя пользователя запустить вредоносное ПО при попытке доступа к каталогу.

Организованная преступность, атакующая энергетический сектор

Можно выделить два основных типа угроз для энергетического сектора, исходящих от криминальных структур:

— активная продажа доступов, в том числе к сетям энергетических компаний;

— атаки с использованием шифровальщиков.

Отдельно стоит отметить, что в некоторые программы-шифровальщики добавлены функции обнаружения процессов, связанных с системами управления промышленными предприятиями, чтобы обеспечить потерю данных, с которыми они работают, и повысить цену за возможность восстановления доступа. Особенно это относится к данным Historian-серверов.

Продажа доступов

2019

Дата	Продавец	Индустрия	Название	Домен	Регион	Цена($)
04.03.2019	Achilles	Горное дело и нефтегазодобыча	Нет	Нет	Нет	Нет
28.04.2019	Lampeduza	Горное дело и нефтегазодобыча	Stevin Rock LLC	stevinrock.com	ОАЭ	900
10.08.2019	bc.monster	Энергетика	Нет	Нет	Нет	4600
15.09.2019	B.Wanted	Горное дело и нефтегазодобыча	Нет	Нет	США	4600
21.09.2019	Gabrie1	Горное дело и нефтегазодобыча	Нет	Нет	США	24 000
11.11.2019	nikolaruss	Горное дело и нефтегазодобыча	Нет	Нет	Турция	3500

2020

Дата	Продавец	Индустрия	Название	Домен	Регион	Цена($)
08.02.2020	ellis.J.douglas	Энергетика	Entrust Energy	entrustenergy.com	США	1600
16.03.2020	rexus	Горное дело и нефтегазодобыча	Нет	Нет	Китай	10000
18.04.2020	cryzaa	Горное дело и нефтегазодобыча	Нет	Нет	Нет	3000
27.04.2020	Network	Горное дело и нефтегазодобыча	Нет	Нет	Нет	Нет
14.05.2020	zeoman	Горное дело и нефтегазодобыча	Нет	Нет	Нидерланды	2000
11.06.2020	fatfish	Энергетика	Нет	Нет	Канада	500
30.06.2020	drumrlu	Горное дело и нефтегазодобыча	Нет	Нет	ОАЭ	2000

В 2019 году злоумышленники стали реже публиковать полные названия компаний, что усложняет определение категории скомпрометированной организации. Всего, исходя из представленных описаний, было выявлено шесть компаний, которые относятся к энергетическому сектору, пять из них связаны с добычей ресурсов.

За 2020 год мы также не зафиксировали прироста продажи доступа к сетям компаний, связанных с энергетикой. За этот год было опубликовано семь компаний, две из которых связаны напрямую с энергетикой и пять — с добычей. Единственная компания, название которой было опубликовано, — Entrust Energy (https://www.entrustenergy.com/).

Атаки с использованием шифровальщиков

Дата	Шифровальщик	Индустрия	Название	Домен	Регион
11.11.2019	DoppelPaymer	Горное дело и нефтегазодобыча	Pemex	pemex.com	Мексика
14.01.2020	Maze	Энергетика	Electricaribe	electricaribe.co	Колумбия
20.02.2020	Clop	Горное дело и нефтегазодобыча	INA Group	ina.hr	Хорватия
02.04.2020	Nefilim	Горное дело и нефтегазодобыча	Aban Offshore	abanoffshore.com	Индия
06.04.2020	Maze	Горное дело и нефтегазодобыча	Groupement Berkine	Нет	Алжир
28.04.2020	Nefilim	Горное дело и нефтегазодобыча	W&T Offshore, Inc.	wtoffshore.com	США
26.05.2020	NetWalker	Энергетика	SolarReserve	solarreserve.com	США
09.06.2020	Snake	Энергетика	Enel Argentina	enel.com.ar	Аргентина
03.07.2020	REvil	Энергетика	Light S.A.	light.com.br	Бразилия
06.07.2020	Ragnar	Энергетика	Energias de Portugal	edp.com	Португалия
24.07.2020	NetWalker	Горное дело и нефтегазодобыча	Axens	axens.net	Франция

11

АТАК

на компании топливно-энергетического комплекса зафиксировано за год

8

СЕМЕЙСТВ

шифровальщиков использовались для реализации атак, что показывает отсутствие отраслевой специализации

УГРОЗЫ ДЛЯ БАНКОВСКОГО СЕКТОРА

Смена приоритетов на шифровальщики

Злоумышленники выбирают простые и прибыльные пути

Слабо защищенные и небольшие банки

пока еще подвергаются успешным атакам для целевого хищения средств

Утечки, в том числе истории транзакций,

могут стать проблемой отрасли, наравне с шифровальщиками

Эпоха целенаправленных атак на банки с целью хищения средств закончилась. В прошлом отчете мы писали о пяти активных группах: Cobalt, MoneyTaker, Silence, SilentCards и Lazarus, которые успешно совершали хищения через SWIFT, ATM Switch, карточный процессинг или банкоматы. В 2020 году хищения практически прекратились.

Последние хищения

Хищения через систему SWIFT

Опыт хищения через SWIFT был только у групп Lazarus и Cobalt, и последняя публичная успешная атака состоялась в феврале 2019 года на мальтийский банк Valletta.

Однако, самое интересное всегда остается за кадром, и попытки хищений не остановились. За последний год инциденты фиксировались в нескольких странах (Аргентина, Индия, Кения, Гана, Иордания) ежеквартально, но не все операции завершались для атакующих успехом. Были активны, как минимум, две группы:

Группа NanoSwift

Известно как минимум об одном инциденте, связанном с этой группой. Для начального доступа злоумышленники использовали легитимный инструмент удаленного доступа RMS, для установки которого использовался VBS скрипт:

install.vbs
c719a030434d3fa96d62868f27e904a6
f2f750a752dd1fda8915a47b082af7cf2d3e3655
2696ee4302a85c6b4101fc6d1ce8e38b94fd9c2bbd1acc73b553576b3aacb92f

Этот скрипт применяется уже давно и впервые был загружен на VirusTotal 8 октября 2018 года.

Для дальнейшей работы атакующие использовали хорошо известный троян NanoCore, который сохранялся в системе с именем lanss.exe в каталоге \LAN Subsystem\lanss.exe, что является стандартным индикатором NanoCore, известным с 2018 года.

Для повышения привилегий использовались следующие средства:

Инструмент	Описание
Invoke-MS16135.ps1	Эксплойты для повышения привилегий, входящих в состав PowerShell Empire
Invoke-MS16032.ps1	
RoguePotato.zip	Инструменты для запуска программ с правами SYSTEM
SysExec.exe	
cve-2020-0796-local.zip	Эксплойт CoronaBlue
Hooker_3.4.zip	Кейлоггер Hooker от Den4b
rkfree_setup_2.26_password_123.exe	Кейлоггер Revealer

Все это указывает на то, что у атакующих очень старый инструментарий, и его использование может быть эффективным только в случае атак на банки с минимальным уровнем безопасности либо если были грамотно расставлены ловушки для тех, кто занимался реагированием.

Тем не менее интерес представляет использование CVE-2020-0796, которая была обнародована в марте 2020 года, тогда же стал доступен первый эксплойт. Однако файл с именем cve-2020-0796-local.zip был опубликован на Github 3 апреля. Это позволяет предположить, что инцидент произошел в интервале с апреля по июль 2020 года.

Группа Lazarus

Lazarus атакует в основном небольшие банки, которые являются более легкой целью.

В 2020 году стало известно, что эта группа покупает загрузки (установки троянов под заказ) у операторов бот-сети TrickBot. Поэтому в нескольких инцидентах было отмечено, что троян TrickBot загружал в память вредоносный код группы Lazarus, скачанный с внешних серверов. В атаках были зафиксированы два домена, используемые группой Lazarus, с которых загружался вредоносный код:

— util98[.]com, зарегистрирован 24 апреля 2019 года
— startmary[.]com, зарегистрирован 13 января 2020 года

Судя по датам регистрации доменов, компрометация организаций произошла в апреле 2019 и в январе 2020 года соответственно, но попытки хищений проводились на 1–2 месяца позже.

Карточный процессинг

Ранее атаки на карточный процессинг осуществляли Cobalt, MoneyTaker, Silence, последние провели успешную операцию данного типа в первой половине 2019 года.

В сентябре 2020 филиппинский банк United Coconut Planters Bank (UCPB), контролируемый государством, был ограблен. В сообщениях упоминалось, что атакующим удалось увеличить лимиты на снятие средств в банкоматах с 20 тыс. до 10 млн песо в день.

Также стало известно, что злоумышленники перевели деньги из банка, используя локальную систему быстрых переводов InstaPay. В итоге им удалось вывести 167 млн песо ($3,44 млн).

В результате расследования были задержаны четверо нигерийцев.

ATM Switch

Единственной группой, которая использовала доступ к ATM Switch, является Lazarus. В августе 2020 года US-CERT выпустил оповещение об активизации этой группы и о том, что в их распоряжении появился вредоносный код, с помощью которого можно совершать хищения через ATM Switch под управлением ОС Windows. Ранее такой код был обнаружен только под ОС AIX. Но, несмотря на это оповещение, последнее успешное хищение было зафиксировано в 2018 году.

ATM

Троянами для банкоматов обладают практически все группы — Cobalt, MoneyTaker, Silence и Lazarus, но активно они не используется.

В сентябре 2019 года исследователи описали троян Dtrack, используемый Lazarus и обнаруженный еще в 2018 году. С того момента не было новых хищений с его применением.

Во второй половине 2019 года атаки на банки проводила только группа Silence. Они успешно проникли в несколько банков Чили, Коста-Рики и Болгарии, но злоумышленников удалось остановить на раннем этапе.

В ноябре 2019 на VirusTotal были загружены два файла: xfs.dll и dns.dll. Загрузка осуществлялась из Республики Сенегал. Файл xfs.dll был скомпилирован 19 октября 2019 года. Вероятно, именно в этот день была проведена атака на банкоматы, и это свидетельство последней подобной успешной атаки группы Silence. Основным трояном группы на тот момент был XDA.RAT.

Исходный код XDA.RAT основан на проекте с открытым исходным кодом: https://github.com/iagox86/dnscat2. Приложение может обрабатывать следующие команды:

- 0 - ping-команда
- 1 - создать cmd.exe процесс
- 2 - исполнить shell-команду
- 3 - загрузить файл
- 4 - выгрузить файл с зараженного устройства на управляющий сервер
- 5 - закрыть все соединения
- 6 - изменить период обращения к серверу
- 7 - сохранить %LOCALAPPDATA%\updatea.bin файл
- 8 - перезаписать <%XDA_path%>\updatea2.bin файл
- 9 - получить информацию о подключенном диспенсере
- 10 - провести атаку ATM jackpotting

Важно отметить, что функциональные возможности работы с ATM были заимствованы из ранее описанного нами в отчете о Silence вредоносе xfs-disp.exe. Таким образом, исходный код XDA.RAT основан на двух проектах: dnscat2 и xfs-disp.exe.

При получении команды 9 приложение собирает информацию аналогично xfs-disp.exe:

1. Пытается подключиться к сервис-провайдеру диспенсера:

- CashDispenser (Nautilus)
- NXCdm (Nautilus)
- DBD_AdvFuncDisp (Diabold)
- CurrencyDispenser1 (NCR)
- CDM30 (WINCOR)
- GEN (WINCOR GEN)
- ATM (GENERIC)

2. Логирует максимальное количество банкнот, которые могут быть выданы пользователю за одну операцию (используя WFS_INF_CDM_CAPABILITIES).

