



Актуальные киберугрозы

IV квартал 2019 года

Содержание

Обозначения	3
Резюме	4
Сводная статистика	5
Динамика атак	9
Методы атак	10
Использование вредоносного ПО	10
Социальная инженерия	11
Хакинг	12
Эксплуатация веб-уязвимостей	13
Подбор учетных данных	13
Категории жертв	14
Государственные организации	15
Промышленные компании	18
Финансовые организации	20
IT-компании	22
Торговля	23
Как защититься организации	26
Как вендору защитить свои продукты	28
Как защититься обычному пользователю	29
Об исследовании	30
Краткое описание группировок	31

Обозначения

Объекты атак



Компьютеры, серверы
и сетевое оборудование



Веб-ресурсы



Люди



Банкоматы и POS-терминалы



Мобильные устройства



IoT

Методы атак



Использование
вредоносного ПО



Подбор учетных данных



Социальная инженерия



Хакинг



Эксплуатация
веб-уязвимостей

Категории жертв



Финансовая отрасль



Государственные учреждения



Медицинские учреждения



Наука и образование



Оборонные предприятия



Промышленные компании



Онлайн-сервисы



Сфера услуг



Транспорт



IT-компании



Торговля



Частные лица



Телекоммуникационные
компании



Блокчейн-проекты



Другие сферы

Резюме

По итогам IV квартала 2019 года мы отмечаем:

- Количество уникальных киберинцидентов растет: зафиксировано на 12% больше кибератак, чем в III квартале года.
- Доля целенаправленных атак выросла на 2 п. п. по сравнению с III кварталом и составила 67%. Это связано с большим числом АРТ-атак против отдельных организаций и целых отраслей.
- Высокую активность проявляли 11 АРТ-группировок, их кампании были направлены преимущественно на государственные учреждения, промышленные предприятия и финансовую отрасль.
- Треть украденной у юридических лиц информации (32%) составили данные платежных карт, что на 25 п. п. больше, чем в III квартале. Мы связываем такой рост, с одной стороны, с традиционно высокой покупательской активностью в предновогодний период, а с другой — с прогрессивным увеличением числа атак MageCart и второй волной атак на сервис Click2Gov.
- Атаки шифровальщиков представляют высокую опасность. Их доля в числе заражений вредоносным ПО составила 36% для юридических лиц и 17% для частных лиц против 27% и 7% в III квартале соответственно.
- Публикация похищенной информации в ответ на отказ платить выкуп — новый тренд, заданный операторами шифровальщиков. Мы связываем это с тем, что все больше организаций делают резервные копии и не платят за расшифрование. Злоумышленники приняли контрмеры и теперь шантажируют жертв возможными санкциями за утечку персональных данных, обращение с которыми регулируется нормами Общего регламента по защите данных (GDPR).

Сводная статистика

В последнем квартале 2019 года соотношение долей атак, направленных на кражу информации, и атак с прямой финансовой выгодой практически не изменилось и осталось на уровне III квартала.

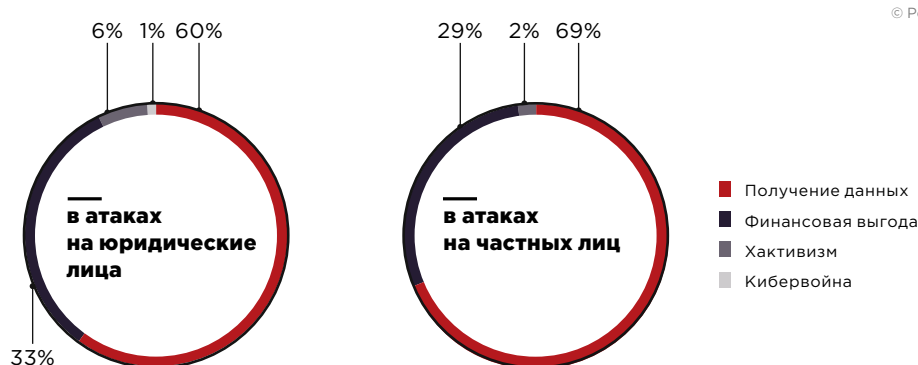


Рисунок 1. Мотивы злоумышленников

В IV квартале данные платежных карт составили треть (32%) от всего объема информации, похищенной у юридических лиц, что в несколько раз больше, чем в III квартале (7%). Такой рост ожидаем. С одной стороны, он объясняется большим числом интернет-покупок в период новогодних праздников. С другой стороны, мы связываем его со стремительным увеличением доли массовых атак MageCart, затронувших тысячи интернет-магазинов, и второй волной атак на сервис Click2Gov, который жители многих американских городов используют для коммунальных платежей.

Доля атак на частных лиц сократилась почти вдвое по сравнению с III кварталом и составила лишь 10% всех атак. Как и в III квартале, учетные данные составляют почти половину (40%) всего объема украденной у частных лиц информации. Один из распространенных способов выманивания у пользователей учетных данных — это фишинговые письма со ссылками на поддельные страницы авторизации. Однако ссылку могут заблокировать средства защиты электронной почты, поэтому злоумышленники придумывают новые схемы. Например, вместо ссылки к письму прикладывается файл в формате HTML — якобы платежный документ. При открытии этого файла сценарий на JavaScript генерирует форму аутентификации прямо в браузере пользователя, не вызывая подозрений перенаправлением на сторонний сайт. После ввода учетных данных скрипт отправляет их злоумышленникам.

