

Актуальные киберугрозы: I квартал 2022 года



Содержание

Резюме	3
Сводная статистика	4
Последствия атак	7
Вредоносное ПО: шпионы и вайперы	11
Курс на пользователей Android	15
Адаптация шифровальщиков	16
Рост числа атак на госучреждения	19
Серьезные последствия для промышленности	20
Криптовалюты и блокчейн	21
Атаки на разработчиков	23
Об исследовании	25

Резюме

Итоги I квартала 2022 года:

- Количество атак увеличилось на 14,8% по сравнению с IV кварталом 2021 года. При этом увеличилась доля массовых атак: теперь их количество составляет 33% от общего числа.
- Доля атак на частных лиц остается на прежнем уровне, составляя 15% от общего числа. Методы и мотивы атак не претерпевают существенных изменений.
- Чаще всего в результате атак организации сталкиваются с утечкой конфиденциальной информации (45%) и нарушением основной деятельности (30%). В атаках на частных лиц чаще всего были скомпрометированы конфиденциальные данные (55%), также пользователи могли понести финансовые потери (25%).
- Вырос интерес к веб-ресурсам: доля атак на них увеличилась до 22% от общего количества по сравнению с 13%, наблюдаемыми в IV квартале 2021 года.
- В пятерке наиболее атакуемых отраслей оказались СМИ: доля атак на них составляет 5%. А чаще всего атакам подвергались госучреждения: количество атак на них выросло практически в два раза по сравнению с предыдущим кварталом.
- Злоумышленники активно распространяют шпионское ПО, направленное на кражу учетных данных. В атаках на частных лиц учетные данные становятся известны злоумышленникам в 46% случаев. Особый интерес представляют учетные данные пользователей различных VPN-сервисов, которые впоследствии продаются на темных форумах.
- Доля шифровальщиков несколько снизилась по сравнению с IV кварталом 2021 года — с 53% до 44%. Такие изменения в определенной степени вызваны тем, что часть группировок вымогателей переходит на промышленный шпионаж без шифрования устройств. Некоторые из шифровальщиков, напротив, не присылают ключи дешифрования, нацеливаясь на разрушение инфраструктуры. Также растет число атак вайперов, которые уничтожают данные.
- ВПО продолжает попадать в официальные магазины приложений: было замечено множество, на первый взгляд, легитимных приложений, нацеленных на пользователей Android. Большинство из таких приложений являются банковскими троянами и загрузчиками, а количество скачиваний пользователями в некоторых случаях превышает сотни тысяч.
- Крупные атаки затронули IT-компании: от утечки данных пострадали такие гиганты отрасли, как Nvidia и Samsung. Также злоумышленники проводят массовые атаки на разработчиков, встраивая вредоносный код в открытые пакеты и библиотеки популярных платформ и фреймворков.

Для защиты от кибератак мы прежде всего советуем придерживаться общих рекомендаций по обеспечению личной и корпоративной кибербезопасности. Учитывая особенности I квартала, мы советуем разработчикам ПО внимательно тестировать библиотеки перед их использованием, а также контролировать защищенность и безопасную конфигурацию используемых сред разработки, проверять безопасность собственного кода. Укрепить безопасность веб-ресурсов на периметре компании можно с помощью современных средств защиты (например, web application firewalls). Чтобы предотвратить заражение устройства вредоносным ПО, мы советуем использовать песочницы, которые анализируют поведение файлов в виртуальной среде и выявляют вредоносную активность.

Сводная статистика

В I квартале 2022 года количество атак увеличилось на 14,8% по сравнению с IV кварталом 2021 года. Мы связываем это с обострением противостояния в киберпространстве. Чаще всего атакам подвергались государственные и медицинские учреждения, промышленные предприятия. Заметны изменения в пятерке самых атакуемых отраслей: здесь оказались СМИ. Также выросло число атак без привязки к отрасли экономики — с 18% до 23%.

Во второй половине квартала проводились множественные атаки на веб-ресурсы, и их доля выросла до 22% по сравнению с 13%, наблюдаемыми в прошлом квартале. Увеличилась доля атак, которые стали возможны из-за компрометации или подбора учетных данных. В основном они проводились на веб-ресурсы и аккаунты компаний в социальных сетях.

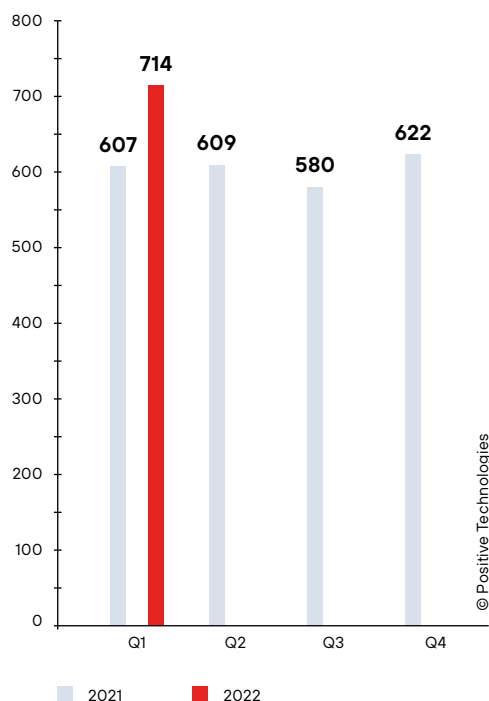


Рисунок 1. Количество атак в 2021 и 2022 годах (по кварталам)

67% атак носили целенаправленный характер



Рисунок 2. Категории пострадавших организаций

15% атак были направлены против частных лиц

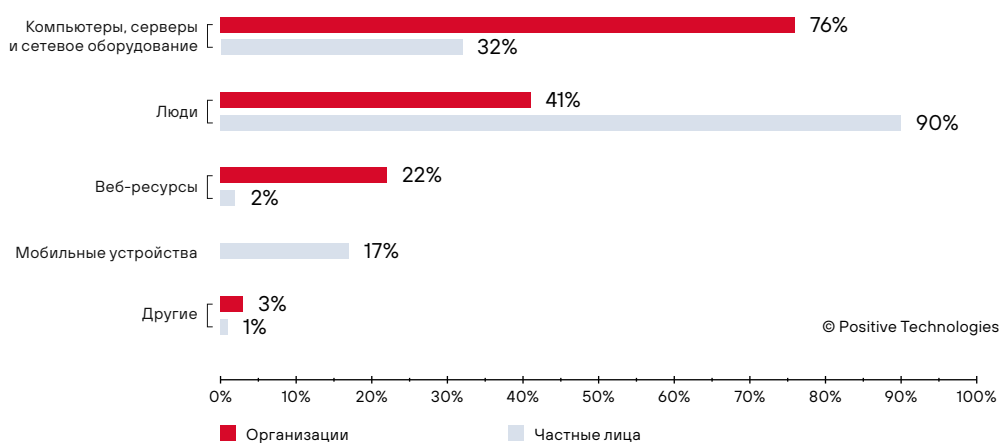


Рисунок 3. Объекты атак (доля атак)