3. Логирует текущее состояние диспенсера (подключен и занят ли он), состояние дверцы диспенсера, состояние логических cash units, состояние задвижки и т. д. Формат:

```
state=%d, safedoor=%d, dispenser=%d, stacker=%d
pos=%d, OutputPosition=%d, shutter=%d, transport=%d
...
pos=%d, OutputPosition=%d, shutter=%d, transport=%d
```

4. Логирует информацию о кассетах и банкнотах в них. Формат:

```
Id:%s(nr=%d)(l=%d,h=%d), %d|%d|%d of %d [%s][%d][%d],[%d][%d]
...
Id:%s(nr=%d)(l=%d,h=%d), %d|%d|%d of %d [%s][%d][%d],[%d][%d]
```

Вместе с командой 10 приложение получает три параметра:

- Флаг:
  - 0 - XDA.Launcher выдаст пользователю определенное количество денег из определенной кассеты.
  - 1 - XDA.Launcher выдаст пользователю все деньги.
- Целочисленное значение — индекс кассеты.
- Целочисленное значение — количество наличности, которое необходимо выдать пользователю.

Приложение выполняет атаку ATM jackpotting аналогично xfs-disp.exe. Единственное отличие — оно может выдать определенное количество денег из определенной кассеты по команде сервера.

Смена приоритетов

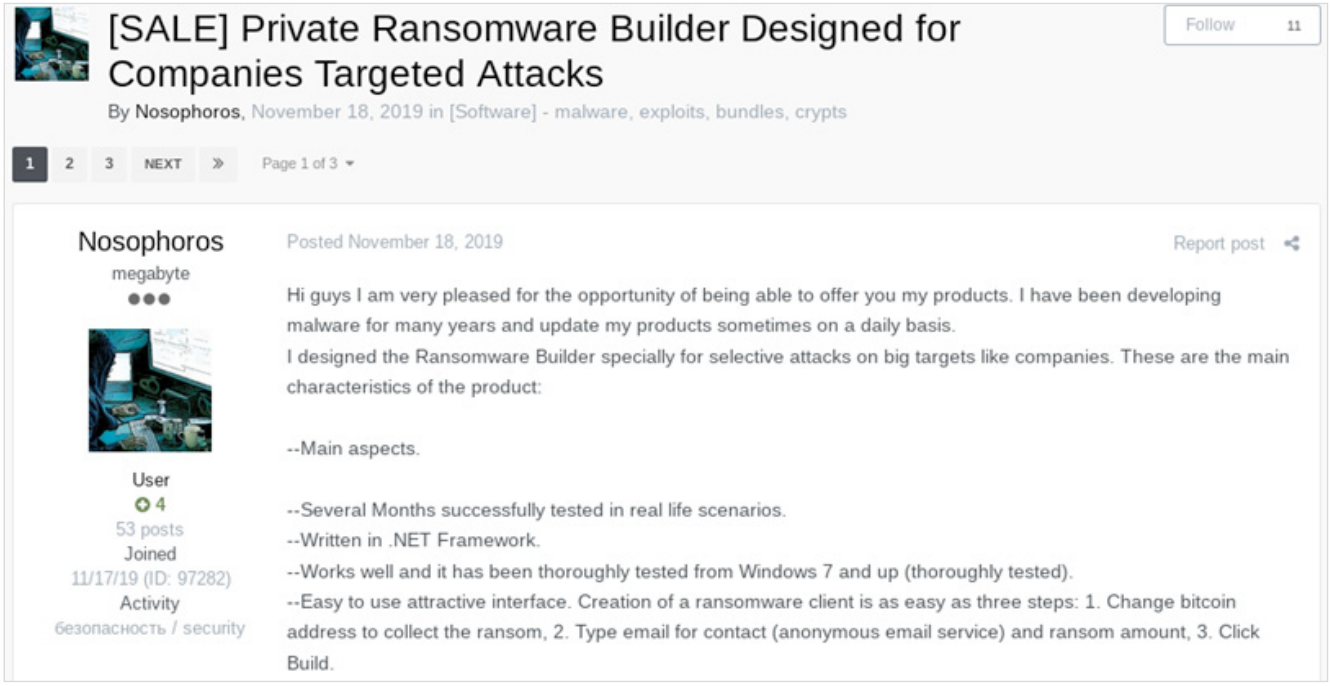
Основной проблемой для атакующих банки является не получение доступа, а финальная стадия — вывод и отмывание похищенных средств. Если у злоумышленников появляется возможность зарабатывать столько же, но при этом меньше привлекать внимание правоохранительных органов и иметь более гарантированный способ получения денежных средств, то они меняют свой фокус.

Так случилось и с группами Cobalt и Silence.

Мы по-прежнему видим уникальный вредоносный код, используемый обеими группировками, но при этом хищения не происходят.

Предположительно, группа Cobalt или ее часть стали участниками приватной партнерской программы с шифровальщиками Thanos. Об этом свидетельствует использование уникального упаковщика для шифровальщика Thanos, который применялся группой для своего трояна CobInt.

Группа Silence тоже не остановилась в 2020 году, и мы обнаруживали новые серверы управления, используемые в атаках на нетипичные для них цели — медицинские и промышленные предприятия Западной Европы.


[SALE] Private Ransomware Builder Designed for Companies Targeted Attacks

Follow 11

By Nosophoros, November 18, 2019 in [Software] - malware, exploits, bundles, crypts

1 2 3 NEXT » Page 1 of 3

Nosophoros
megabyte

User
4
53 posts
Joined
11/17/19 (ID: 97282)
Activity
безопасность / security

Posted November 18, 2019

Report post

Hi guys I am very pleased for the opportunity of being able to offer you my products. I have been developing malware for many years and update my products sometimes on a daily basis.
I designed the Ransomware Builder specially for selective attacks on big targets like companies. These are the main characteristics of the product:

--Main aspects.

--Several Months successfully tested in real life scenarios.
--Written in .NET Framework.
--Works well and it has been thoroughly tested from Windows 7 and up (thoroughly tested).
--Easy to use attractive interface. Creation of a ransomware client is as easy as three steps: 1. Change bitcoin address to collect the ransom, 2. Type email for contact (anonymous email service) and ransom amount, 3. Click Build.

Рисунок 9 — Объявление о продаже конструктора шифровальщиков

УГРОЗЫ ДЛЯ РЕТЕЙЛА

В 2,5 раза

увеличилось количество JS-снифферов

63,7 млн дампов банковских карт,

полученных через POS-трояны, были выставлены на продажу

92% дампов карт

приходится на долю США, затем идут Индия и Южная Корея

Для ретейла можно выделить четыре основные угрозы, которые могут привести к потерям для бизнеса:

— атаки с помощью JS-снифферов;
— атаки на POS-терминалы;
— использование скомпрометированных данных (credential stuffing);
— атаки с помощью шифровальщиков.

Атаки с использованием шифровальщиков понятны, и, как правило, компании о них хорошо осведомлены, поэтому более подробно мы расскажем о первых трех угрозах, лежащих в основе рынка кардинга и массового мошенничества.

Общие тенденции в кардинге

Рынок кардеров можно поделить на два основных сегмента: продажа текстовых данных о картах (номер, дата истечения, имя держателя, адрес, CVV) и дампов (содержимое магнитных полос карт).

Текстовые данные собираются с помощью фишинговых сайтов, банковских троянов для ПК, Android и банкоматов, а также в результате взломов сайтов электронной коммерции и использования JS-сниффероов. Именно JS-сниффероы стали основной новинкой этого года, и заметен тренд на все большую их популяризацию.

Дампы получают через скимминговые устройства, а также с использованием троянов для компьютеров с подключенными POS-терминалами.

Общий рынок кардинга вырос с $880 млн до $1,9 млрд по сравнению с прошлым годом. Двойной рост касается как текстовых данных, так и дампов. Количество предлагаемых к продаже текстовых данных выросло с 12,5 до 28,3 млн карт, а дампов — с 41 до 63,7 млн.

Атаки с помощью JS-снифферов

За прошедший год увеличилось количество атак на сайты онлайн-магазинов, так как использование JavaScript-снифферов для кражи банковских карт стало одним из основных способов получения больших объемов платежной информации. На их рост также повлиял тренд на перепродажу доступов к различным сайтам и организациям на подпольных форумах.

Наиболее популярные семейства JS-снифферов

Всего на данный момент специалистами Group-IB отслеживается 96 семейств JavaScript-снифферов, и каждое из них достойно детального изучения. Например, в прошлом году было известно только о 38 семействах.

Всего, по данным Group-IB, за прошедший год было обнаружено почти 460 тыс. банковских карт, скомпрометированных при помощи JavaScript-снифферов. Дополнительно еще 645 тыс. карт были выставлены на продажу на одном из кардшопов на общую сумму $3,6 млн.

Топ-9 банков, выпустивших украденные карты, находятся в США, на их долю пришлось 170 тыс. карт. Помимо американских эмитентов, злоумышленников также интересуют карты, выпущенные в Бразилии, Австралии, Канаде, Испании, Великобритании, Индии, Сингапуре и Франции.

Семейство снифферов	Стоимость	Количество украденных банковских карт
Inter Разработано пользователем подпольных форумов под псевдонимом Sochi (разработчик Android-трояна Red Alert)	$990	—
CoffeMokko Является собственной разработкой использующей его преступной группы. Для монетизации украденных данных преступники создали магазин по продаже карт.	N/A	180 тыс.
ImageId Было разработано пользователем подпольных форумов под ником poter, который продавал свое решение с 2017 года. На сегодняшний день продажи данного сниффера закрыты. Одна преступная группа использует его модифицированную версию.	$5 тыс.	22 тыс.

Lazarus, JS-снифферы и хищение Bitcoin

В июле 2020 года специалистами по информационной безопасности была опубликована информация о том, что прогосударственная APT-группа Lazarus использовала JS-снифферы для кражи банковских карт из 25 онлайн-магазинов, работающих по всему миру.

Специалисты обнаружили две кампании, в ходе которых использовалась инфраструктура, ранее замеченная в атаках, приписываемых северокорейским хакерам.

Первая кампания стартовала в мае 2019 года. Атакующие использовали семейство снифферов ClientToken и заразили 20 онлайн-магазинов.

Вторая кампания началась в феврале-марте 2020 года и была нацелена на крупные магазины. Всего было подтверждено три заражения сайтов снифферoм Preloader. Специалисты Group-IB также обнаружили еще два сайта для сбора украденных карт в ходе кампании Preloader, что может свидетельствовать о большем количестве жертв.

Также, была выявлена кампания BTC Changer, в процессе которой модифицированная версия сниффера ClientToken использовалась для подмены адреса Bitcoin-кошелька в момент платежа на сайтах магазинов, принимающих Bitcoin. Всего было обнаружено два сайта, зараженных в ходе этой кампании, что принесло атакующим 0,66983720 BTC (примерно $7800).

Продажа доступов к онлайн-магазинам

Доступ к взломанному онлайн-магазину для последующей установки сниффера может быть куплен на подпольных форумах. Цена на такой товар сильно зависит от страны, в которой работает магазин, от количества покупателей в сутки, а также от типа оплаты, установленной на сайте. Если платеж происходит в отдельном окне, открытом в iframe, или после перенаправления на сайт платежной системы, то на таком сайте сложнее настроить сниффер. Потому такие лоты будут стоить дешевле, чем те сайты, на которых данные карты вводятся на самом ресурсе.

Для получения доступа к магазину или для установки сниффера злоумышленники по-прежнему используют известные уязвимости в популярных eCommerce CMS, а также вредоносное программное обеспечение для кражи паролей и брутфорс-атаки на административные панели управления магазинами или СУБД.