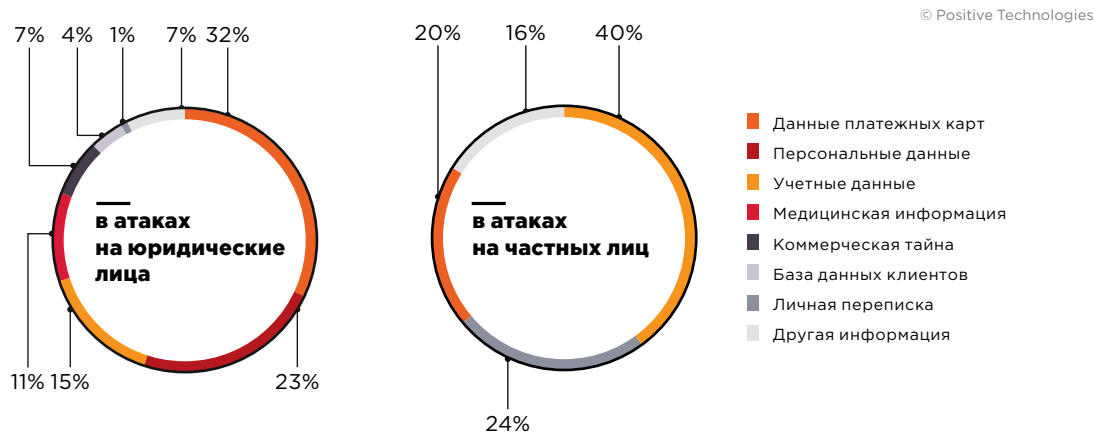


Рисунок 2. Типы украденных данных

Высокая доля целевых атак сохраняется. Две трети атак (67%) носили целенаправленный характер: злоумышленники атаковали выборочные компании, представляющие для них интерес, либо интересующую их отрасль в целом. Как следствие, снизилась доля атак без привязки к отрасли — с 26% в начале 2019 года до 14% в конце.

В пятерке самых атакуемых отраслей по-прежнему остаются госучреждения, промышленность, здравоохранение, финансы и образование. В то же время мы отмечаем двукратный рост доли атак на IT-компании и сферу торговли. Далее мы рассмотрим наиболее громких из них.

Доля атак, направленных на блокчейн-проекты, на протяжении года снижалась и приблизилась к 1%, тем не менее владельцы криптокошельков по-прежнему под угрозой. Так, в IV квартале был скомпрометирован сайт криптовалюты Monero. Злоумышленники разместили на нем вредоносное ПО под видом легитимного криптокошелька. Сообщается, что один из пользователей потерял в результате этой атаки 7000 долл. США.

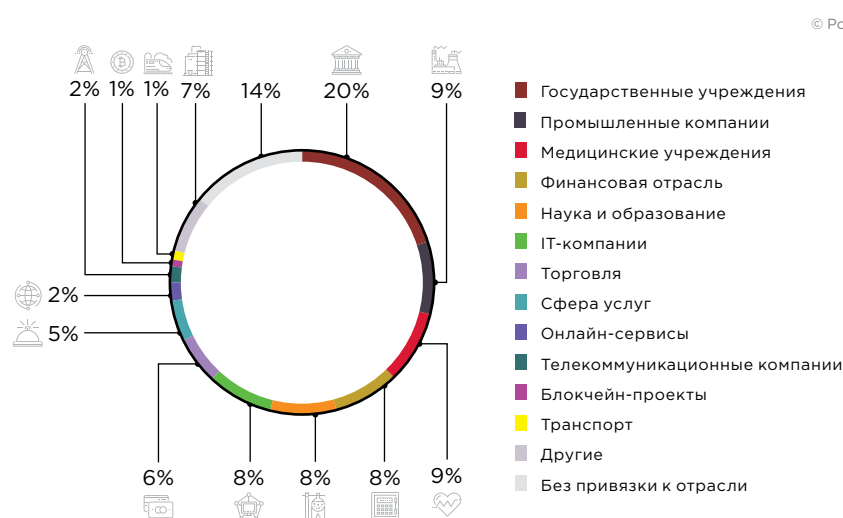


Рисунок 3. Категории жертв среди юридических лиц

Почти в четверти случаев (23% атак) источником угрозы для частных лиц стали их мобильные устройства. Пользователи гаджетов могут сами помогать злоумышленникам, скачивая на смартфоны сомнительные программы. Так, в IV квартале ряд владельцев устройств Apple, искавших способы повысить привилегии (выполнить jailbreak), стали жертвами кибермошенников. Осенью 2019 года в открытом доступе появилась утилита checkra1n, которая путем эксплуатации аппаратной уязвимости позволяет повышать привилегии на всех смартфонах iPhone до десятой модели включительно, а также на ряде моделей iPad. Работа checkra1n не зависит от версии iOS, поэтому jailbreak быстро набрал популярность как среди исследователей безопасности мобильных устройств, так и среди обычных пользователей. Отметим, что мы настоятельно не рекомендуем пользователям делать jailbreak, поскольку повышение привилегий приводит к снижению уровня защищенности устройства от вредоносного ПО. Популярностью checkra1n не преминули воспользоваться кибермошенники. Исследователи Cisco Talos выявили поддельный веб-сайт checkra1n[.]com, где под видом утилиты checkra1n распространялся вредоносный сертификат (файл с расширением .mobileconfig). После его установки и запуска имитировалась процедура jailbreak, якобы для завершения которой пользователям предлагалось загрузить на устройство ряд мобильных приложений: таким образом поддельный checkra1n помогал злоумышленникам рекламировать данные приложения и повышать число их загрузок.