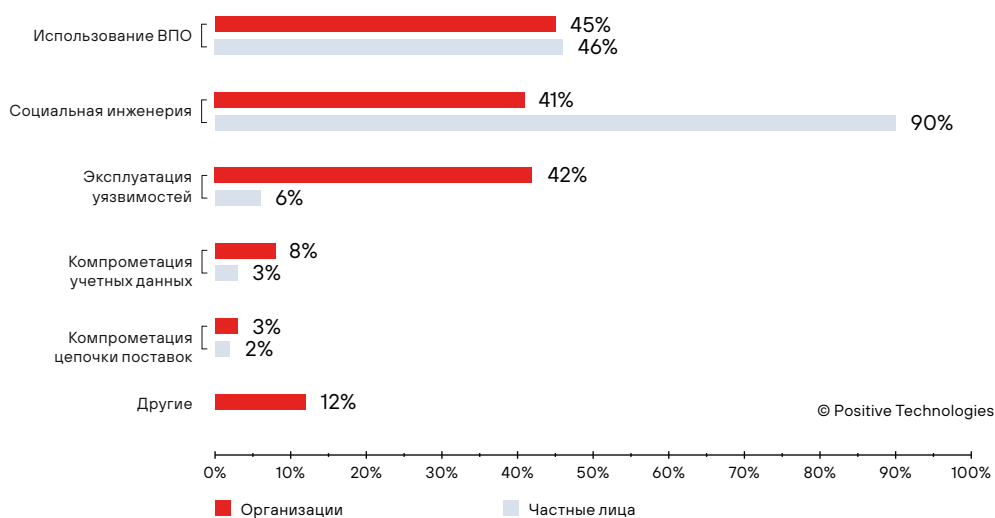


Рисунок 4. Методы атак (доля атак)



Последствия атак

Последствия атак разнообразны, и масштаб их влияния может варьироваться от воздействия на одного человека до воздействия на функционирование целой отрасли экономики или всего региона. Чаще всего атаки злоумышленников были направлены на получение конфиденциальной информации. Также из-за действий преступников возникали перебои в работе организаций, нарушение основной деятельности.

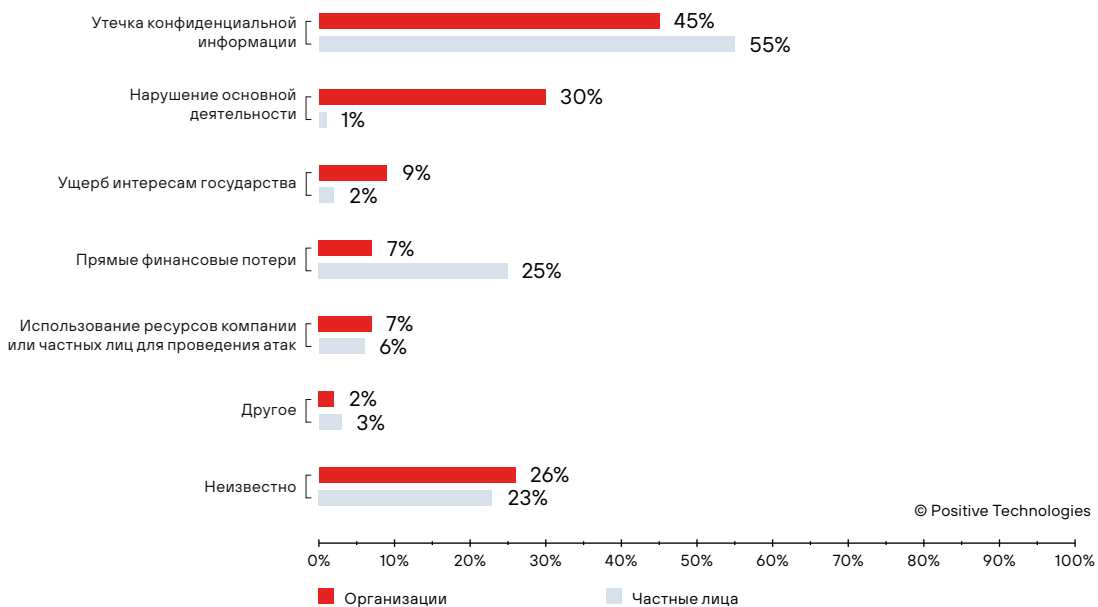
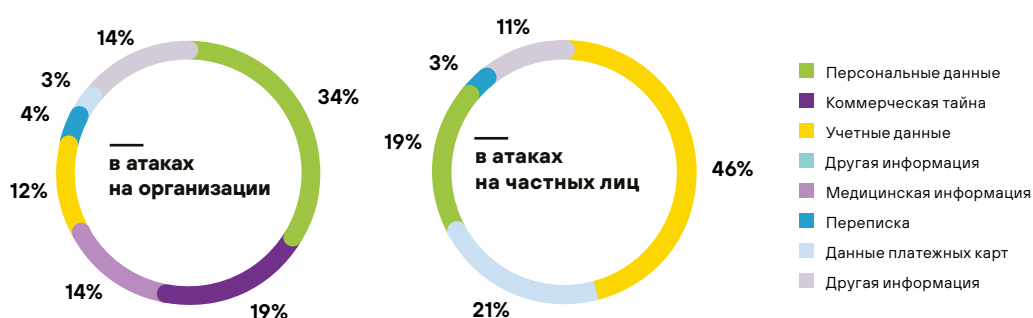


Рисунок 5. Последствия атак злоумышленников (доля атак)

Данные прежде всего

В I квартале действия злоумышленников были преимущественно направлены на кражу конфиденциальной информации: для организаций это в первую очередь персональные данные (34%) и сведения, составляющие коммерческую тайну (19%). Также пользовались популярностью медицинская информация (14%) и учетные данные (12%). В атаках на частных лиц были украдены учетные данные (46%), персональные данные (19%) и данные платежных карт (21%).



© Positive Technologies

Рисунок 6. Типы украденных данных

Громкие утечки коснулись преимущественно IT-компаний, более подробно их последствия рассмотрены в разделе «Атаки на разработчиков».

Стоит отметить, что наибольшую ценность в атаках как на организации, так и на частных лиц представляют учетные данные, которые позже могут быть проданы на теневом рынке или же использоваться для развития атаки внутри корпоративной сети. Охота на такую информацию ведется постоянно: так, в середине марта специалисты PT Expert Security Center (PT ESC) зафиксировали фишинговую рассылку на российские организации, отправленную якобы от Госуслуг, целью которой был сбор доменных учетных записей. В теле письма содержалась ведущая на поддельную страницу ссылка, которая формировалась интересным образом: злоумышленники использовали всего лишь несколько доменов, однако, чтобы ссылка была похожа на домен компании, вставляли в третий уровень домен атакуемой компании. Структура ссылки выглядела следующим образом: `mail.[домен_компании].[фишинговый_домен].ru`.