К примеру, по-прежнему остаются актуальными атаки с использованием вредоносного ПО GoBrut: это программное обеспечение, написанное на Golang, используется для распределенных брутфорс-атак на сайты онлайн-магазинов и административные панели CMS Magento, OpenCart, phpMyAdmin и cPanel. В дальнейшем доступ к административной панели и инструменту администрирования может быть использован для установки JS-сниффера на сайт.

Способы избежать обнаружения

Чтобы избежать обнаружения и удаления вредоносного кода с сайта, злоумышленники используют несколько техник:

— в основе большинства из них лежит использование JavaScript-скриптов для подгрузки основного кода сниффера в момент, когда пользователь находится на странице оплаты. Ранее они зачастую просто подгружались по ссылке при помощи тега script;
— другой техникой является популярное в последнее время сокрытие кода JS-сниффера внутри настоящего изображения. Код инжектора скачивает картинку с сервера злоумышленников, извлекает код сниффера и исполняет его на странице онлайн-магазина;
— злоумышленники по-прежнему используют код для обнаружения открытой консоли браузера, чтобы не привлекать внимание исследователей и средств защиты. Вредоносный код не запускается и не выполняет основную нагрузку, если обнаружено, что в браузере посетителя сайта открыта консоль разработчика;
— также некоторые семейства JavaScript-снифферов используют несколько различных проверок, за которые отвечает серверная часть сниффера, чтобы избежать обнаружения: основной код JS-сниффера будет получен только тогда, когда IP-адрес пользователя не принадлежит сетям крупных облачных провайдеров, страна пользователя, определяемая по IP-адресу, соответствует стране

магазина, а в поле Referer указан адрес страницы оплаты зараженного магазина. Если хотя бы одна из этих проверок завершилась неудачей, в ответ на запрос кода сниффера вернется абсолютно безвредный JavaScript-скрипт легитимной библиотеки;

— загрузка основного кода сниффера с использованием JavaScript предоставила злоумышленникам возможности сокрытия адреса, с которого будет загружаться этот код. Самые простые семплы кода используют Base64 для сокрытия ссылки на вредоносный JS-файл, но зачастую можно встретить образцы вредоносного кода, в которых ссылка на сниффер хранится в зашифрованном виде, а также в виде конкатенации частей URL-адреса или строки с обратным порядком символов;

— также были обнаружены семплы вредоносного кода, которые использовали алгоритм генерации доменов (DGA) для получения адреса сайта, с которого необходимо скачать основной код сниффера. Актуальный адрес зависел от даты, в частности злоумышленники создавали по одному домену на каждый месяц, а в случае блокировки одного из доменов достаточно было подождать некоторое время — и поток банковских карт с сайта зараженного магазина возобновлялся.

Атаки на POS-терминалы

Основным товаром у кардеров являются именно дампы банковских карт. Всего были обнаружены 63,7 млн дампов, выставленных на продажу, что на 156% больше, чем в прошлом году.

Основной целью мошенников являются банковские карты, выпущенные банками США, на их долю приходится более 92% всех дампов карт, затем идут Индия и Южная Корея.

Основным способом компрометации данных магнитной полосы является заражение компьютеров с подключенными POS-терминалами специальными троянами, собирающими данные из оперативной памяти. За отчетный период была выявлена активность 14 троянов:

— RtPOS
— TinyPOS
— UdPOS
— FighterPOS
— DiamondFox
— GratefulPOS
— FrameworkPOS
— MajikPOS
— DMSniff
— PinkKite
— BADHATCH
— Pillowmint
— GlitchPOS
— Alina POS

Страна	Количество дампов за H2 2019 — H1 2020	Процент	Количество дампов за H2 2018 — H1 2019	Разница 2020 vs 2019
США	58 921 367	92,37%	39 895 064	1,48
Индия	1 723 722	2,70%	17 246	99,95
Южная Корея	644 672	1,01%	77 573	8,31
Соединенное Королевство	584 519	0,92%	466 296	1,25
Канада	565 535	0,89%	198 741	2,85
Бразилия	447 412	0,70%	168 294	2,66
Мексика	276 935	0,43%	43 832	6,32
Франция	234 076	0,37%	53 804	4,35
ОАЭ	208 089	0,33%	82 446	2,52
Австралия	182 263	0,29%	41 288	4,41

58 921 367
ДАМПОВ БАНКОВСКИХ КАРТ,

выпущенных в США, продавались в H2 2019 — H1 2020

Дата	Скомпрометированная компания	Название базы данных в кардшопе	Количество карт
Июль 2019	Deer Valley Resort	—	—
Август 2019	Hy-Vee (Hy-Vee Market Grilles, Market Grille Expresses and Wahlburgers)	SOLAR ENERGY	3188056
Август 2019	Russell Stover's retail stores	—	—
Сентябрь 2019	Krystal, Moe's, McAlister's Deli and Schlotzsky's	NEW WORLD ORDER	3419867
Ноябрь 2019	North american fuel dispenser merchants (visa report)	—	—
Ноябрь 2019	Church's Chicken	—	—
Ноябрь 2019	Catch	—	—
Ноябрь 2019	on the Border	—	—
Декабрь 2019	Noth american fuel dispenser merchants (visa report)	—	—
Декабрь 2019	WAWA	BIGBADABOOM-III	15065318
Декабрь 2019	Islands Restaurants	—	—
Декабрь 2019	Champagne French Bakery Cafe	—	—
Январь 2020	Landry's	—	—
Январь 2020	The crack shack	—	—
Февраль 2020	—	NIRVANA BREACH	1049577
Февраль 2020	Rutter's	—	—
Февраль 2020	Quaker Steak & Lube	—	—
Март 2020	Key Food	—	—
Апрель 2020	Main Event	—	—

19
СЛУЧАЕВ КОМПРОМЕТАЦИИ,

в результате которых были выставлены на продажу миллионы банковских карт удалось выявить за год

15 065 318

карт похищено у компании WAWA

Несмотря на то что сервисов по продаже дампов банковских карт (кард-шопов) много, наиболее крупные базы выставлялись на двух хорошо известных ресурсах — Joker's Stash и Trump's Dumps. Эти всплески наглядно демонстрируют, что реальное количество скомпрометированных ретейл-сетей значительно больше:

Дата	Кол-во дампов	Название базы	Кардшоп	Кол-во дампов в указанной базе	Распределение по странам в базе	Стоимость целой базы
2019-08-02	471540	GOOD-KARMA-DISCOUNT-SALE	Joker's Stash	320518	USA (99,7%)	$961 554,00
2019-08-20	689382	SUNRISE-01-US (SOLAR ENERGY BREACH)	Joker's Stash	481071	USA (99,7%)	$12 099 755,00
2019-08-20	689382	SUNRISE-01-EU (SOLAR ENERGY BREACH)	Joker's Stash	203875	Lebanon (26,8%), France(9,08%), Brazil (8,72%) and other EU countries	$40 114 790,00
2019-10-28	1727559	INDIA-MIX-NEW-01	Joker's Stash	1333266	India (98%)	$133 326 600,00
2019-11-22	921549	NEW-WORLD-ORDER-01-US (NWO BREACH)	Joker's Stash	225242	USA (100%)	$4 541 410,00
2019-11-22	921549	NEW-WORLD-ORDER-02-US (NWO BREACH)	Joker's Stash	485113	USA (100%)	$9 517 595,00
2020-01-27	3845727	BIGBADABOOM-III-US-part1 (BBB3 BREACH)	Joker's Stash	974877	USA (99,9%)	$20 415 497,00
2020-01-27	3845727	BIGBADABOOM-III-US-part2 (BBB3 BREACH)	Joker's Stash	974829	USA (99,9%)	$20 408 637,00
2020-01-27	3845727	BIGBADABOOM-III-US-part3 (BBB3 BREACH)	Joker's Stash	1237912	USA (99,9%)	$25 922 342,00
2020-01-27	3845727	BIGBADABOOM-III-EU-part1 (BBB3 BREACH)	Joker's Stash	381940	UK (21,8%), Australia (16,8%), Puerto Rico (16,3%) and other EU countries	$74 813 895,00
2020-03-06	598510	BIGBADABOOM-III-US-part19 (BBB3 BREACH)	Joker's Stash	186074	USA (99,9%)	$3 895 216,00
2020-03-06	598510	DWELL-DISCOUNT-SALE	Joker's Stash	136270	USA (94,2%), Korea (4,29%)	$681 350,00
2020-03-06	598510	06.03_USA_ASIA_PIN_DISCOUNT	Trump's Dumps	66929	Hong Kong (39,3%), China (26,3%), Taiwan (13,4%)	$996 435,00
2020-03-23	564950	AURIFEROUS-DISCOUNT-SALE-5USD	Joker's Stash	292121	USA (98,5%)	$1 460 605,00
2020-03-23	564950	BIGBADABOOM-III-US-part25 (BBB3 BREACH)	Joker's Stash	189945	USA (100%)	$3 973 479,00
2020-04-09	531978	SCARFACE-DISCOUNT-SALE-5USD	Joker's Stash	397465	Korea (49,9%), USA (49,3%)	$1 987 325,00
2020-04-12	461865	12.04_USA	Trump's Dumps	431542	USA (74,5%), Korea (22%)	$3 590 317,00
2020-04-25	455377	CONSERVATIVE-DISCOUNT-SALE-5USD	Joker's Stash	382643	USA (77,4%), Korea (21%)	$1 913 215,00
2020-04-29	1061346	STOCK-DISCOUNT-SALE-5USD	Joker's Stash	281652	USA (98,8%)	$1 408 260,00
2020-04-29	1061346	29.04_USA	Trump's Dumps	223864	USA (98,9%)	$1 953 469,50
2020-04-29	1061346	BIGBADABOOM-III-US-part35 (BBB3 BREACH)	Joker's Stash	186883	USA (99,9%)	$3 915 851,00
2020-04-30	526638	30.04_USA	Trump's Dumps	389592	USA (78,4%), Korea (18,2%)	$3 264 337,00
2020-05-01	610381	IRONY-DISCOUNT-SALE-5USD	Joker's Stash	365602	USA (88,9%), UAE (9%)	$1 828 010,00
2020-05-11	1007295	ZONDER-DISCOUNT-SALE-3USD	Joker's Stash	613333	USA (98,6%)	$1 839 999,00
2020-05-12	691320	12.05_US_AE	Trump's Dumps	370549	USA (88,8%), UAE (8,33%)	$2 953 153,25
2020-06-11	672373	12.06_US_AE	Trump's Dumps	344273	USA (91,5%), UAE (5,8%)	$3 258 824,00
2020-06-22	504060	19.06_USA_ZIP_PIN_DISCOUNT	Trump's Dumps	257547	USA (56,6%), UAE (10,1%)	$3 863 205,00
2020-06-22	504060	BIGBADABOOM-III-US-part53 (BBB3 BREACH)	Joker's Stash	181718	USA (99,9%)	$3 792 718,00
2020-06-29	566534	XXXBBB-DISCOUNT-SALE-1USD	Joker's Stash	229644	USA (99,9%)	$229 644,00
2020-06-29	566534	BIGBADABOOM-III-US-part56 (BBB3 BREACH)	Joker's Stash	181549	USA (99,9%)	$3 789 953,00
ВСЕГО						$352 602 650

Использование скомпрометированных данных (credential stuffing)

Пожалуй, одной из самых распространенных проблем является техника credential stuffing — извлечение из различных утечек известных пар логин-пароль (под логином могут выступать email, телефон и другие идентификационные данные) для последующего брутфорса (перебора) аккаунтов на разных онлайн-ресурсах.