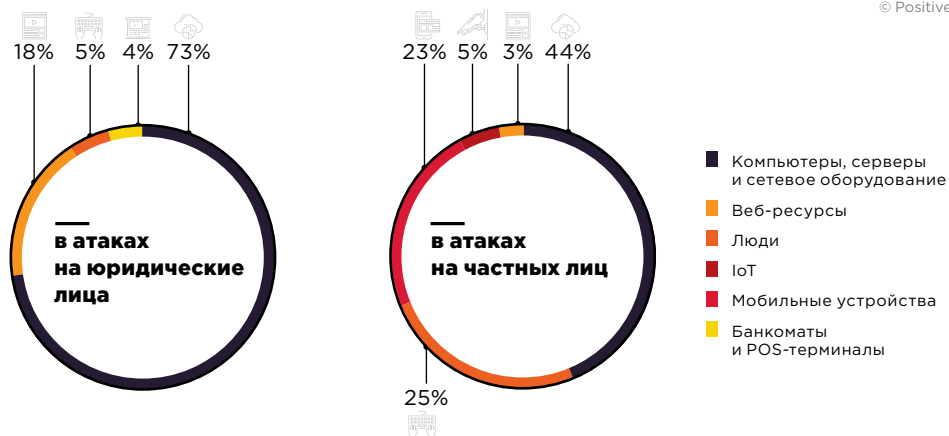


Рисунок 4. Объекты атак

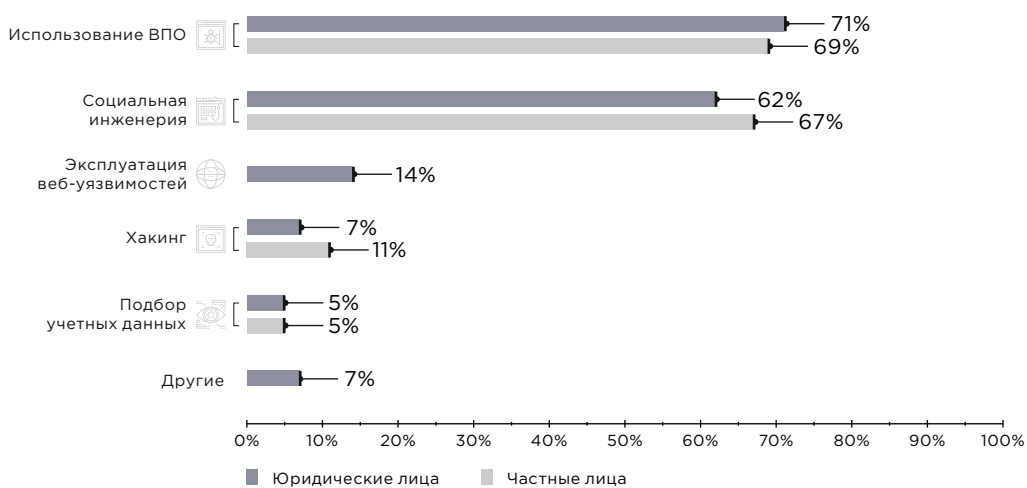
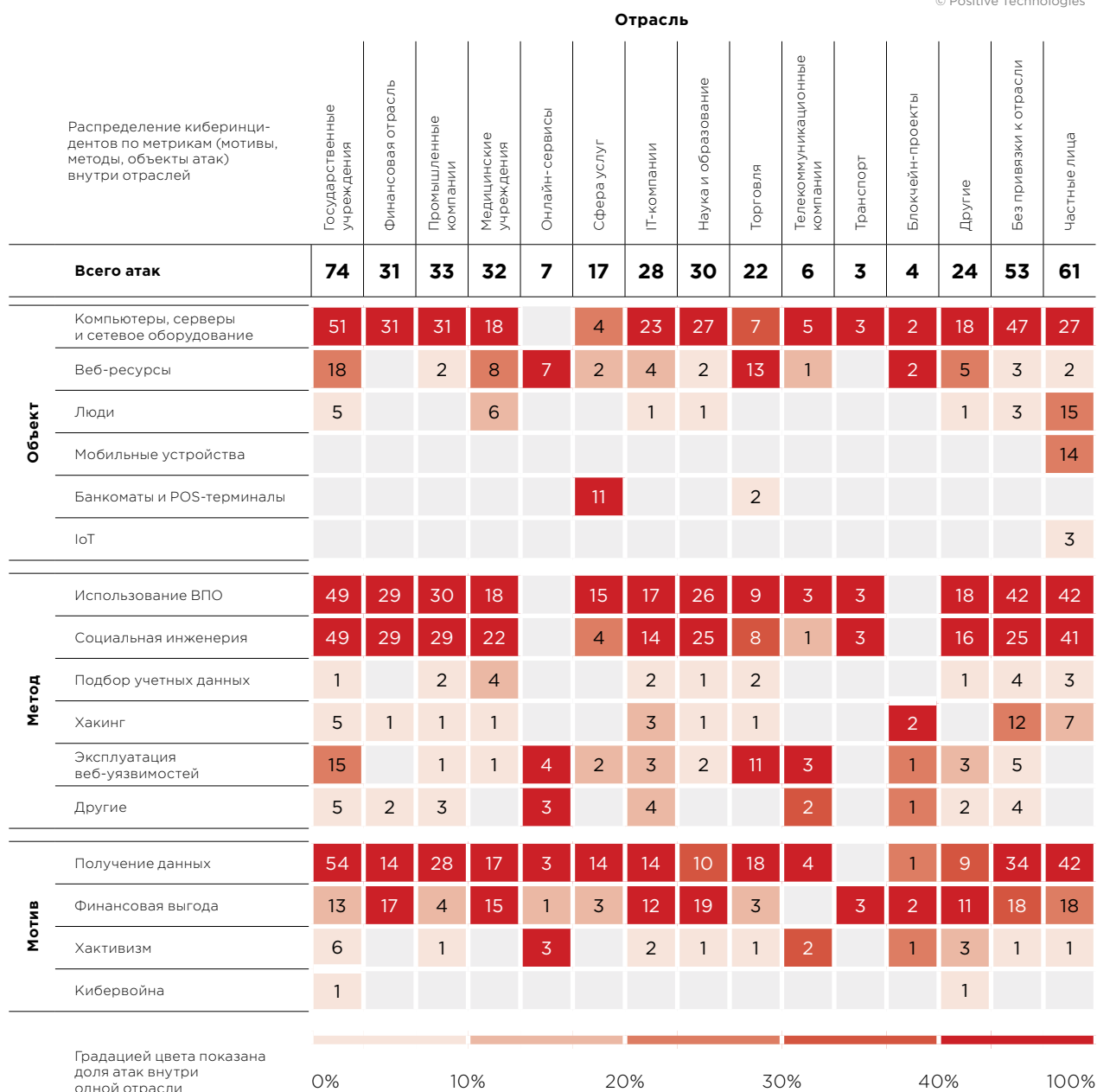