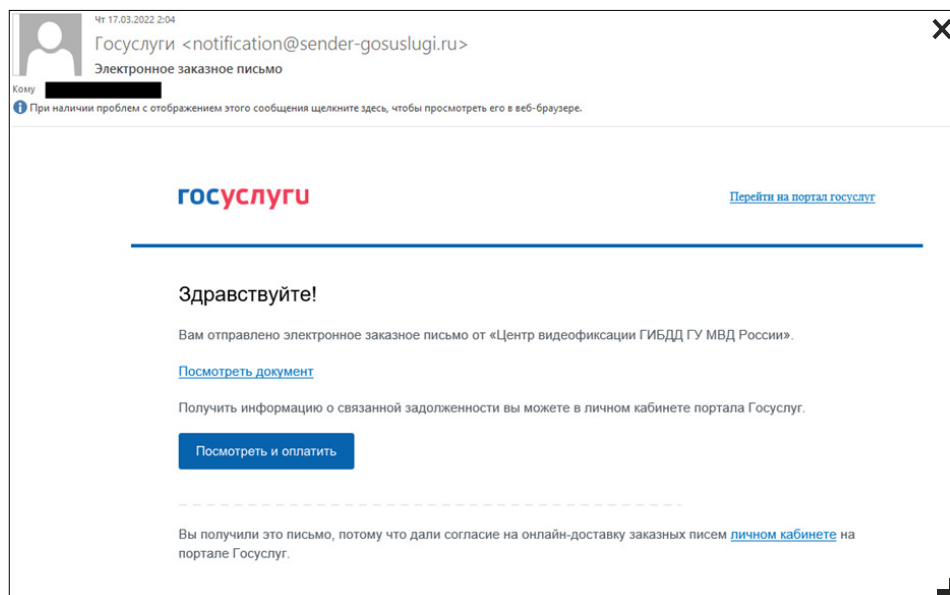


Рисунок 7. Фишинговая рассылка, имитирующая письмо от Госуслуг

Сбои в предоставлении услуг: от округа до целой страны

Февральская атака на телекоммуникационного оператора Vodafone вызвала сбои в обслуживании по всей стране, в том числе в работе сетей 4G и 5G, а также при передаче SMS-сообщений и предоставлении телевизионных услуг. Vodafone Portugal обслуживает более четырех миллионов абонентов сотовой связи в стране и еще 3,4 миллиона интернет-пользователей, поэтому масштабы последствий атаки почувствовали многие граждане Португалии. Кроме того, компании потребовалось много времени на восстановление своих систем: например, сайты организации снова стали функционировать спустя почти месяц.

Другой случай произошел в Нью-Мексико, США. В результате атаки на государственные системы округа Берналлилло многие госучреждения закрылись на несколько дней, а предоставление некоторых услуг населению стало невозможным. Атака затронула 675 000 жителей округа, а работы по восстановлению основных систем заняли 12 дней.

Транспортные системы под прицелом

В I квартале крупные атаки ждали и транспортную отрасль. В результате было затруднено передвижение пассажиров, возникали перебои с поставками продукции и сырья. И если из-за атаки на итальянскую железнодорожную компанию Ferrovie dello Stato Italiane была приостановлена продажа билетов, то белорусские железные дороги ждали более серьезные последствия. В результате первой атаки злоумышленники зашифровали серверы «Белорусской железной дороги», из-за чего онлайн-касса выдавала ошибку. В результате повторной атаки было парализовано движение поездов в Минске и Орше, а на белорусских форумах появились сообщения о перебоях с движением поездов в Минске.

Проблемы с транспортом касались не только железных дорог: злоумышленники могли влиять и на авиасообщение. Так, в I квартале компания Swissport International, оказывающая услуги по обслуживанию аэропортов, сообщила об атаке программы-вымогателя, которая привела к задержке рейсов.

Последствия кибератак на транспортную отрасль могут затрагивать цепочку поставок сырья и продукции: например, кибератаки на крупные нефтяные терминалы SEA-invest (Бельгия) и Evos (Нидерланды) повлияли на работу портов во всей Европе и Африке и привели к задержкам в поставках топлива.

Вредоносное ПО: шпионы и вайперы

Лидирующие позиции, как и ранее, занимают шифровальщики, использующиеся практически в каждой второй атаке с использованием ВПО, а также вредоносные инструменты для удаленного управления. Также в I квартале были замечены кампании по распространению ПО для удаления данных и для проведения DDoS-атак.

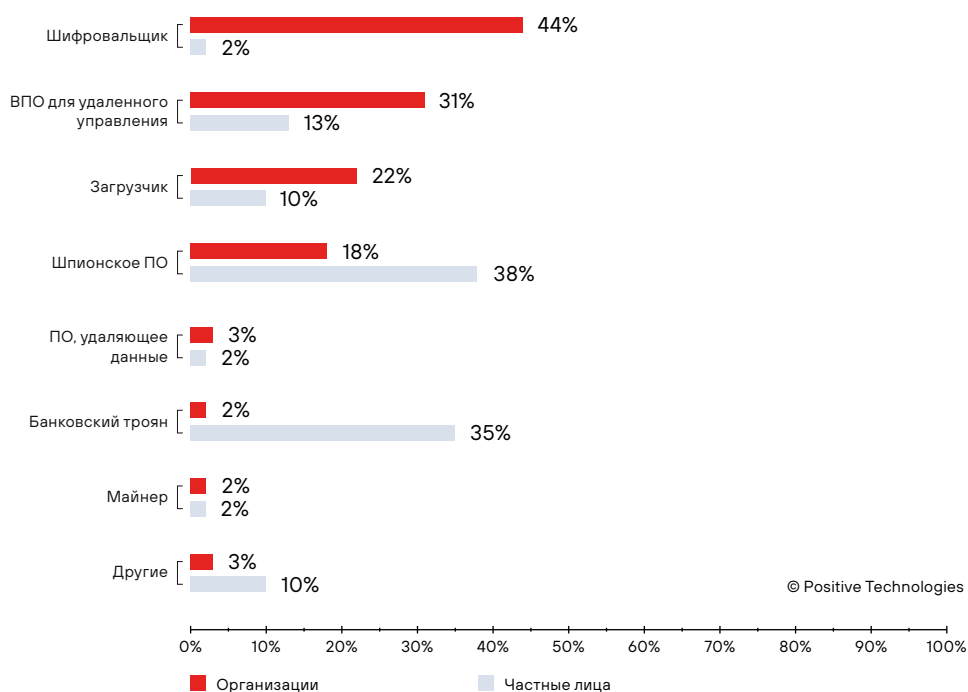


Рисунок 8. Типы вредоносного ПО (доля атак с использованием ВПО)

Волна вайперов

В I квартале увеличилось количество атак с использованием ПО для удаления данных: для организаций их доля составляет 3%, а для частных лиц — 2%. Среди таких «очистителей» данных, получивших распространение в I квартале, можно отметить WhisperGate, HermeticWiper, IsaacWiper, DoubleZero, CaddyWiper. Интересно, что в ряде случаев (а именно с WhisperGate) такое ВПО имитировало атаку программы-вымогателя: жертвам даже были оставлены сообщения с информацией о выкупе, однако ключи дешифрования предоставлены не были, а данные были необратимо повреждены.

Занимательно и ВПО CaddyWiper, которое проверяло, не являлось ли устройство контроллером домена: если оно являлось таковым, то данные не удалялись. Предполагается, что такая тактика использовалась злоумышленниками для сохранения доступа к зараженной системе.

Способы распространения вайперов также разнообразны: например, HermeticWiper распространялся через HermeticWizard — сетевого червя, а DoubleZero содержался в архивах, распространяемых в целевых фишинговых атаках. В случае с CaddyWiper злоумышленники обычно уже имели доступ к скомпрометированным сетям организаций.