Дело в том, что многие пользователи используют одинаковые пароли на различных сайтах, и в случае компрометации одного ресурса существует вероятность того, что те же аутентификационные данные были использованы и на других. Стоит также отметить, что на данный момент практически все крупные утечки появляются изначально в продаже, а затем в публичном доступе на андерграундных форумах, что позволяет злоумышленникам достаточно легко собирать базы для credential-stuffing-атак. Это касается всех ретейлеров с личными кабинетами на онлайн-ресурсах, а также некоторых банковских аккаунтов и электронных кошельков.

Виды монетизации

Получение доступа к банковским аккаунтам и электронным кошелькам

Одной из самых очевидных целей злоумышленников являются банковские аккаунты и электронные кошельки, т. е. те онлайн-ресурсы, которые напрямую дают доступ к денежным средствам жертвы. Некоторые банки предоставляют доступ в интернет-банкинг с использованием пары email:пароль или телефон:пароль, что делает их целями подобных атак.

Стоит отметить, что напрямую вывести денежные средства с банковских счетов достаточно сложно для злоумышленников, так как обычно такие операции требуют подтверждения (двухфакторной аутентификации) от пользователя аккаунта, поэтому данный способ монетизации не является основным.

Однако в электронных кошельках не используются настолько сложные меры защиты, как в банковских аккаунтах. Таким образом, получив к ним доступ, злоумышленники пытаются либо совершить покупки за счет жертвы, либо вывести денежные средства на другой кошелек, зарегистрированный на дропа, посредством различных обменных сервисов.

Монетизация бонусных баллов

Онлайн- и офлайн-ретейлеры часто предлагают участникам своих программ лояльности кешбэк за покупки в виде бонусных баллов или денег. Как правило, такими бонусными баллами можно оплатить только часть покупки, но в некоторых случаях возможна оплата и всего чека.

— Популярный вариант вывода бонусных баллов — покупка товаров для последующей перепродажи. Злоумышленники могут купить карты предоплаты для магазинов, продающих цифровой контент (например, PlayStation Store, Xbox Store и др.). Такую карту злоумышленники перепродают или используют для оплаты в магазинах.
— Если злоумышленники получили доступ ко многим аккаунтам пользователей, они могут консолидировать бонусные баллы и оплатить ими большое количество покупок и/или купить более дорогие товары.
— В некоторых ретейл-сетях возможна оплата бонусными баллами на кассе офлайн-магазина. В таком случае злоумышленники могут использовать виртуальные карты лояльности, штрихкоды или купоны на скидку из личного кабинета пользователя для списания бонусных баллов и оплаты покупок.

Списание средств на платные услуги

Некоторые ретейлеры предлагают пользователям услуги, которые оплачиваются через пополнение личного счета на сайте.

Если злоумышленники получают доступ к аккаунту пользователя, у которого на личном счете положительный баланс, они могут использовать эти средства, чтобы получить платные услуги ретейлера для собственной выгоды. В некоторых случаях злоумышленники продают доступ к таким аккаунтам.

Получение подарочных баллов или товаров

Ретейлеры предлагают пользователям бонусы и подарки за переход на более высокий уровень обслуживания или более дорогой тариф.

Злоумышленники могут воспользоваться доступом к аккаунту пользователя и самостоятельно перевести его на другой уровень обслуживания, чтобы получить вознаграждение, которое впоследствии перепродается.

Доступ к персональным данным

В личном кабинете пользователя на сайте ретейлера злоумышленники могут получить доступ к персональным данным:

— ФИО,
— контактные данные (номер телефона, почта, адреса доставки),
— данные о способах оплаты (номера банковских карт и/или счетов, учетные записи платежных систем)

Если эта информация слабо защищена, злоумышленники могут выгрузить и использовать ее для мошенничества с применением социальной инженерии либо перепродать другим заинтересованным лицам.

Способы реализации атаки

Для проведения такой активности нужны:

— списки логин:пароль из различных утечек;
— списки прокси-серверов для обхода блокировок по количеству запросов с одного IP-адреса;
— программа, которая получает на вход списки логинов, прокси и адрес ресурса, на котором будет проверяться существование пользователя с таким логином и паролем.

Наибольший интерес представляют инструменты, используемые для проведения таких атак, которые можно разделить на три основные категории:

— боты без браузеров;
— браузерные боты;
— гибридные решения.

Боты без браузеров

Это самый примитивный вид реализации подобных инструментов. Они очень просты, работают надежно и быстро, но при этом не способны эффективно обходить решения по защите от ботов.

На рынке существует множество предложений с готовыми решениями, но широкое распространение получил OpenBullet — инструмент с открытым исходным кодом. Его основным плюсом является простая расширяемость. Под каждый онлайн-ресурс, на котором надо проводить проверку существования пользователя, нужно адаптировать код. В OpenBullet, как и во многих других инструментах, такая адаптация реализована конфигурационными файлами. Таким образом, множество пользователей пишут конфигурационные файлы под разные ресурсы, и наиболее крупные из них уже давно в списке.

Отличительной особенностью платных ресурсов является более комплексное предложение. Авторы этих инструментов добавляют постоянно пополняемые списки прокси, пишут парсеры логов для извлечения контактной и платежной информации из личных кабинетов.

Поскольку такая атака проста в реализации, некоторые мошенники предпочитают писать свои скрипты для ее реализации на конкретных ресурсах.

Гибридные решения

Поскольку боты без браузеров не могут решать CAPTCHA и получать cookie-файлы, то мошенники пришли к гибридному решению.

Они автоматически или в ручном режиме запускают браузер и получают файлы cookie. Далее эти файлы добавляются в конфигурационный файл ботов и уже без необходимости запуска браузера осуществляется проверка логинов и паролей. Такая схема тоже проста в реализации, а главное — работает быстро и не требует множества вычислительных ресурсов.

Для того чтобы обходить различные виды CAPTCHA, есть как отдельные инструменты, решающие ее простые варианты, так и специальные SaaS-сервисы. В последнем случае мошенники автоматически передают ссылку в сервис через API и в ответ получают cookie-файлы или решение.

Такие гибридные методы позволяют обойти почти все решения по борьбе с ботами.

Браузерные боты

Ресурсы с надежной защитой встречаются редко. Как правило, это крупные социальные сети или ИТ-гиганты, которые используют свои решения по противодействию ботам. В этом случае мошенники пишут уникальные браузерные боты под каждый ресурс.

Они представляют из себя полноценный браузер, который автоматически запускается, осуществляет открытие страницы, инициирует скрипты, эмулирует поведение пользователя на сайте.

В отличие от предыдущих схем, такая реализация значительно дороже. Она требует значительной кастомизации, а запуск множества браузеров требует больше серверных мощностей, и главное — это работает значительно медленнее.

БАНКОВСКИЕ ТРОЯНЫ

Латинская Америка

остается основным регионом роста этого вида угроз

12 из 19 банковских троянов

разработаны русскоговорящими авторами

Переход на шифровальщики

владельцы банковских бот-сетей следуют популярному тренду

Каждый год несколько банковских бот-сетей уходит с рынка, и их место практически никто не занимает. Этот год не стал исключением. Такими темпами рынок банковских троянов может исчезнуть через 3–5 лет.

Трояны для ПК

Всего в этом году активность проявляли 19 банковских троянов, 12 из которых разработаны русскоговорящими авторами, шесть — авторами из Латинской Америки.

Русскоговорящие владельцы крупнейших банковских бот-сетей тоже следуют основному тренду и переключаются на использование шифровальщиков, например:

— Trickbot использует шифровальщики Ryuk (позже Conti), Kraken, Thanos;
— Dridex использует WastedLocker, DoppelPaymer, а ранее — BitPaymer, Locky, Bart, Jaff;
— Qbot (Quakbot) начал использовать шифровальщик ProLock.
— zLoader/Silent Night тоже переключились на использование пока неустановленной программы-вымогателя;
— RTM, единственная активная в России банковская бот-сеть, использует шифровальщик Cerber.

Смена фокуса не означает, что злоумышленники не совершают хищений: как только они видят возможность сделать перевод крупной суммы, они это возможностью пользуются. Но основной заработок поступает именно от программ-вымогателей.

Такое изменение поведения приводит к снижению ущерба от хищений и заставляет меняться рынок отмывания денежных средств.

Поскольку ранее самыми распространенными банковскими троянами были разработки русскоговорящих

Старые и активные	Guildma (Astaroth), Grandoreiro, Javali, Melcoz, CamuBot, Metamorfo, Qbot, Gootkit, Trickbot, Gozi (ISFB, Ursnif, Dreambot), IcedID (Bokbot), Ramnit, Backswap, Dridex, LokiPWS, Retefe, RTM, Danabot
Новые	zLoader/Silent Night
Исчезнувшие	TinyNuke (aka NukeBot), Panda Banker, Osiris, MnuBot

киберпреступников, то снижение активности хищений приводит к еще большей деградации этого сегмента. За анализируемый период появился только один новый банковский троян от русскоговорящих авторов — Silent Night. Он является усовершенствованной версией старого трояна Axebot и замечен в атаках на пользователей Германии. При этом за этот же период активность полностью прекратили еще три трояна, созданны ранее русскоязычными авторами: TinyNuke, Panda Banker, Osiris.

Россия

Единственным банковским трояном для ПК остался только RTM, который не показывает большой активности и в ближайшее время прекратит свое существование. Эта банковская бот-сеть использует шифровальщик Cerber.

Латинская Америка

Является единственной точкой роста банковских троянов. В 2020 году стало известно о пяти новых троянах: Guildma (Astaroth), Grandoreiro, Javali, Melcoz, Metamorfo, которые активны уже несколько лет, но внимание исследователей привлекли недавно.

Разработчики этих троянов находятся в Латинской Америке, и применяются они в этом же регионе, хотя некоторые из них начинают атаковать Европу и США.

США и Канада

Традиционно США и Канада являются основной целью для банковских троянов. Даже латиноамериканские разработчики добавили американские банки в свои конфигурационные файлы.

Сейчас угрозу для клиентов банков США и Канады представляют 11 троянов для ПК, десять из которых разработаны русскоговорящими хакерами: Metamorfo, zLoader/Silent Night, Gootkit, Trickbot, Gozi, IcedID, Danabot, Ramnit, Dridex, LokiPWS, Qbot.

Азиатско-Тихоокеанский регион

В Азиатско-Тихоокеанском регионе банковские трояны практически не претерпели значительных изменений. Атакуемыми странами являются Япония и Австралия, и для этого используются все те же трояны: Trickbot, Gozi, Danabot, Ramnit.

Трояны для Android

Рынок Android-троянов похож на рынок троянов для ПК. Основными разработчиками таких вредоносных программ являются русскоговорящие авторы, но на арену активно выходят разработчики из Латинской Америки, которые используют эти инструменты для атак на клиентов банков в своем регионе.

Всего в этом году была зафиксирована активность десяти банковских Android-троянов, пять из которых являются новыми.

Автор трояна Red Alert с псевдонимом Sochi прекратил разработку и переключился на работы с JS-снифферами.

Старые и активные	Anubis, Flexnet, Gustuff, BasBanke (Coybot), Cerberus
Новые	Ginp, Alien Bot, BlackRock, Hydra, EventBot
Исчезнувшие	Red Alert, Asacub

Авторы Android-троянов не очень разборчивы в именах. В 2020 году появился Alien Bot, однако трояны от других разработчиков, но с таким же именем, уже существовали ранее.

Android-трояны в основном используют веб-фейки — диалоговые окна, запрашивающие у жертвы необходимую информацию (пароли, номера банковских карт и т.п.). В русскоговорящем сегменте появились сервисы по их разработке. В результате авторам банковских троянов уже не нужно тратить время на поддержку работы с определенными приложением для сбора финансовой информации. Достаточно купить набор веб-фейков, и троян можно использовать практически в любом регионе, что и происходит с творениями русскоговорящих киберпреступников.