Рисунок 5. Методы атак



Динамика атак

© Positive Technologies

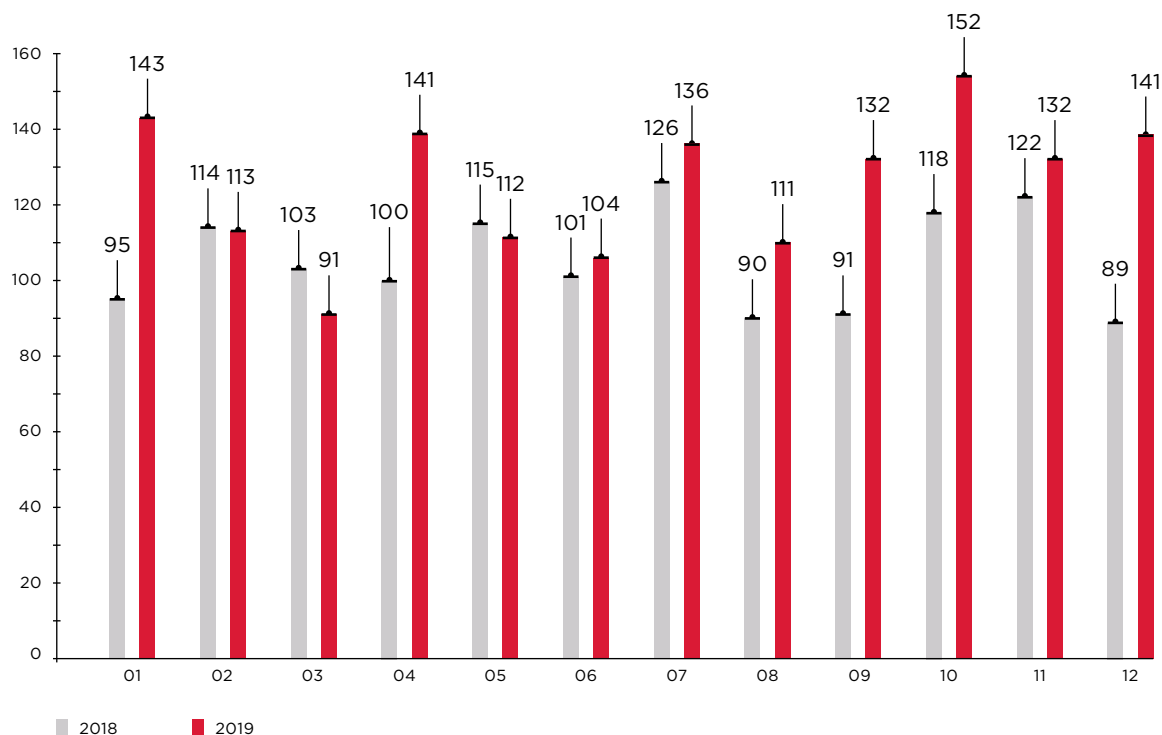


Рисунок 6. Количество инцидентов в 2018 и 2019 годах (по месяцам)

© Positive Technologies

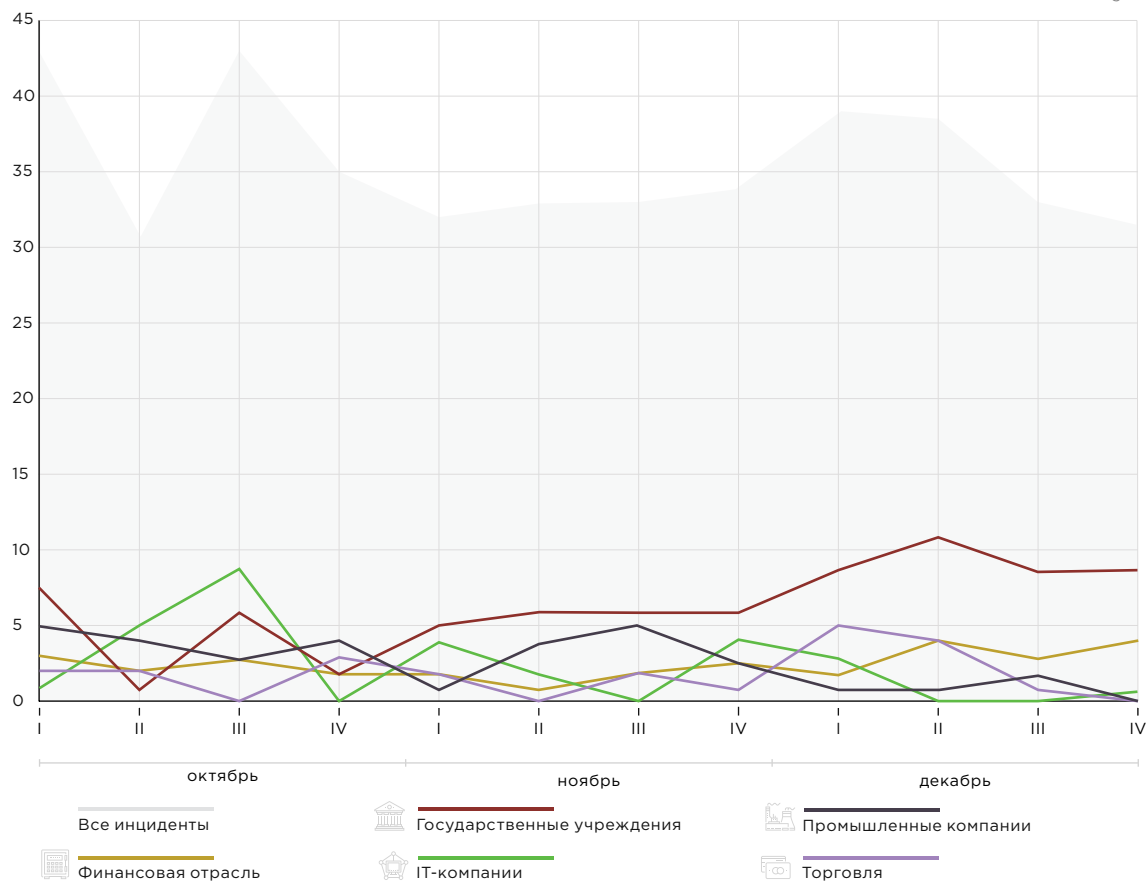


Рисунок 7. Количество инцидентов в IV квартале 2019 года (по неделям)

Методы атак

Рассмотрим подробнее методы атак, которые используют злоумышленники, на примере самых громких киберинцидентов IV квартала 2019 года.