Для защиты от атак вайперов в первую очередь проверяйте все полученные файлы в песочнице — специальной виртуальной среде. Убедитесь, что сеть корректно сегментирована: это усложнит распространение вредоносной программы в инфраструктуре. При этом особое внимание уделите изоляции критически важных систем и защите хранилищ резервных копий данных, чтобы избежать недопустимых для организации последствий.

Перепродажа доступов: VPN и не только

Злоумышленники активно распространяют инфостилеры для сбора информации о пользователе и системе, эксплуатируя разнообразные методы заражения. Доля шпионского ПО в атаках на организации составила 18%, а на рядовых пользователей — 38%.

Злоумышленники особо заинтересовались учетными данными пользователей VPN-сервисов, их теперь собирают инфостилеры: например, RedLine, Phoenix, Jester Stealer, Saintstealer. Так, стилер Phoenix может собирать данные из браузеров, инструментов VPN, Discord, местоположений файловой системы и криптовалютных кошельков, после чего отправлять их на удаленный сервер. Интересно, что это ВПО было замаскировано под другое, такое же незаконное: изначально пользователи скачивали программу для проведения DDoS-атак.

RedLine, еще одно широко используемое ВПО, нацелено на хищение учетных данных, хранящихся в браузере, паролей VPN, данных платежных карт и криптовалютных кошельков, файлов куки и другой информации. Впоследствии данные пользователей часто продаются на площадках в дарквебе: так, больше половины учетных данных на одной из площадок продавцы получают с помощью RedLine. При этом цена за доступ к одной учетной записи составляет от пяти долларов, но дальнейший ущерб для организации может исчисляться миллионами долларов, если злоумышленники скомпрометируют учетные данные сотрудника для удаленного подключения к корпоративной сети.

В I квартале мы также видели множество объявлений об услугах по подключению к VPN-сервисам. Стоит отметить, что такие «услуги» могут включать в себя продажу скомпрометированных учетных данных.

Способы распространения вредоносного ПО

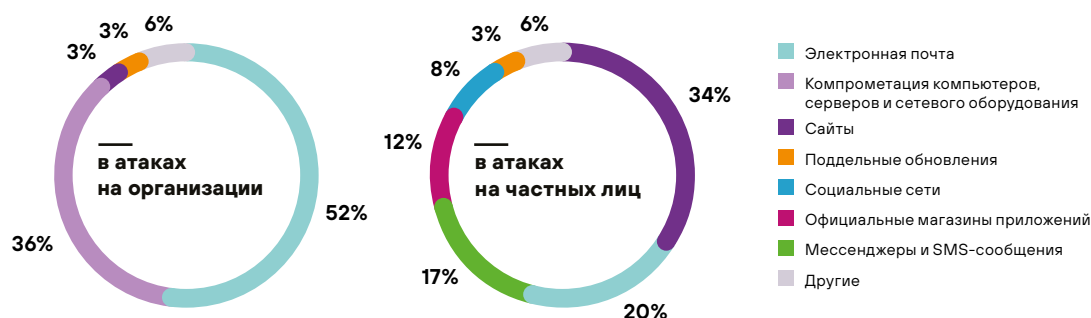


Рисунок 9. Способы распространения вредоносного ПО

Самым распространенным способом доставки ВПО по-прежнему является электронная почта, этот метод используется в 52% атак на организации. Так, например, специалисты РТ ESC зафиксировали рассылку с вложением, содержащим информацию о мероприятиях, якобы проводимых Роскомнадзором. На самом деле злоумышленники эксплуатировали уязвимость CVE-2021-40444 и загружали Cobalt Strike Beacon на устройство.

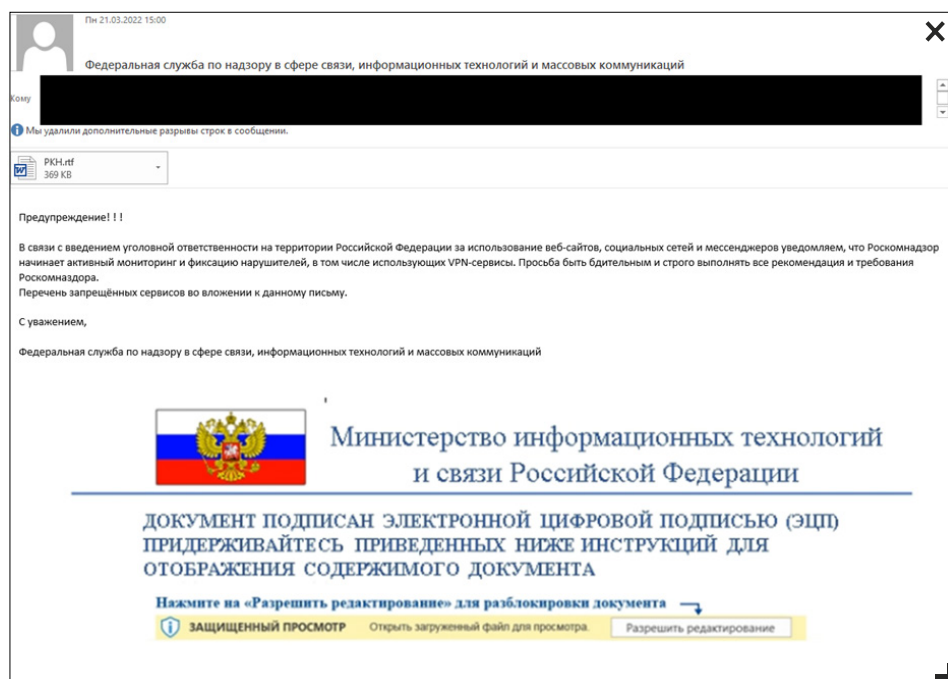


Рисунок 10. Фишинговое письмо с вредоносным вложением

Также в марте в атаках на российские научные предприятия использовались массовые рассылки. Пользователям предлагалось открыть вложение, чтобы ознакомиться со списком лиц, попавших под санкции, однако сам шаблон содержал вредоносный макрос, с помощью которого на устройство попадал загрузчик.

В атаках на частных лиц злоумышленники чаще всего использовали поддельные или скомпрометированные сайты, электронную почту, различные мессенджеры и социальные сети. Так, упомянутый выше стилер RedLine был нацелен на игроков Valorant и распространялся через YouTube: пользователям предлагалось перейти по ссылке в описании к видео, чтобы загрузить бота с автоматическим прицеливанием.

Способы сокрытия вредоносной деятельности

Чтобы скрыть свою деятельность, злоумышленники адаптируют методы и подходы для противодействия обнаружению. Например, ВПО BazarBackdoor распространяется через контактные формы на сайтах организаций вместо обычных фишинговых писем, чтобы вредоносное вложение не было обнаружено.

Также преступники продолжают злоупотреблять функциями легитимных сервисов и ПО. Например, в атаках на пользователей с учетными записями Google злоумышленники использовали функцию упоминания в Google Документах: пользователь получал уведомление об упоминании по почте, после чего мог перейти по вредоносной ссылке, оставленной в комментариях. А Raccoon Stealer использовал Telegram в качестве сервера контроля и управления: это позволяло скрыть подозрительный трафик в тех компаниях, в которых использовался этот мессенджер. Из-за популярности приложения злоумышленники все чаще используют этот инструмент.

Для противодействия анализу в некоторые вредоносные программы встраивают специальные функции, выполняющиеся в случае обнаружения. Так, в последнюю версию BRATA, ВПО для Android, была добавлена функция, сбрасывающая настройки устройства для удаления всех следов вредоносной деятельности.