Россия

В России активность проявляли всего два Android-трояна: Flexnet и Anubis, но значительного ущерба они нанести не смогли. Flexnet распространялся более массово и смог заразить 50 тыс. устройств, перехватить чуть более 5 тыс. банковских карт.

Anubis распространялся более точечно, используя посадочные страницы, сделанные под бренд одного российского банка, и целенаправленно заразил около 400 клиентов.

Латинская Америка

Наибольшую активность в регионе проявляет троян, разработанный местными авторами, — BasBanke, работающий по партнерской схеме, когда его распространением могут заниматься сразу несколько человек.

США и Канада

Русскоязычные авторы придерживаются политики, что их Android-трояны не должны использоваться для атак на клиентов США, хотя авторы веб-фейков активно создают окна для сбора данных американских финансовых организаций.

Угрозу представляют только два трояна: новый Alien Bot и BlackRock.

Азиатско-Тихоокеанский регион

Угрозы для Азиатско-Тихоокеанского региона представляют все трояны, разработанные русскоговорящими разработчиками: Anubis, Gustuff, Cerberus и новый Alien Bot.

Трояны для ПК

	PT	CL	CA	BR	EC	DE	PE	FR	IT	ES	PL	AT	NL	AU	JP	NZ	GB	CH	US	NO	LI	LU	SE	MX
Латиноамериканские разработки																								
Guildma (Astaroth)	●			●																				
Grandoreiro	●			●		●	●			●							●							●
Javali				●																				●
Melcoz		●		●						●														●
CamuBot				●																				
Metamorfo		●	●	●	●					●									●					●
Русскоязычные разработки																								
zLoader/Silent Night			●			●											●		●					
Gootkit	●					●		●	●		●	●							●					
Trickbot			●			●				●	●			●	●		●		●					
Gozi (ISFB, Ursnif, Dreambot)			●			●			●		●			●		●			●					
IcedID (Bokbot)			●														●		●					
RTM*																								
Danabot						●			●		●	●		●										
Ramnit									●						●									
Dridex**																								
LokiPWS**																								
Retefe																		●		●	●	●	●	
Qbot													●						●					
Неизвестные разработки																								
Backswap										●														

Трояны для Android

	PT	CL	CA	BR	TR	DE	PE	FR	IT	ES	PL	AT	NL	AU	JP	IL	GB	CH	US	IN	MY	LU	TH	MX	CZ	HR	HU	BE	BG
Латиноамериканские разработки																													
BasBanke (Coybot)	●	●		●					●	●														●					
Русскоязычные разработки																													
Anubis**																													
Gustuff**																													
Cerberus**																													
Неизвестные разработки																													
Alien Bot			●		●	●	●	●	●	●			●	●	●	●	●		●	●	●	●	●		●				
Ginp										●	●						●												
BlackRock			●		●	●		●	●	●	●	●		●			●		●							●	●	●	●
Hydra																													
EventBot					●	●		●	●	●							●	●											

* Атаковала CIS
** Атаки по всему миру

ВЕБ-ФИШИНГ И СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

На 118% больше фишинг-ресурсов

выявлено и заблокировано в этом году по сравнению с прошлым

Ставки на спорт и онлайн-сервисы

быстро набирают популярность у создателей фишинговых страниц

Новые техники и инструменты

используются злоумышленниками, чтобы избежать обнаружения

В промежутке с II квартала 2019 года по II квартал 2020 года было выявлено и заблокировано на 118% больше фишинг-ресурсов, чем в предыдущем отчетном периоде.

Такой значительный рост объясняется двумя основными причинами:

— **Пандемия**. Во время самоизоляции у многих атакующих вынужденно появилось больше времени, которое они могут уделять вредоносной активности. Кроме того, фишинг как одна из наиболее простых схем заработка привлек внимание большей аудитории, лишившейся доходов.
С другой стороны, режим самоизоляции увеличил спрос на покупки через интернет. Люди начали все чаще заказывать товары и услуги удаленно, не выходя из дома.
Мошенники быстро подстроились под данный тренд и начали проводить фишинговые атаки на сервисы и отдельные бренды, которые ранее не имели для них особого экономического эффекта.

— **Смена тактики**. В предыдущие годы злоумышленники прекращали свои кампании после блокировки мошеннических веб-ресурсов и быстро переключались на другие бренды. Сегодня они автоматизируют атаку, выводя новые фишинговые единицы на смену заблокированным.

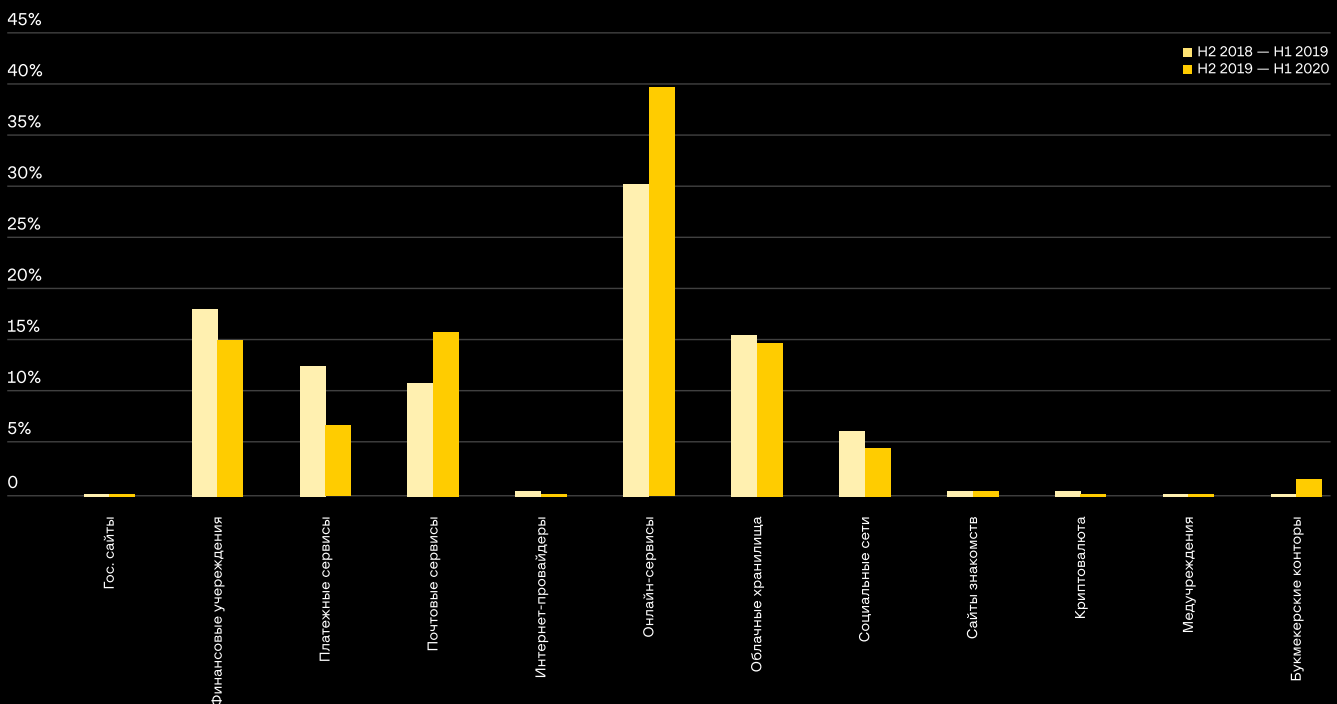
Во II квартале 2020 было замечено увеличение фишинга, нацеленного на букмекерские конторы, — 6% против 2% за предыдущий квартальный период. В рамках сравнения периода H2 2018 — H1 2019 с H2 2019 — H1 2020 рост фишинга, нацеленного на букмекерские конторы, составил больше 20%.

Почтовые сервисы и финансовые организации также остаются основными целями злоумышленников.

Еще одной категорией, показавшей значительный рост, стали онлайн-сервисы. Сюда входит фишинг для сбора учетных записей Microsoft, Netflix, Amazon, eBay, Valve Steam и т.п.

Практически исчезли фишинг-ресурсы, нацеленные на криптовалютные проекты. Основная причина кроется в угасании интереса к ICO-проектам, которые на протяжении 2017–2018 годов были популярны у фишеров.

Организации	H2 2018 — H1 2019	H2 2019 — H1 2020
Государственные сайты	0,3%	0,1%
Финансовые учреждения	18,3%	15,0%
Платежные сервисы	12,9%	6,6%
Почтовые сервисы	11,6%	15,6%
Интернет-провайдеры	1,6%	0,7%
Онлайн-сервисы	30,5%	39,6%
Облачные хранилища	15,8%	14,5%
Социальные сети	6,0%	4,5%
Сайты знакомств	1,4%	1,2%
Криптовалюта	1,5%	0,0%
Медучреждения	0,1%	0,0%
Букмекерские конторы	0,1%	2,2%



Защита фишинга от обнаружения

Трендом этого года стало использование одноразовых ссылок. Пользователь получает уникальную ссылку, которая становится неактивной после первого открытия. Это приводит к тому, что если кто-то перешел по ссылке хотя бы раз, то получить этот же контент повторно для сбора доказательной базы не получится. А без нее процесс блокировки фишингового ресурса значительно усложняется.

Общий обзор используемых фишерами защитных техник представлен ниже:

— **Одноразовые ссылки**. Генерация уникальной одноразовой ссылки для каждого пользователя.
— **Блокировка по подсетям**. Подсети многих компаний, оказывающих услуги обнаружения фишинговых страниц, уже находятся в черных списках, и если запрос на страницу приходит с их подсетей, то фишинговый контент отдаваться не будет.
— **Блокировка по User-agent**. Атакующие понимают, кто их основная аудитория, и если из User-agent понятно, что это не реальный пользователь, то фишинговый контент тоже не отдается. Например, атакующий проводит атаку на владельцев мобильных устройств, в таком случае все посетители с браузером для ПК не будут получать фишинговую страницу. Обычно в скриптах фишинговых наборов зашит список ключевых слов, которые проверяются в поле User-agent.
— **Блокировка по регионам**. Базы GeoIP активно используются разными атакующими, и фишинг не исключение. Если атакуемая аудитория находится в Сингапуре, то отдавать фишинговую страницу пользователям из США нет смысла.
— **Редиректы на официальные сайты**. При несоблюдении некоторых проверок вместо фишингового контента посетители будут перенаправляться на официальные сайты атакуемого бренда либо на сайты других легальных сервисов.

Партнерские программы

Каждый отдельный мошенник, занимающийся фишингом, не может нанести значительного ущерба. Поэтому появляются партнерские программы, которые объединяют множество желающих заработать на фишинге.

В России основной причиной роста стали различные партнерские программы вокруг тем, связанных с выплатой бонусов от банков, розыгрышей лотереи, прохождения платных опросов и т. п. На финальной стадии жертву просят ввести свои платежные данные либо сделать перевод самостоятельно.

Задачей партнеров является распространение ссылок среди как можно большей аудитории. А организаторы партнерской программы создают веб-страницы, принимают платежи и обеспечивают отмывание денежных средств. Например, в рамках одной из партнерских программ за небольшой период времени были созданы более 12 тыс. аккаунтов денежных мулов для приема похищенных средств.

Такой тренд пока наблюдается только в России, которую часто используют как тестовую площадку, поэтому мы ожидаем, что аналогичные схемы могут появиться и в других регионах.