Использование вредоносного ПО

Шифровальщики атакуют организации по всему миру. В IV квартале их жертвами стали организации из самых разных отраслей: школы, медицинские учреждения, промышленные предприятия, государственные организации, IT-компании. Наиболее агрессивные атаки проводят операторы шифровальщиков Sodinokibi, Maze, Ryuk и Bitpaymer. Только в Испании жертвами последних двух стали по меньшей мере три компании: консалтинговая фирма Everis, радиоккомпания Cadena SER и производственная компания TECNOL.

Все больше компаний признают угрозу троянов-вымогателей и начинают внимательно следить за наличием резервных копий на случай атаки, поэтому операторы шифровальщиков ищут новые способы вынудить компании-жертвы заплатить выкуп. Операторы Maze копируют чувствительные данные перед их шифрованием на свои серверы, после чего шантажируют жертву публикацией этих данных в открытом доступе в случае отказа платить. Жертвами таких атак уже стали компании Allied Universal, от которой потребовали выкуп в 300 биткойнов, и Southwire, данные которой оценили в 850 биткойнов. В обоих случаях компании не заплатили выкуп, и злоумышленники привели свои угрозы в исполнение: файлы атакованных компаний оказались в сети.

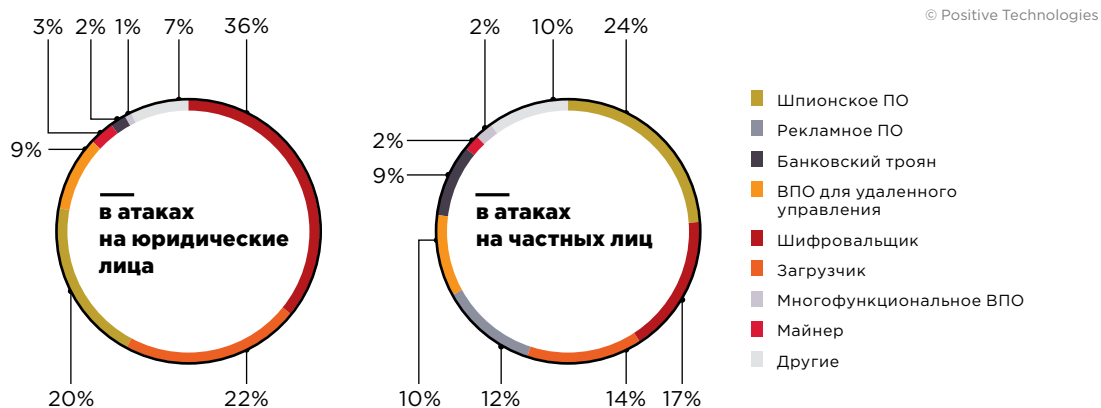


Рисунок 8. Типы вредоносного ПО

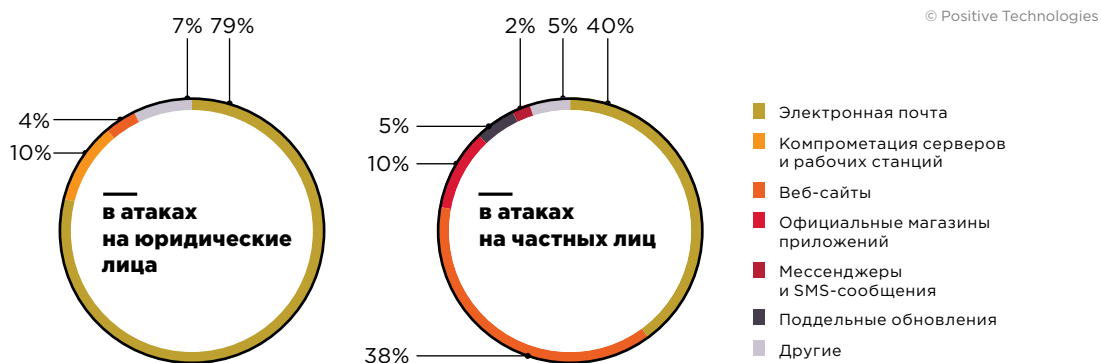


Рисунок 9. Способы распространения ВПО

Большинство (79%) заражений юридических лиц вредоносным ПО начинались с фишинговых писем. Такие письма могут как попасть в организацию в ходе массовых атак, так и быть отправлены специально для нее. Точечные рассылки, как правило, проводят APT-группы. В рамках мониторинга и исследования угроз информационной безопасности на протяжении IV квартала эксперты Positive Technologies Expert Security Center (PT ESC) фиксировали атаки APT-группировок TA505, Sofacy (APT28), Donot (APT-C-35), Cloud Atlas, Bronze Union (LuckyMouse, APT27), Leviathan (APT40), Bisonal, Gamaredon, SongXY, Cobalt, RTM. Некоторые из этих группировок рассылают вредоносные документы с убедительным текстом-заглушкой. Например, группа Cloud Atlas в своих атаках использовала текст на русском языке, посвященный геополитическому противостоянию между Китаем и США в области искусственного интеллекта.