Можно отметить и появление новых киберпреступников, еще не реализовавших свой потенциал. Исследователи из Symantec сообщают, что неизвестный злоумышленник использует новый сложный и мощный загрузчик вредоносного ПО Verblecon в относительно простых атаках, направленных на майнинг криптовалюты. Это ВПО на основе Java использует полиморфизм на стороне сервера, что помогает избежать обнаружения: с помощью шифрования и обфускации Verblecon может изменяться для сканеров безопасности каждый раз, когда загружается.

Курс на пользователей Android

Вредоносные программы снова и снова попадают в официальные магазины приложений, обходя защиту. В I квартале в Google Play появлялись и удалялись программы, содержащие вредоносные приложения: FluBot, TeaBot, SharkBot, Escobar, Vultur.

Ранее мы прогнозировали увеличение числа атак на пользователей онлайн-банков. Большинство распространяемых инфостилеров — это банковские трояны, а их доля от общего числа ВПО в атаках на частных лиц составляет 35%. Мы советуем быть осторожными при установке новых приложений и внимательно просматривать отзывы: ВПО может содержаться даже в безобидных, на первый взгляд, программах. Так, банковский троян FluBot распространялся как Flash Player, но, попав на устройство и получив необходимые разрешения, мог красть учетные данные из онлайн-банкинга, перехватывать SMS-сообщения и одноразовые пароли. Другой банковский троян, TeaBot, неоднократно появлялся в Google Play с декабря 2021 года, выдавая себя за приложения для считывания QR-кодов, приложения с прогнозом погоды, инструменты для очистки данных, и заразил более 140 000 устройств. Некоторые ВПО, например SharkBot, могут выдавать себя даже за антивирусные программы.

Злоумышленники все чаще добавляют в приложения возможность перехвата кодов многофакторной аутентификации (некоторые ВПО выдают себя за MFA-приложения, как, например, банковский троян Vultur) и увеличивают число встроенных функций. Так, банковский троян Escobar имеет широкий спектр возможностей: контроль над зараженными устройствами с помощью VNC Viewer, запись аудио, снимки экрана, перехват SMS-сообщений, чтение и запись хранилища, получение списка учетных записей, отключение блокировки клавиатуры, совершение вызовов и доступ к точному местоположению устройства. И это, по всей видимости, неокончательная версия ВПО: автор сдавал в аренду бета-версию программы за 3000 долларов в месяц, при этом другие злоумышленники могли бесплатно тестировать бота в течение трех дней.

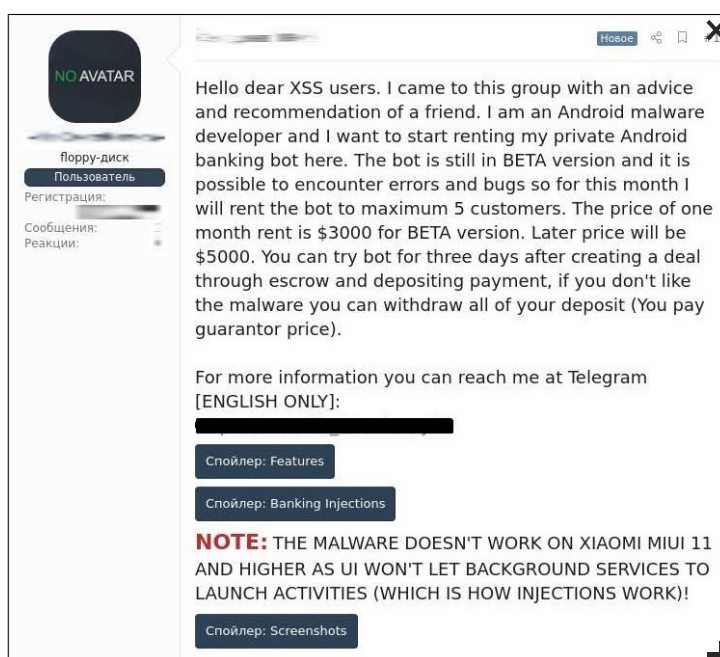


Рисунок 11. Объявление о сдаче в аренду банковского трояна Escobar

Адаптация шифровальщиков

В I квартале шифровальщики были все так же активны, и большая часть атак была направлена, как и ранее, на медучреждения: злоумышленников привлекал объем содержащейся в системах информации в сочетании с низкой защищенностью инфраструктуры. Выросла доля атак, направленных на госучреждения (с 8% до 13%). Кроме того, мы вновь наблюдали случаи громких атак на промышленные предприятия и IT-компании.



Рисунок 12. Доля атак шифровальщиков по их целям

Продолжение атак на устройства QNAP

Владельцам сетевых накопителей все еще необходимо держать руку на пульсе, своевременно устанавливая обновления системы безопасности: в январе программа-вымогатель Qlocker вернулась с новой кампанией. Сообщения о выкупе начали массово появляться на взломанных устройствах.

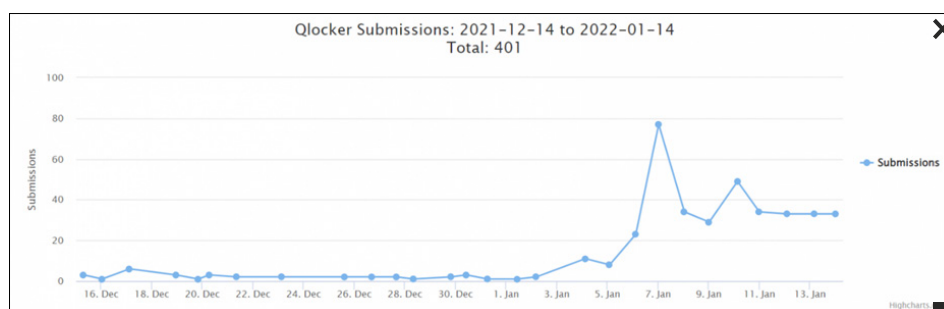


Рисунок 13. Количество атак Qlocker

Позже, также в январе, уже новая группа вымогателей DeadBolt массово шифровала устройства QNAP NAS по всему миру, используя уязвимость нулевого дня в программном обеспечении. Также DeadBolt оставила сообщение для компании: злоумышленники предложили сообщить детали уязвимости или прислать универсальный мастер-ключ для дешифрования за 50 BTC.

Адаптация к разным системам и кроссплатформенность

Для адаптации шифровальщиков к различным системам злоумышленники переписывают программы на другие языки: например, команда шифровальщиков BlackCat (бывшие участники BlackMatter, она же Darkside) делает новое мультиплатформенное ВПО на Rust. На этот же язык переписала свое ВПО и группировка Hive.

Атаки на системы виртуализации продолжаются. В начале квартала злоумышленники активно использовали нашумевшую уязвимость в библиотеке Log4j для атак на серверы VMware, при этом операторы-вымогатели адаптируют программы для разных операционных систем. Например, шифровальщик AvosLocker перешел на Linux и атакует серверы VMware ESXi.

Что будет дальше

Небольшое снижение доли атак шифровальщиков объясняется тем, что некоторые вымогатели переходят на кражу данных, шифруя инфраструктуру не во всех своих атаках. Примером может послужить группировка Lapsus\$, вновь заявившая о себе атаками на такие крупные компании, как Nvidia, Samsung, Microsoft и Globant. Скомпрометированные данные были выложены в открытый доступ, при этом системы не были зашифрованы.