Автоматизация управления фишинговыми проектами

С начала года наблюдается рост продвинутой социальной инженерии, где в фишинговой атаке применяются многоходовые сценарии. В таких набирающих популярность фишинговых схемах жертву предварительно прорабатывают — устанавливают с ней контакт (например, посредством мессенджера), создают вокруг нее атмосферу легитимности действий и только после этого направляют на фишинговую страницу.

Особенно интересен процесс взаимодействия между членами таких новых преступных группировок. Координация атак, коммуникация, распределение похищенных средств осуществляются с помощью специальных Telegram-каналов и ботов. Типичная инфраструктура такого проекта, построенного на базе Telegram, может включать:

— бот для рекрутинга, куда вносится информация о новом кандидате, участнике кибергруппы — опыт работы в скаме, сколько лет, линк на профиль на форуме и прочее;
— бот для отображения информации об успешных хищениях (кто — никнейм в Telegram, сколько денег и на чем заработал);
— закрытые каналы для взаимодействия/общения/помощи между участниками скам-группы;
— боты для генерации фишинговых ссылок по определенным настройкам, которые вносят участники группировки во время атак;
— и т. д.

На подпольных хакерских форумах, помимо уже традиционных фишинговых наборов, сегодня предлагаются готовые платформы управления, предназначенные для автоматизации фишинговых проектов. За счет таких платформ, распространяющихся по формату SaaS, растет количество атакующих группировок, легко поддающихся масштабированию. Количество участников группы, построенной вокруг таких платформ, может достигать нескольких десятков человек. Автоматизация управления преступной группировкой, в свою очередь, приводит к появлению и распространению более сложной социальной инженерии, которая начинает применяться в масштабных атаках, а не только в точечных, как было ранее.

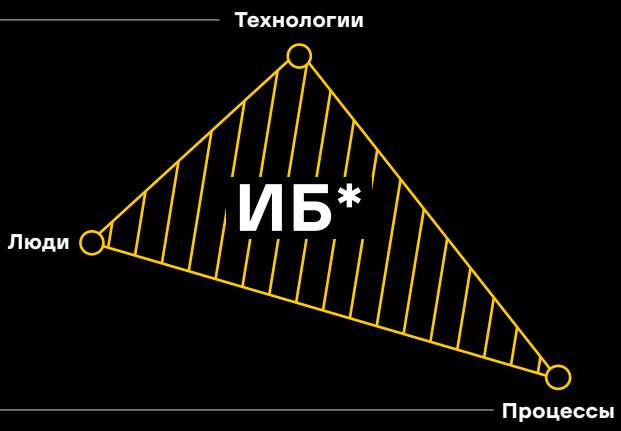
РЕКОМЕНДАЦИИ

Фундамент информационной безопасности

Инструменты, тактики, техники преступников сегодня становятся более изощренными и меняются быстрее, чем происходит обновление систем защиты во многих компаниях. Именно это влияет расстановку сил на поле боя информационной безопасности. Используйте возможности последних разработок и классов решений, доступных на рынке, чтобы не давать сопернику получить превосходство.

Даже автоматизированные системы последнего поколения управляются командой специалистов. Именно от них зависит, насколько вы используете возможности продукта, а значит, и эффективность решения. Процесс обучения и инноваций можно приостановить, но не закончить.

Важно не только количество человек в вашей команде по реагированию, но и слаженность и заменимость каждой единицы в команде. Консультанты всегда советуют распределить роли, но проводите ли вы отработку сценариев на регулярной основе? Знает ли каждый член команды, как он должен действовать в той или иной ситуации? При написании сценариев задействуйте вашу команду и налаживайте эффективное взаимодействие между командами и сотрудниками.



* Информационная безопасность

Общие рекомендации

Защита уже стала проактивной

Мониторинг и проактивный поиск угроз уже не в новинку для индустрии ИБ, но далеко не все успели внедрить эти процессы. Собирать и сопоставлять индикаторы компрометации и TTPs атакующих нужно постоянно. Обучайте свою команду новым техникам, повышайте их квалификацию и предоставляйте новейшие инструменты для работы.

Гигиена, гигиена и еще раз гигиена

Среди трендов последних лет в списке самых популярных векторов первоначальной компрометации уверено держатся фишинг и социальная инженерия. Рядовые сотрудники компании держат оборону информационной безопасности каждый день за своими мониторами и в своих почтовых ящиках. Парольная политика, обучения и внеплановые социотехнические тестирования помогут защититься от фишинга и предотвратить утечки корпоративных данных.

Доверяем провайдерам и партнерам

Появляется все больше продуктовых новинок, и все больше технических навыков требуется для обеспечения информационной безопасности. Компании отдают определенную часть задач информационной безопасности на MSS провайдеров. Это не только эффективно в контексте подбора и найма редких сотрудников с высокой технической подготовкой, но и выгодно для распределения бюджета.

Общайтесь с конкурентами

Для повышения осведомленности о новых угрозах вам будет полезно не только проходить обучения и повышения квалификации, но и присоединиться к диалогу с коллегами по отрасли. В чем конкуренты могут объединяться, так это в борьбе с общим врагами: APT, прогосударственными группировками, шифровальщиками и другими.

Глубокие проверки и страхование киберрисков

Как человеку нужно проходить медицинский осмотр, так и компания должна проводить на регулярной основе оценку безопасности. Сегодня это касается не только аудита инфраструктуры, но и проверок команды и процессов. Стандартный набор таких проверок следует дополнять участием третьей стороны, а также оценкой потенциальной ретроспективной компрометации. Все это не отменяет важности страхования киберрисков, особенно когда вы несете ответственность за информацию ваших клиентов и сотрудников.

Измерение эффективности

Информационная безопасность из года в год становится дороже для компаний, появляется запрос на оценку и сравнение эффективности решений. Насыщенный рынок диктует новые правила, решение должно быть не просто современным и эффективным, но и выгодным для бизнеса. Соизмерение затрат к эффективности инструмента на этапе пилотов требует и определения метрик бизнеса, которые так или иначе зависят от размера компании и ее инфраструктуры. На запрос рынка о ведении метрик оценки эффективности отвечают аналитики Gartner, Forrester и других аналитических агентств.

Рекомендации по техническому оснащению инфраструктуры и подготовке команды информационной безопасности

- Проводить поиск следов скрытого присутствия злоумышленников в сети организации, направленный на недопущение успешного завершения атаки, первые стадии которой не были выявлены средствами обеспечения информационной безопасности организации.
- Внедрить решение класса Malware Detonation Platform, позволяющее осуществить изолированный запуск подозрительных файлов и ссылок для их подробного анализа и последующего блокирования.
- Используя решение класса Threat Intelligence, выявлять угрозы, утечки, взломы и хакерскую активность до того, как они смогут вам навредить
- Производить регулярное резервное копирование, при этом резервные копии должны располагаться отдельно от основной сети, у атакующего не должно быть к ним доступа даже при компрометации учетных записей администраторов.
- Проведение круглосуточного мониторинга событий ИБ с возможностью быстрого реагирования на выявленные инциденты
- Каждому инциденту должен присваиваться уровень сложности, и инциденты, требующие разбора, должны быть расследованы, а также необходимо выявлять причины и последствия, устранять неполадки, вызвавшие инцидент. Для второго уровня реагирования, важно заранее иметь стороннюю команду специалистов по реагированию на инциденты, которая сможет ассистировать в остановке сложной целевой атаки.
- Убедитесь, что в вашей команде есть необходимые навыки для осуществления Threat Hunting & Intelligence.
- Проводите регулярные тренинги по цифровой гигиене для сотрудников.
- Проводите аудиты информационной безопасности в формате, имитирующем действия злоумышленников. Они помогут выявить слабые места в инфраструктуре компании и покажут, насколько компания готова к реагированию на реальные инциденты ИБ.
- Проводите периодические оценки рисков мошенничества для понимания того, соответсвуют ли ваши решения и процедуры существующим атакам и мошенническим схемам, использующим разные каналы. Определяйте основные факторы риска и отталкивайтесь от существующих и возможных проблем, чтобы обоснованно выбрать решение для защиты от мошенничества.
- Выстраивайте эшелонированную защиту веб-портала, используя не только анализ транзакций со стороны пользователей, но и решения для сессионного анализа поведения и устройства защиты от ботов на веб-каналах.

К сожалению, обнаружить атаку на ранних этапах удается не всегда: атакующие постоянно улучшают свои навыки и реализуют все новые техники для получения доступа к сетям различных компаний. Чтобы получить возможность обнаруживать следы компрометации на разных этапах жизненного цикла кибератаки, необходим комплексный подход, предполагающий наличие централизованного источника информации и происходящем в сетевой инфраструктуре, а также позволяющий при необходимости изолировать скомпрометированные узлы.

В качестве такого источника могут быть использованы решения класса XDR, которые позволяют успешно обнаружить потенциально вредоносную активность на различных уровнях, вне зависимости от используемых злоумышленниками тактик, техник и процедур.

Время нахождения атакующих в сети также обуславливает необходимость не только качественного реактивного, но и проактивного анализа, который могут осуществлять как сотрудниками организации, при наличии соответствующих компетенций, так и привлеченные специалисты, что значительно сокращает время и увеличивает качество такого анализа.

Безусловно, как реактивный, так и проактивный анализ, требуют не только наличия соответствующих компетенций, но и значительного объема данных киберразведки, которые обеспечивают специалистов организаций знаниями об угрозах, включая и стратегические, и операционные, и тактические данные. Так можно идентифицировать атакующих в ходе проводимого анализа, а иногда и обнаруживать компрометацию на самых ранних этапах.

Компетенции команды реагирования

Анализ записей логов и журналов событий
Firewall, Proxy, NetFlow, AV, EDR и др.

Анализ вредоносного ПО

Цифровая криминалистика конечных устройств

Cyber Threat Intelligence

Системное администрирование
Windows (Active Directory), Unix/ Linux, hypervisor, cloud

Управление инцидентом
менеджмент рисков, кризисное управление

Киберпрофессии будущего — профессии основанные на навыках востребованных уже сегодня. Этим профессиям не научат в классических учебных заведениях.

1. **Digital Forensics Analyst**
   Windows Forensics, Network Forensics, Memory Forensics, Forensics Data Recovery Mobile Forensics,
2. **Incident Responder**
3. **Threat Hunter**
4. **Malware Analyst**
5. **Threat Intelligence Analyst**

ТЕХНИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ВЫДЕЛЕННЫХ В ОТЧЕТЕ АТАК

Банковские бот-сети, трояны (TrickBot, Qbot, Silent Night и др.)