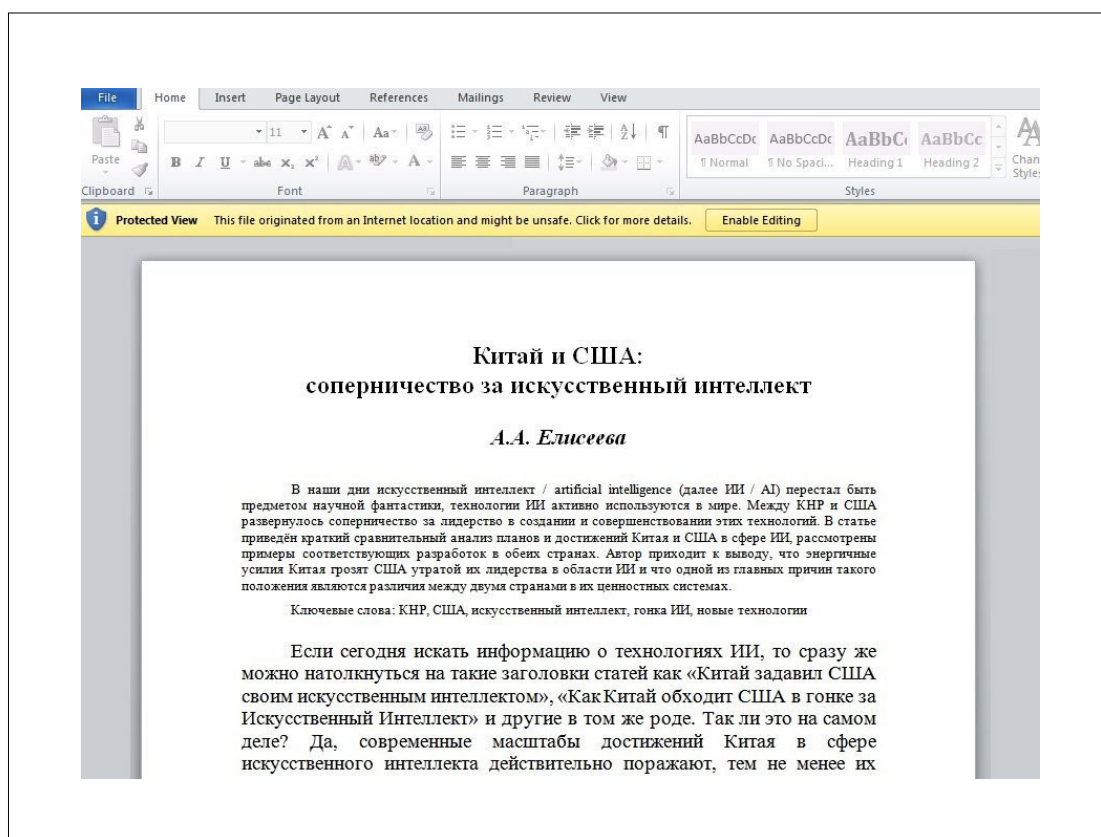


Рисунок 10. Фрагмент документа из рассылки Cloud Atlas

Социальная инженерия

Злоумышленники часто манипулируют эмоциями людей для успешной доставки вредоносного ПО, например в электронных письмах. В IV квартале 2019 года социальная инженерия в сочетании с ВПО использовалась в 54% атак. Пользователям стоит быть особенно внимательными к электронной корреспонденции в период праздников. К знаменательным датам злоумышленники приурочивают фишинговые рассылки. Например, ко Дню благодарения в США киберпреступники разослали письма якобы с поздравительными открытками. В действительности же вложения к письмам были вредоносными — доставляли на компьютеры жертв Emotet и другое вредоносное ПО. Массовые рассылки писем якобы с приглашениями на вечеринку, доставляющих во вложениях Emotet, были приурочены также к Хэллоуину и Рождеству.

Если вы не переходите по подозрительным ссылкам и не загружаете сомнительные вложения, это еще не означает, что вы не можете попасть на удочку интернет-мошенников. Так, в IV квартале злоумышленники использовали для фишинговых атак особенности Microsoft OAuth API. Протокол OAuth позволяет выдавать сторонним приложениям токен на доступ без знания учетных данных. Суть атаки в следующем. Фишинговое письмо содержит ссылку на файл якобы в OneDrive или SharePoint. Однако после перехода по ссылке и ввода учетных данных пользователь видит форму с запросом на предоставление доступа к аккаунту Office 365. Если жертва невнимательна, она может предоставить запрашиваемые права одним кликом. В результате злоумышленники получают список контактов, файлы и личную переписку.

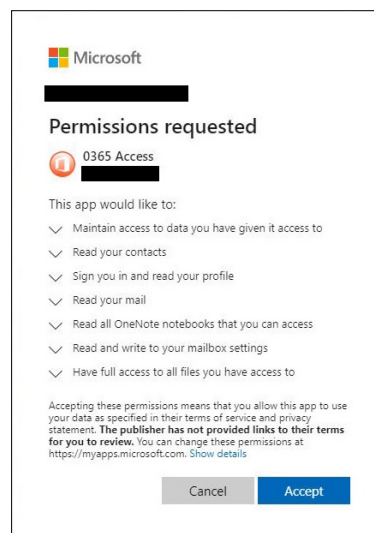


Рисунок 11. Запрос от фишингового приложения 0365 Access

Письма, в которых злоумышленники шантажируют жертв разглашением якобы имеющегося у них компромата, — далеко не новый способ незаконного заработка, однако он по-прежнему приносит киберпреступникам немалый доход. Например, по оценке специалистов Check Point, за пять месяцев операторы ботнета Phorpiex, рассылающего подобные письма, заработали около 115 тысяч долл. США. Злоумышленники включают в текст письма пароли жертв как доказательство компрометации. Мошенники берут их из утекших в интернет баз данных. Плату за неразглашение компрометирующих материалов, как правило, требуют заплатить в биткойнах. Однако специалисты компании Cofense отмечают, что вымогатели все чаще просят выкуп в альтернативной валюте, например в лайткойнах (LTC), чтобы обойти средства защиты электронной почты, которые блокируют письма с адресами биткойн-кошельков для противодействия подобного рода вымогательствам. С этой же целью некоторые злоумышленники вставляют в письма адрес биткойн-кошельков в виде QR-кодов.