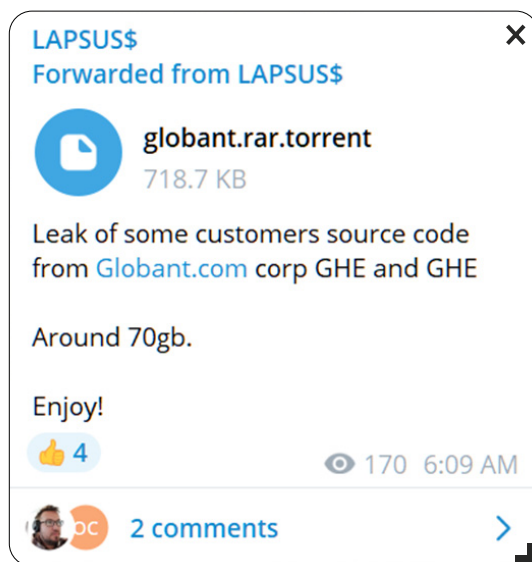


Рисунок 14. Архив скомпрометированных данных, опубликованный Lapsus\$

Мы предполагаем, что такой тренд могут подхватить и другие группировки. В дарквебе стали чаще появляться объявления о предоставлении услуг промышленного шпионажа и поиска информации в корпоративных сетях.

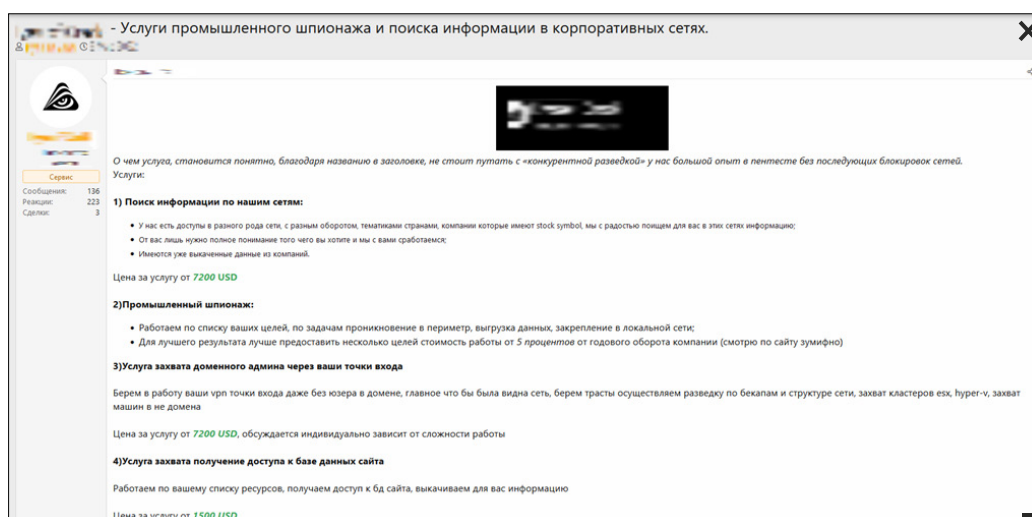


Рисунок 15. Объявление о промышленном шпионаже на теневого форуме

В проведении атак злоумышленники переключаются на страховые компании. Группировка REvil пояснила в интервью, почему такие организации являются привлекательной целью: в системах содержатся сведения о компаниях, которые с большой вероятностью заплатят выкуп, так как имеют полисы киберстрахования.

Рост числа атак на госучреждения

В I квартале 2022 года количество атак, направленных на госучреждения, вернулось на прежний уровень, увеличившись практически в два раза по сравнению с данными IV квартала 2021 года.

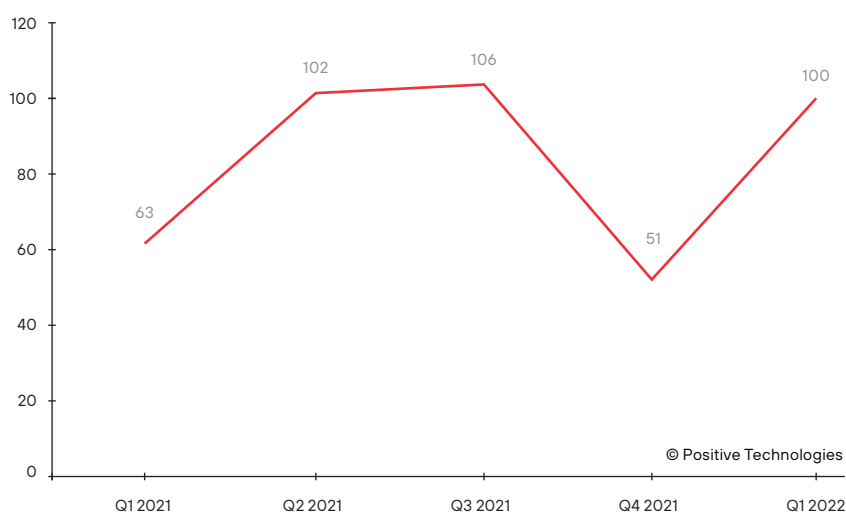


Рисунок 16. Количество атак на госучреждения

Действия злоумышленников в основном были направлены на нарушение деятельности организаций, а также на кражу конфиденциальной информации. Во второй половине квартала мы отметили всплеск атак на веб-ресурсы различных государственных учреждений.



Рисунок 17. Объекты атак на госучреждения (доля атак)

Чтобы вывести системы из строя, злоумышленники целились не только непосредственно в веб-ресурсы, но и в телекоммуникационные компании — поставщиков услуг: так, в Израиле был объявлен режим ЧС из-за беспрецедентной кибератаки на системы государства. Некоторые израильские правительственные сайты были недоступны. В оборонном ведомстве утверждают, что это была крупнейшая кибератака, когда-либо совершенная против Израиля.

Серьезные последствия для промышленности

I квартал не обошелся без масштабных атак, направленных на различные отрасли промышленности: нефтегазовую отрасль, энергетику, агропромышленность. Чаще всего злоумышленники атаковали компании для кражи конфиденциальной информации, но вредоносные воздействия значительно влияли и на основную деятельность компаний, наносили им серьезный ущерб: возникали простои из-за остановки целых заводов, поломки из-за вмешательства в технологические и бизнес-процессы.