Рекомендации связаны со стандартными векторами атаки:

1. Атаки на уязвимое ПО, браузеры, операционные системы.
— своевременно обновлять ПО
— не переходить по подозрительным ссылкам
— не устанавливать ПО из недоверенных источников

2. Фишинговые рассылки:
— не открывать подозрительные письма и вложения
— использовать решения класса Group-IB Threat Hunting Framework и подобные решения

Уязвимые версии программного обеспечения в публичных сервисах или слабые пароли. Уязимости с публичными эксплойтами

Рекомендации соответствуют уровню ошибок:

— Своевременно обновлять ПО
— Проводить автоматизированную инвентаризацию ПО на предмет выявления устаревших версий
— Регулярно проводить анализ защищенности и тестирования на проникновение, чтобы выявить «слабые места» в сети и продемонстрировать возможные векторы атак
  — Усилить парольную политику
  — Включить многофакторную аутентификацию
  — Скрывать сервисы за VPN на внешнем сетевом периметре. Где нет VPN – внедрять SSO

Распределенный перебор паролей к интерфейсам удаленного доступа (RDP, SSH, VPN) и другим сервисам (с помощью новых бот-сетей)

— Проводить инвентаризацию внешнего сетевого периметра, правил межсетевого экранирования (Firewall) и правил трансляции сетевых адресов (NAT), для исключения ошибочно опубликованных сервисов
— Ни при каких обстоятельствах, даже временно, не публиковать в Интернет устройства, которые могут быть легко скомпрометированы: видеонаблюдение, «умный дом», оргтехнику (принтеры, сканеры, МФУ), устройства хранения (типа NAS серверов сегмента SOHO)
— Не публиковать на внешнем сетевом периметре сервисы непосредственного удаленного доступа для операционных систем (RDP, SSH, VNC, SMB/RPC и др.)
  — Если все-таки этого невозможно избежать, необходимо сменить порт SSH/RDP на нестандартный, и обязательно создать «белый список» IP-адресов, которые имеют к ним доступ
— Реализовать удаленный доступ, который бы отвечал следующим требованиям:
  — Наличие многофакторной аутентификации
  — Усиленная парольная политика
  — Возможность ограничения сетевого доступа по задачам конкретной учетной записи (к примеру, подрядчик получает доступ только к нужному ему серверу, а не всему сегменту или всей сети).
  — Выставлять поля вида «expires at» для учетных записей и правил доступа, на случай, если даст сбой процесс ручного отзыва удаленного доступа

Программы-вымогатели

— Успешность RAAS напрямую зависит от общего уровня защищенности всей компании.
— Актуальны рекомендации для угроз, которые злоумышленники используют в более традиционных взломах:
— Уметь выявлять признаки изначального доступа, закрепления в системе, продвижения по сети. Хотя в большинстве случаев техники атакующих достаточно примитивны, и их можно увидеть прямо невооруженным глазом, для более сложных атак может помочь регулярная проактивная охота за угрозами (threat hunting);
— Детектировать и регулярно дополнительно проверять свою инфраструктуру на known-bad индикаторы компрометации
— Соответствующей рекомендацией будет использование систем, таких как Group-IB Threat Hunting Framework и Group-IB Threat Intelligence & Attribution

Фреймворки для постэксплуатации: бесплатный Metasploit либо взломанная версия Cobalt Strike, значительно реже — фреймворки PoshC2 или Koadic

— Убедитесь, что имеющиеся средства информационной безопасности могут детектировать следы использования популярных пост-эксплуатационных фреймворков
— Используется достаточное количество различных и уникальных источников информации при проверке защищенности своей инфраструктуры и подготовке к атаке

Supply-chain-атаки

— Убедиться, что существующие средства защиты могут обнаруживать аномальную активность в контексте использования легитимного программного обеспечения, установленного в организации. Например, запуск нетипичных процессов, создание файлов, модификации файловой системы или реестра, характерные для техник закрепления в системе, и т.п.
— Стандартные средства защиты далеко не всегда способны справиться с подобными задачами, поэтому стоит обратить внимание на Group-IB Threat Hunting Framework

Получение более высоких прав доступа с помощью различного ПО (например, Mimikatz, LaZagne) или брутфорса

— Что касается брутфорса, то рекомендации здесь касаются парольной политики, аутентификации и т.п.
— Что касается Mimikatz, рекомендуем:
— Перейти на Windows 10/2016 с функционалом Credentials Guard
— Пользоваться группой "Protected users" для администраторских учетных записей.
— Выстраивать систему привилегированного доступа, согласно рекомендациям самой Microsoft
— Если предполагается, что атакующий может обойти перечисленные выше методы (относительно Mimikatz), или если невозможно реализовать предыдущие рекомендации, нужно убедиться, что системы защиты детектируют использование Mimikatz (чаще всего, запущенный с помощью фреймворка для постэксплуатации)
— Логировать обращение к памяти lsass.exe и определять подозрительные процессы, осуществляющие такую активность

Инструменты для атак на физически изолированные сети с использованием USB-носителей для преодоления воздушного зазора

— Не пользоваться недоверенными USB-устройствами или USB-устройствами неизвестного/сомнительного происхождения

Новые рекорды мощности DDoS атак: 2,3 Тб/с и 809 млн пакетов в секунду

— Перейти на использование внешнего балансировщика или проксирующего сервиса, усложнять архитектуру, переносить IP-адреса на внешние сервисы для защиты всей инфраструктуры.
— Увеличивать полосы пропускания
— Закупать аппаратные средства фильтрации
— Переходить на операторов с соответствующими anti-ddos мощностями

Перехват BGP или утечка BGP-маршрутов

— Повышать общую осознанность среди других участников в сети, чтобы выработать цифровой аналог «группового иммунитета»
— Иметь как можно больше «стыков» с другими провайдерами, чтобы было больше цепочек распространения правильного маршрута.
— Наблюдать за своими сетевыми префиксами в других AS, в случае ошибочного анонса префикса или обнаружения атаки, срочно связываться с RIR, которые допускают транзитную передачу ложного префикса для пресечения подобной активности

Карточный процессинг, системы межбанковских переводов

— Успех атак на эти системы напрямую зависит от общего уровня защищенности всей инфраструктуры. Рекомендуем обратиться к комплексным решениям (Group-IB Threat Hunting Framework) и системам киберразведки (Group-IB Threat Intelligence & Attribution)

JS-снифферы

— Своевременно обновляйте CMS-системы, плагины, контролируйте версии файлов сайтов
— Усиливайте парольную политику административных аккаунтов на сайтах
— Используйте такие решения, как Group-IB Fraud Hunting Platform для обнаружения подобного вредоносного кода на сайте

Атаки на POS-терминалы

Успех атак на эти системы напрямую зависит от общего уровня защищенности всей инфраструктуры. Рекомендуем обратиться к комплексным решениям (Group-IB Threat Hunting Framework) и системам киберразведки (Group-IB Threat Intelligence & Attribution)

Получение доступа к SCADA-системам, чтобы манипулировать процессом производства

Успех атак на эти системы напрямую зависит от общего уровня защищенности всей инфраструктуры. Рекомендуем обратиться к комплексным решениям (например, у Group-IB Threat Hunting Framework есть функционал по защите почты) и системам киберразведки (Group-IB Threat Intelligence & Attribution)

Credential stuffing

- По возможности, запретить пользователям регистрироваться на каких-либо сторонних сервисах с использованием корпоративной почты, так как пользователи склонны использовать один и тот же пароль на многих сервисах или незначительные модификации этого пароля. При утечке паролей из одного сервиса злоумышленник может атаковать всю компанию
  - Также, пароль в руках злоумышленника может использоваться для социотехнической атаки на конкретного пользователя
- Проверять наличие «своих» учетных записей в утечках (например, используя систему Group-IB Threat Intelligence & Attribution)

Веб-фишинг и социальная инженерия

Рекомендации для потенциальных жертв по взаимодействию с различными площадками (например, маркетплейсами):

- обращать внимание на доменные имена, особенно в рекламных ссылках в поисковых системах, а также при общении с потенциальным продавцом
- на популярных платформах для покупки/продажи товаров не переходить на общение в чаты за ее пределами, так как в этом случае история переписки и правила антифрода платформы не сработают
- для платформ самостоятельной продажи/покупки товаров нужно обращать внимание на рейтинг продавца.
- не стоит быстро реагировать на неадекватно низкую стоимость товара с невнятными причинами дешевизны. Как правило подобные низкие цены призваны усыпить бдительность потенциальной жертвы

Для самих платформ:

- создать систему фродмониторинга, борьбы с фродом.
- использовать систему Group-IB Fraud Hunting Platform

Прочие сайты, интернет-магазины и их посетители:

- обращать внимание на дату регистрации доменного имени, правильность написания домена
- обращать внимание на сайт – насколько полно описана информация о товаре, отзывы пользователей
- внимательно относиться к сайтам, которые выдаются в топе рекламы в поисковых системах. Часто рекламу там выкупают злоумышленники и рекламируют свои сайты
- внимательно относиться к сайтам, где цена продажи товара заниженна
- подключить систему Group-IB Fraud Hunting Platform для владельцев сайтов
- подключить Group-IB Digital Risk Protection для владельцев сайтов

Рост спроса на вредоносный код для Linux

- ставить пакеты только из официальных репозиториев
- тщательно проверять информацию о разработчиках пакетов, отсутствующих в официальных репозиториях
- следовать общим рекомендациям Linux-сообществ по информационной безопасности (например, снять суидные биты на ненужных бинарниках)
- использовать минимум прав при работе с недоверенным ПО

Владельцы IoT-ботнетов могут начать продавать доступ к устройствам, которые установлены в корпоративных сетях

- проводить инвентаризацию внешнего сетевого периметра, правил межсетевого экранирования (Firewall) и правил трансляции сетевых адресов (NAT), для исключения ситуаций, когда имеются ошибочно опубликованные сервисы.
- ни при каких обстоятельствах, даже временно, не публиковать в Интернет устройства, которые могут быть легко скомпрометированы: устройства видеонаблюдения, устройства «умного дома», оргтехнику (принтеры, сканеры, МФУ), устройства хранения типа NAS серверов сегмента SOHO
- не публиковать на внешнем сетевом периметре сервисы непосредственного удаленного доступа для операционных систем (RDP, SSH, VNC, SMB/RPC и др.)
  - если все-таки этого невозможно избежать, необходимо сменить порт SSH/RDP на нестандартный, и обязательно сделать «белый список» IP-адресов, которые имеют доступ
- реализовать удаленный доступ, который бы отвечал следующим требованиям:
  - наличие многофакторной аутентификации
  - усиленная парольная политика
  - возможность ограничения сетевого доступа по задачам конкретной учетной записи (к примеру, подрядчик получает доступ только к нужному ему серверу, а не всему сегменту или всей сети)
  - рекомендуется выставление полей вида «expires at» для учетных записей и правил доступа, на случай, если даст сбой процесс ручного отзыва удаленного доступа

Эксплойты и шпионские программы для Android и iOS

- не заходить на недоверенные/подозрительные сайты
- не устанавливать ПО из непроверенных источников
- своевременно обновлять ОС и программное обеспечение гаджетов
- разделять личное устройство и рабочее. Если речь о шпионаже – использовать для работы одно устройство, для личного – другое, не смешивать
- Использовать такие системы, как Group-IB Threat Intelligence & Attribution, где появляются уведомления о новых атаках, новом ПО, эксплойтах
- Использовать такие системы, как Group-IB Fraud Hunting Platform, который умеет определять активный RAT на мобильном устройстве

Мобильные RAT

- Не устанавливать недоверенное ПО
- Следовать рекомендациям против атак с использованием социальной инженерии, например. не поддавать на уговоры поставить TeamViewer для подключения сотрудника поддержки
- Своевременно обновлять ПО и операционные системы гаджетов
- Использовать такие системы, как Group-IB Fraud Hunting Platform, который умеет определять активный RAT на мобильном устройстве

Вектор атаки с точкой входа через VPN-сервер

- Реализовать удаленный доступ, который бы отвечал следующим требованиям:
  - наличие многофакторной аутентификации
  - усиленная парольная политика
  - возможность ограничения сетевого доступа по задачам конкретной учетной записи (к примеру, подрядчик получает доступ только к нужному ему серверу, а не всему сегменту или всей сети)
  - рекомендуется выставление полей вида «expires at» для учетных записей и правил доступа, на случай, если даст сбой процесс ручного отзыва удаленного доступа

Group-IB — один из ведущих разработчиков решений для детектирования и предотвращения кибератак, выявления мошенничества, расследования высокотехнологичных преступлений и защиты коммерческой и интеллектуальной собственности в сети.