Хакинг

Уязвимость CVE-2019-0708 (известная также как BlueKeep) теперь используется в реальных атаках для доставки майнеров. Однако мы не исключаем, что в будущем эта брешь может использоваться злоумышленниками и в других кампаниях, в том числе в APT-атаках.

В октябре эксперты компании Wallarm сообщили об уязвимости в PHP 7 (CVE-2019-11043), позволяющей выполнять произвольные команды на серверах nginx с поддержкой PHP-FPM. Производитель облачного хранилища NextCloud, клиенты которого оказались под угрозой, опубликовал инструкции, как защититься от новой угрозы. Однако не все администраторы NextCloud своевременно приняли меры защиты, и спустя непродолжительное время стали поступать сообщения об атаках шифровальщика NextCry. Вредонос целенаправленно заражает серверы NextCloud, уязвимые для CVE-2019-11043. Поскольку брешь новая, NextCry на момент первых атак не детектировался ни одним антивирусом, что и обусловило заражения.

Хакинг может сочетаться с методами социальной инженерии, например если речь идет об уязвимостях в браузерах. В ноябре стало известно, что злоумышленники активно используют брешь в Mozilla Firefox для атак, в которых выдают себя за техподдержку. Пользователя уязвимого браузера заманивают на подконтрольный злоумышленникам веб-ресурс (например, посредством фишинговых писем). После перехода пользователя на этот ресурс браузер блокируется всплывающим окном с текстом о том, что для продолжения работы якобы необходимо обратиться в техподдержку либо купить какое-то ПО. Способ не новый, но он по-прежнему работает.

Эксплуатация веб-уязвимостей

Веб-ресурсы продолжают быть мишенями для атак хактивистов. Власти американского штата Огайо сообщают, что злоумышленники атаковали систему электронного голосования в день выборов, 5 ноября, попытавшись выполнить внедрение SQL-кода.

Привлекают злоумышленников и веб-сайты коммерческих организаций. Взламывая их, злоумышленники рассчитывают на базы данных клиентов, данные платежных карт и учетные данные зарегистрированных на сайте пользователей. Если атака успешна и чувствительная информация похищена, добросовестная компания-жертва вынуждена уведомить пострадавших пользователей и принять меры для предотвращения успешных атак в будущем. Так, в IV квартале производитель смартфонов OnePlus после инцидента с утечкой персональных данных клиентов интернет-магазина был вынужден вступить в программу bug bounty, заключив партнерство с HackerOne. Утечка произошла из-за веб-уязвимости, подробности которой не разглашаются.

Веб-уязвимости могут использоваться и для проведения атак, направленных на отказ в обслуживании сетевого оборудования (DoS-атак). Специалисты Cisco сообщают, что зафиксировали всплеск попыток эксплуатации уязвимости CVE-2018-0296 в веб-интерфейсе управления межсетевыми экранами Cisco Adaptive Security Appliance и Firepower Appliance. Уязвимость позволяет удаленно без авторизации перезагружать атакуемые устройства, посылая специальные HTTP-запросы, а также читать системную информацию, используя технику directory traversal. О бреши стало известно еще в середине 2018 года, но она до сих пор остается «рабочей лошадкой» для злоумышленников.

Подбор учетных данных

Злоумышленники ищут доступные в интернете сетевые устройства со слабыми паролями, чтобы установить на эти устройства ВПО и включить их в ботнет для майнинга криптовалюты или распределенных DoS-атак. Новый ботнет Mozi находит в сети маршрутизаторы Netgear, D-Link и Huawei со слабыми паролями к службе Telnet и заражает их вредоносным ПО. Ботнет Muhstik нацелен на маршрутизаторы с прошивкой Tomato, у которых установлен пароль по умолчанию admin.

Существуют и другие способы, как злоумышленники распоряжаются списками учетных данных, полученными в ходе массовых брутфорс-атак. Один из них — продажа в дарквебе, но иногда злоумышленники публикуют базы учетных данных на безвозмездной основе. Владелец одного из сервисов для проведения заказных атак на отказ в обслуживании (DDoS for hire) выложил в свободный доступ на хакерском форуме список учетных данных для службы Telnet более чем для 515 тысяч серверов, маршрутизаторов и IoT-устройств, объяснив свой поступок тем, что он отказался от ботнетов и перешел на аренду высокопроизводительных серверов у облачных провайдеров.

Категории жертв



Далее мы подробно проанализируем атаки на отдельные отрасли, которые нам показались наиболее интересными в IV квартале 2019 года.