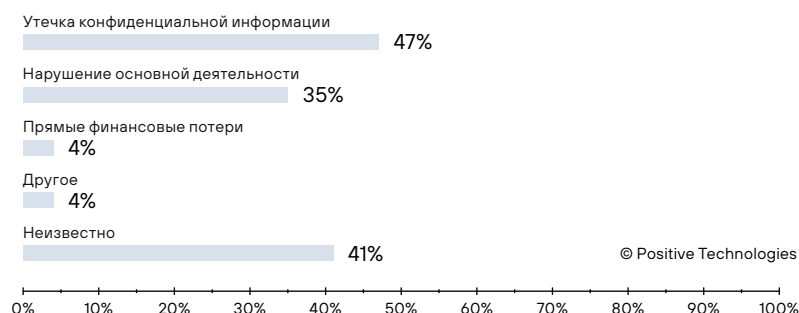


Рисунок 18. Последствия атак злоумышленников на отрасли промышленности

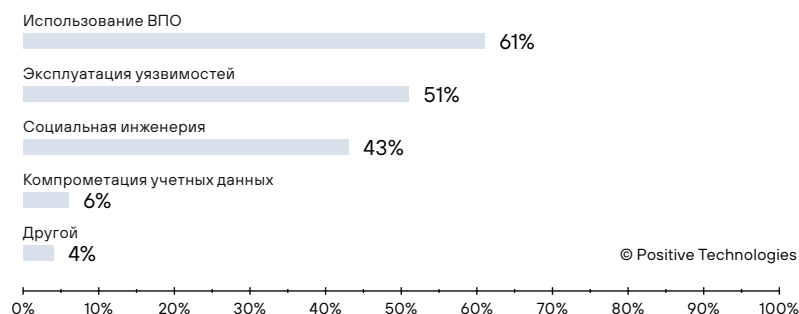


Рисунок 19. Методы атак, направленных на промышленную отрасль

В конце января жертвами кибератак стали две дочерние компании группы Marquard & Bahls — Oiltanking, немецкий дистрибьютор бензина, и Mabanaft, поставщик нефти. Предполагается, что они пострадали от атаки программы-вымогателя, а точкой взлома в обоих случаях могла стать группа компаний Marquard & Bahls. Последствия этих атак значительны не только для организаций, но и для обычных граждан: компании снабжают топливом множество заправочных станций страны, и нехватка бензина может вызвать кризис, повлияв на национальную экономику Германии. Затраты на устранение сбоев, вызванных кибератакой, также значительны: многие автоматизированные технологические процессы (например, связанные с загрузкой и разгрузкой резервуаров) полностью зависят от компьютерных систем, которые какое-то время были отключены.

Вновь оказался под ударом и энергетический сектор: в мартовском уведомлении ФБР сообщено об атаках с использованием специализированного вредоносного ПО TRITON, которое нацелено на автоматизированную систему противоаварийной защиты. Встраивание вредоносного кода может привести к повреждению объектов, простоя системы и даже к гибели людей, если система не сможет корректно инициировать процедуры безопасного отключения.

Отметим и крупные атаки на агропромышленность, произошедшие в I квартале в России: например, в марте один из крупнейших производителей и дистрибьютеров мясной продукции «Мираторг» подвергся атаке шифровальщика BitLocker, а в Ростовской области в результате атаки был временно остановлен завод «Тавр». Крупные атаки были вызваны не только шифровальщиками: в феврале злоумышленники попытались испортить 40 тонн продукции в агрохолдинге «Селятино»: получив несанкционированный доступ к системам, преступники изменили ключевые параметры, отвечающие за температурный режим хранения замороженной продукции.

Серьезные последствия вызвала и атака на Kojima Industries, японского производителя пластиковых компонентов для производства автомобилей: в результате Toyota приостановила работу 14 заводов в Японии. Судя по сообщению Kojima Industries, сбой в работе систем был также вызван программой-вымогателем.

Криптовалюты и блокчейн

Криптовалюты обретают все большую популярность. Этим пользуются злоумышленники, исследуя уязвимости криптовалютных бирж и протоколов передачи средств, а также модифицируя схемы обмана, направленные на частных лиц и криптоинвесторов.

Криптоинвесторы и владельцы криптокошельков под прицелом

Многие инфостилеры переключаются на компрометацию кошельков, реже воруют данные банковских карт. Например, исследователи Bitdefender обнаружили новое модульное ВПО BHUNT, предназначенное для кражи криптовалютных кошельков, нацеленное на их содержимое, пароли и защитные фразы.

Продолжаются атаки на криптоинвесторов: исследователи из Akamai описали действия злоумышленников, злоупотребляющих брендом Amazon, чтобы заставить потенциальных инвесторов перевести им биткоины. Также злоумышленники используют растущую популярность NFT. Например, в январе проект CryptoBatx организовал распродажу NFT через Discord-канал, но по ошибке оставил активным используемый ранее URL-адрес вместе со старыми твитами, ссылающимися на него. Мошенники установили поддельный сервер, и, переходя по легальной ссылке, пользователи вместо покупки NFT переводили деньги на кошельки преступников.

Крупные финансовые потери

В I квартале мы отметили рост атак на блокчейн-проекты и криптовалютные биржи. Более того, в марте произошла атака на сайдчейн Ronin компании Axie Infinity, которую на данный момент можно считать крупнейшим взломом. Злоумышленник попытался вывести почти 620 миллионов долларов в токенах Ethereum и USDC, получив доступ к большей части узлов валидатора, необходимых для вывода средств.

Часто после атак компании предлагают денежное вознаграждение за раскрытие найденных и проэксплуатированных уязвимостей. В январе была взломана DeFi-платформа Qubit Finance и похищено около 80 миллионов долларов в криптовалюте. Восстановить средства своими силами Qubit не могла, поэтому сначала компания отправила злоумышленнику предложение о вознаграждении за описание уязвимости, используя функцию private note транзакции. После этого Qubit дополнительно опубликовала обращение в своем аккаунте в Twitter.

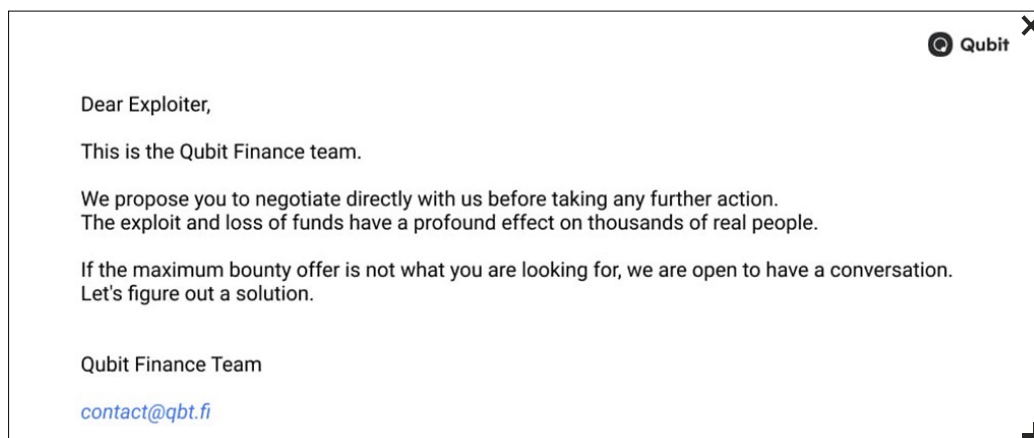


Рисунок 20. Обращение в официальном аккаунте Qubit

Другой случай связан с ошибкой в межсетевом протоколе Multichain, ущерб от эксплуатации которой составляет уже 1,5 миллиона долларов. Один из хакеров, похитивший 200 000 долларов с помощью этой уязвимости, позже заявил, что является белым хакером, и предложил вернуть 80% средств.

Атаки на разработчиков

Кража исходного кода и сертификатов для подписей

В I квартале мы смогли наблюдать крупные атаки, направленные на IT-компании: в феврале Lapsus\$ атаковали американского разработчика графических процессоров Nvidia, а в начале марта под ударом оказалась компания Samsung, был украден исходный код Samsung Galaxy.