INTERPOL И EUROPOL

Group-IB — партнер и участник совместных расследований

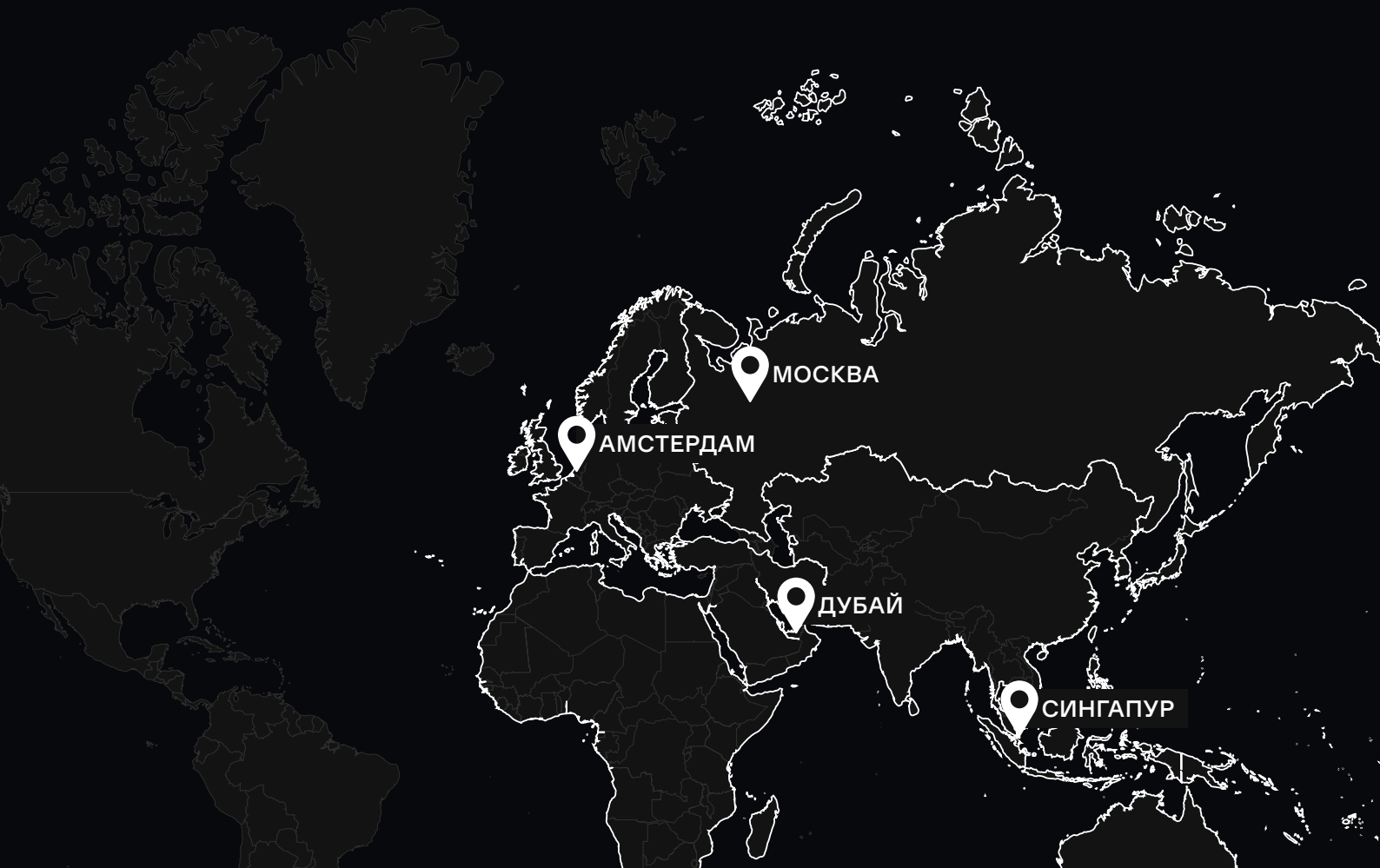
ТОП-10 В APAC

Group-IB вошла в топ-10 компаний по кибербезопасности в регионе APAC согласно APAC CIO Outlook

Центры исследования киберугроз Group-IB

- Европа
- Россия
- Ближний восток
- Азиатско-Тихоокеанский регион

- Распределенная по миру инфраструктура наблюдения за киберпреступностью
- Лаборатории компьютерной криминалистики
- Расследования киберпреступлений
- Круглосуточные центры мониторинга и оперативного реагирования CERT-GIB



Решения Group-IB

Опыт Group-IB в международных расследованиях, киберразведке и выявлении преступлений на разных уровнях подготовки был интегрирован в экосистему решений, объединившую чрезвычайно сложное программное и системное обеспечение, с целью мониторинга, обнаружения и предотвращения кибератак и мошенничества. Миссия Group-IB — защищать наших клиентов в киберпространстве, создавая и используя инновационные продукты и решения.

Решения Group-IB признаны мировыми агентствами в категориях:

— Innovation Excellence,
— Product Leader,
— Innovation Leader.

IDC
Gartner
FORRESTER
kuppingercole ANALYSTS
FROST & SULLIVAN

GARTNER IDC FROST & SULLIVAN FORRESTER

Threat Intelligence & Attribution

Система исследования и атрибуции кибератак, охоты за угрозами и защиты сетевой инфраструктуры на основании данных о тактиках, инструментах и активности злоумышленников

KUPPINGERCOLE ANALYSTS AG

Threat Hunting Framework

Реактивная защита и проактивная охота за угрозами внутри и за пределами вашей сети

FROST & SULLIVAN

Digital Risk Protection

Выявление и устранение цифровых рисков на основе искусственного интеллекта

KUPPINGERCOLE ANALYSTS AG FORRESTER GARTNER

Fraud Hunting Platform

Выявление и предотвращение мошенничества и бот-активности в режиме реального времени

NEW

Atmosphere: Cloud Email Protection

Облачная защита электронной почты от целевых атак, детонация полезных нагрузок и атрибуция угроз

550+	70 000+	1 300+	18 лет
экспертов международного класса	часов реагирования на инциденты информационной безопасности	успешных расследований по всему миру	практического опыта

Intelligence-driven services

FORRESTER
GARTNER

В основе технологического лидерства компании и возможностей в сфере научных исследований и разработки — 18-летний практический опыт расследования киберпреступлений по всему миру и более 70 000 часов реагирования на инциденты информационной безопасности, аккумулированные в распределенной по миру инфраструктуре наблюдения за киберпреступностью.

РАССЛЕДОВАНИЯ И КРИМИНАЛИСТИКА

Компьютерная криминалистика.
Анализ вредоносного кода.
Расследования:

- сложных высокотехнологичных преступлений;
- утечек информации;
- финансовых, корпоративных киберпреступлений;
- сложных атак на объекты КИИ и другие.

АУДИТ И ОЦЕНКА РИСКОВ

Тестирование на проникновение.
Анализ исходного кода.
Выявление следов компрометации сети.
Киберобучение в формате Red Teaming.
Проверка готовности к реагированию на инциденты.
Оценка соответствия.

THREAT HUNTING И РЕАГИРОВАНИЕ

24/7 Центр реагирования CERT–GIB.
Проактивный хантинг угроз.
Выездное реагирование на сложные кибератаки.
Реагирование на инциденты по подписке.

ОБУЧАЮЩИЕ ПРОГРАММЫ

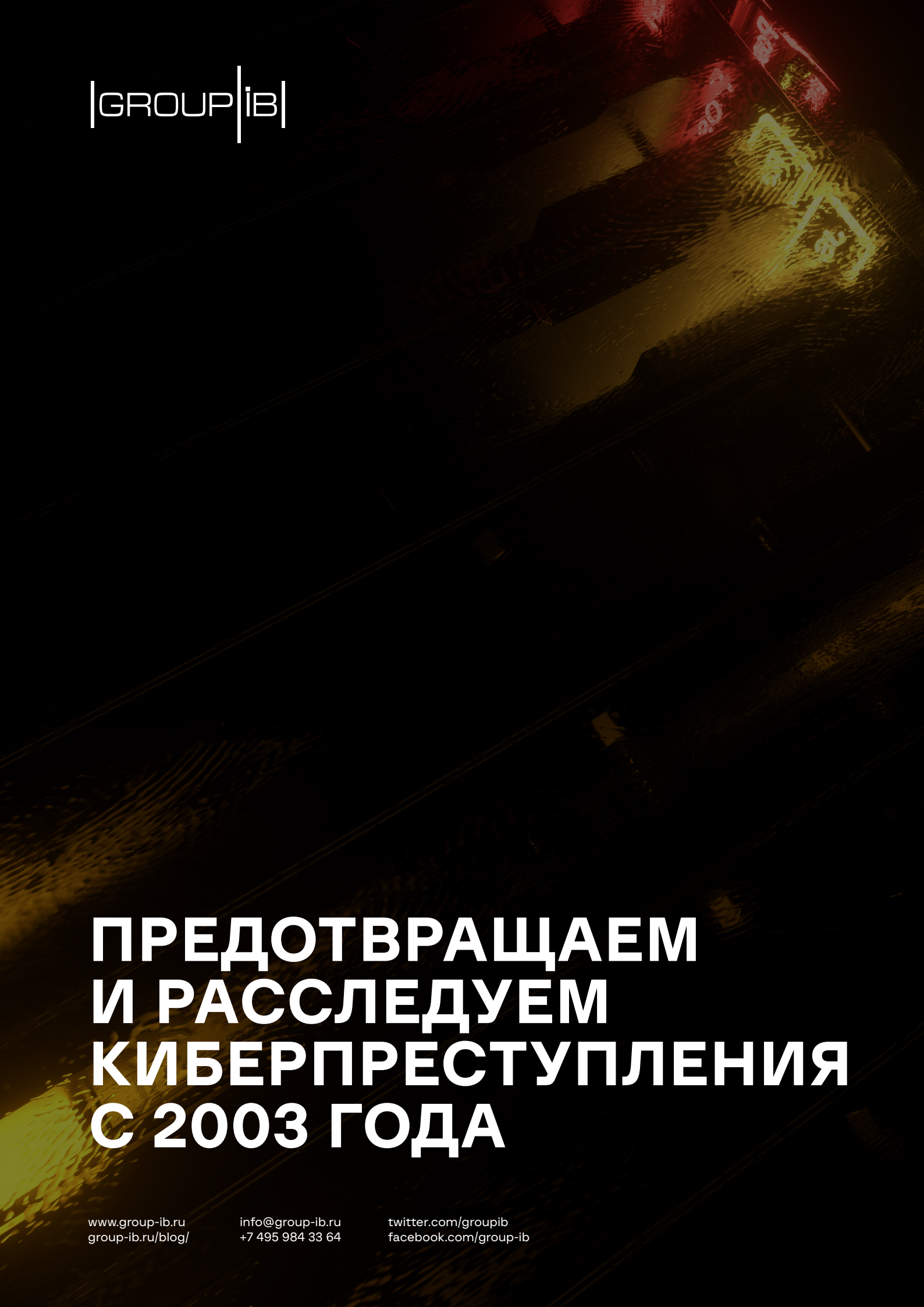
Курсы для технических специалистов:

- Реагирование на инциденты,
- Анализ вредоносного кода,
- Проактивный поиск угроз и другие.

Программы для широкой аудитории:

- Цифровая гигиена,
- Личная кибербезопасность,
- Управление репутацией в интернете и другие.

Мастер-классы для школьников и студентов.



ПРЕДОТВРАЩАЕМ И РАССЛЕДУЕМ КИБЕРПРЕСТУПЛЕНИЯ С 2003 ГОДА

www.group-ib.ru
group-ib.ru/blog/
info@group-ib.ru
+7 495 984 33 64
twitter.com/groupib
facebook.com/group-ib