В результате атаки на Nvidia был украден 1 ТБ данных. Группировка также опубликовала архив объемом почти 20 ГБ, содержащий, согласно сообщению, исходный код драйверов видеокарт. Позже через открытый чат Lapsus\$ стали предлагать свой инструмент для майнинга на графических процессорах компании, позволяющий обходить внутренние ограничения.

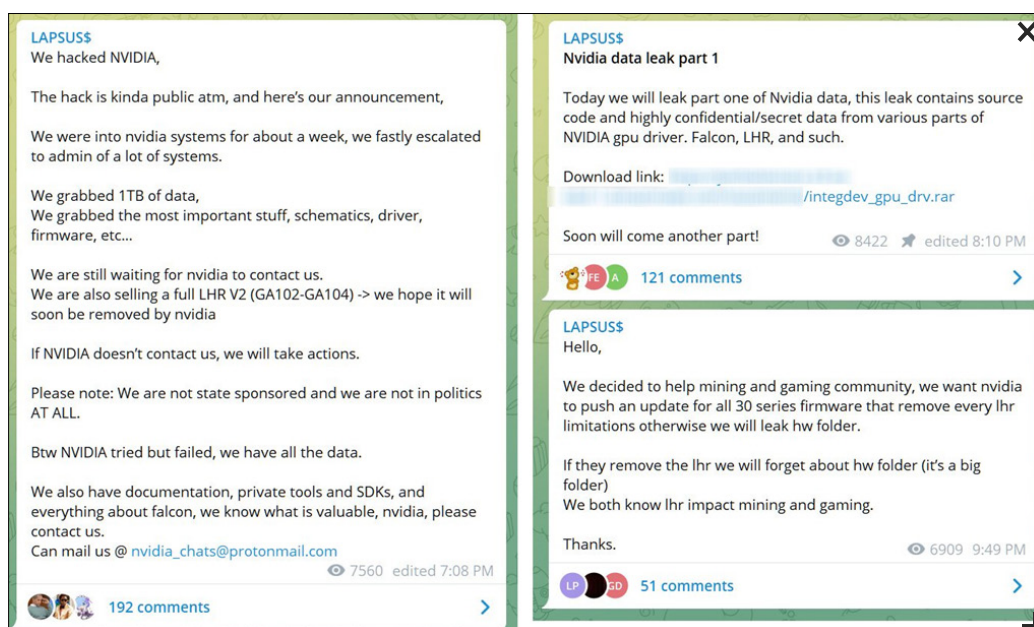


Рисунок 21. Сообщения Lapsus\$, опубликованные в телеграм-канале

И это еще не все последствия атаки: позже украденные сертификаты Nvidia использовались злоумышленниками для подписи своего ВПО, чтобы создавать видимость легитимной программы. Согласно образцам, загруженным в службу сканирования вредоносных программ VirusTotal, украденные сертификаты использовались для подписи Cobalt Strike Beacon и Mimikatz, а также различных бэкдоров и троянов удаленного доступа.

Этот случай не единственный, замеченный в I квартале. Исследователи из AhnLab обнаружили новую кампанию по распространению программы-вымогателя Magniber под видом поддельных обновлений Chrome и Firefox, подписанных действительными сертификатами Microsoft.

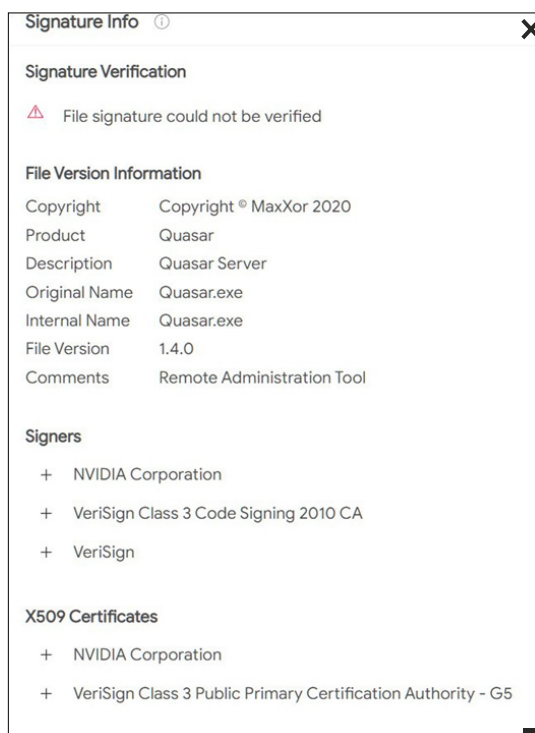


Рисунок 22. ВПО Quasar RAT, подписанное сертификатом Nvidia

ВПО в открытых библиотеках

Многих разработчиков в I квартале ждал сюрприз — массовое распространение вредоносного ПО, встроенного в коды открытых библиотек.

В марте разработчик node-ipc, популярного пакета npm, выпустил версии библиотеки, при исполнении которых на компьютерах пользователей удалялись и перезаписывались все данные. Потенциально такая атака может нанести пользователям большой ущерб: node-ipc — важный пакет, используемый основными библиотеками для разработки, который загружается более миллиона раз в неделю. Например, Vue.js, фреймворк JavaScript, также использует node-ipc в качестве зависимости, поэтому многие пользователи обратились к разработчикам проекта с просьбой привязать зависимость node-ipc к безопасной версии, после того как некоторые из систем были повреждены.

Злоумышленники часто используют тайпсквоттинг — метод атаки, при котором жертву можно обмануть с помощью пакетов, имена которых схожи с именами легитимных. Также в марте аналитики компании JFrog обнаружили 218 вредоносных пакетов, нацеленных на разработчиков npm, использующих область @azure, а также @azure-rest, @azure-tests, @azure-tools и @cadl-lang. Перечисленный набор законных пакетов загружается десятки миллионов раз каждую неделю, поэтому вероятность ошибки при печати и скачивания шпионского ПО частью пользователей является достаточно высокой.

Разработчикам важно следить за сохранением безопасности специализированных сред, предназначенных для разработки. В конце марта исследователи Aqua Security обнаружили программу-вымогатель, написанную на Python и нацеленную на тех, кто случайно оставил свою среду уязвимой из-за неправильной конфигурации Jupyter Notebook. Эта среда разработки используется для анализа и построения моделей данных, поэтому такая атака может нанести значительный ущерб организациям.

Об исследовании

Этот отчет содержит информацию об общемировых актуальных угрозах информационной безопасности, основанную на собственной экспертизе компании Positive Technologies, результатах расследований, а также на данных авторитетных источников.

По нашей оценке, большинство кибератак не передается огласке из-за репутационных рисков, поэтому подсчитать точное число угроз невозможно даже для организаций, занимающихся расследованием инцидентов и анализом действий хакерских групп. Наше исследование проводится для того, чтобы привлечь внимание компаний и обычных граждан, интересующихся современным состоянием информационной безопасности, к наиболее актуальным методам и мотивам кибератак, а также чтобы выявить основные тенденции в изменении ландшафта киберугроз.

В рамках отчета каждая массовая атака (в ходе которой злоумышленники проводят, например, фишинговую рассылку на множество адресов) рассматривается как одна атака, а не как несколько атак. Термины, которые мы используем в исследовании, приведены в словаре терминов ИБ на сайте Positive Technologies.