Государственные организации

© Positive Technologies

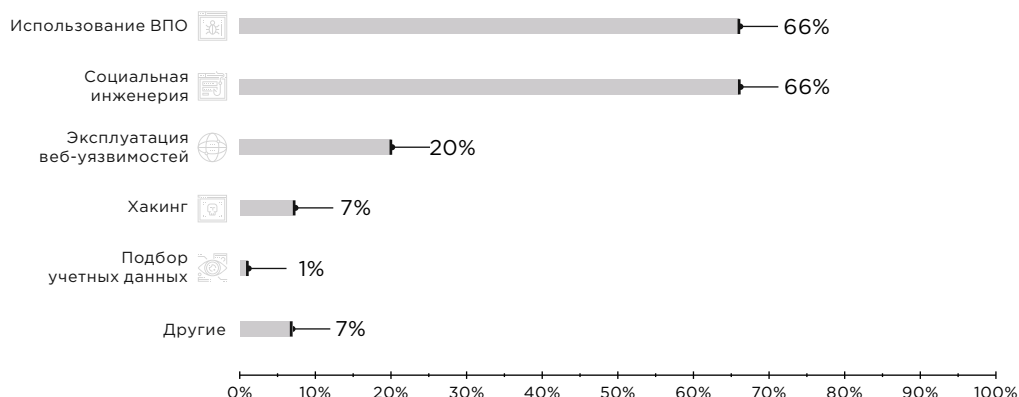


Рисунок 12. Методы атак на государственные организации в Q4 2019

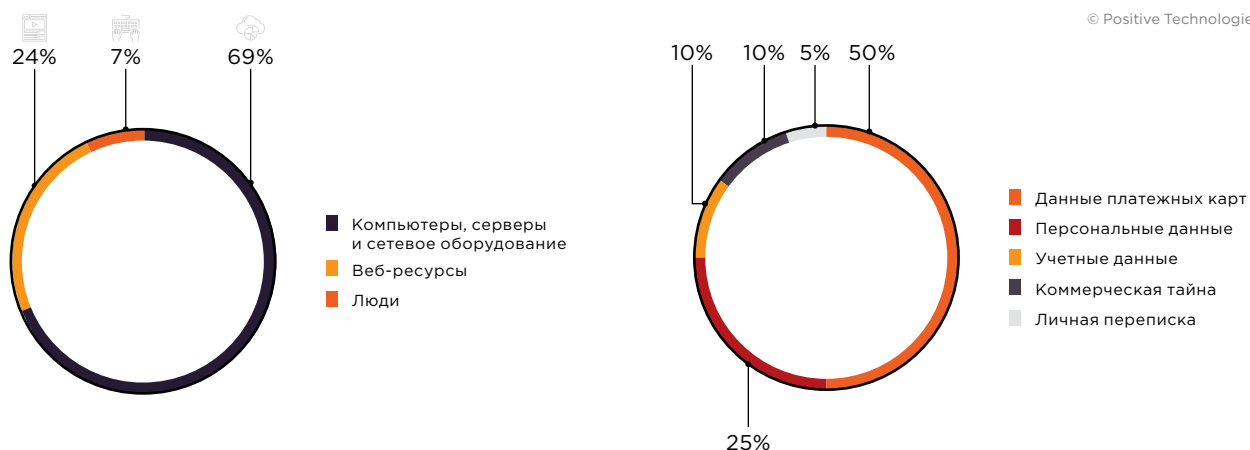


Рисунок 13. Объекты атак

Рисунок 14. Украденные данные

По США прокатилась волна атак на сервис Click2Gov. Год назад мы уже подробно [писали](#) о них. В IV квартале 2019 года атаки повторяются: администрации восьми городов заявили, что граждане, оплачивавшие коммунальные услуги через данный сервис в период примерно с конца августа по ноябрь, стали жертвами злоумышленников.



Рисунок 15. География жертв атак на портал Click2Gov (желтый — первая волна атак, синий — новая волна атак)

Государственные учреждения по-прежнему под прицелом АPT-групп. В IV квартале продолжа-
ется активность АPT-группы Gamaredon. Специалисты РТ ESC в ходе мониторинга актуальных угроз в течение ноября и декабря 2019 года зафиксировали 17 атак группы, направленных на го-
сударственные учреждения и военно-промышленный комплекс Украины. Киберпреступники изменили способ доставки полезной нагрузки. В предыдущих атаках группа рассылала доку-
менты с макросами. В конце года киберпреступники использовали технику template injection, ко-
торая позволяет обходить средства антивирусной защиты. При таком способе документ не со-
держит ни OLE-объектов, ни макросов. Вместо этого в него встроена ссылка на вредоносный документ-шаблон, который автоматически загружается с сервера злоумышленников. Этот доку-
мент содержит макрос, который сохраняет в каталог автозагрузки вредоносный скрипт на языке Visual Basic (VBScript). Кроме того, макрос модифицирует значение в реестре, которое отвечает за предупреждение пользователя при исполнении макроса. После этой модификации все доку-
менты, содержащие макрос, исполняются автоматически.

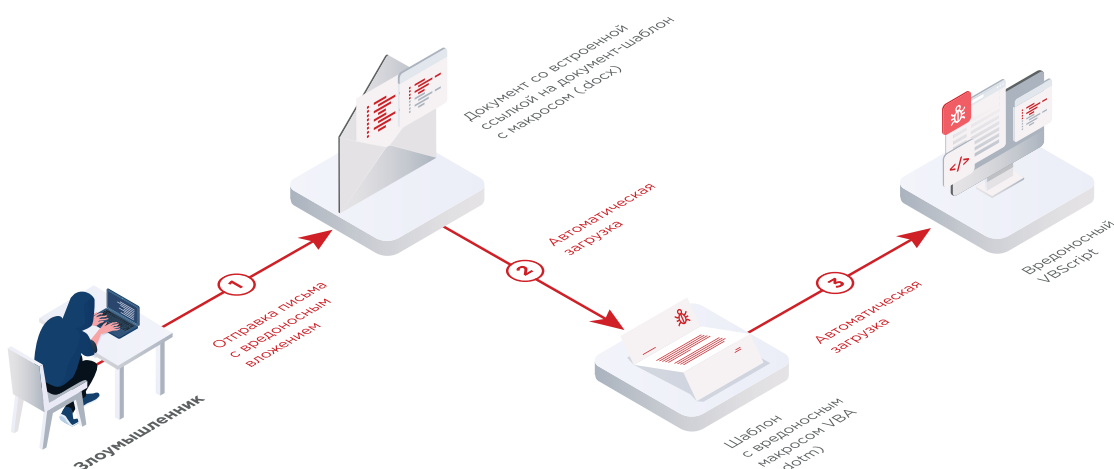


Рисунок 16. Схема заражения template injection, использованная в атаках Gamaredon



Рисунок 17. Документы из писем Gamaredon со встроенной ссылкой на документ-шаблон с макросом

В декабре специалисты PT ESC в ходе мониторинга обнаружили следы трех атак группы Bisonal против государственных учреждений Монголии, Южной Кореи и России. Во вредоносных рассылках группа использовала документы в формате RTF с эксплойтом для уязвимости [CVE-2018-0798](#). Документы были сгенерированы с помощью билдера под названием 8.t, который используют и другие APT-группы — Goblin Panda, IceFog, SongXY.

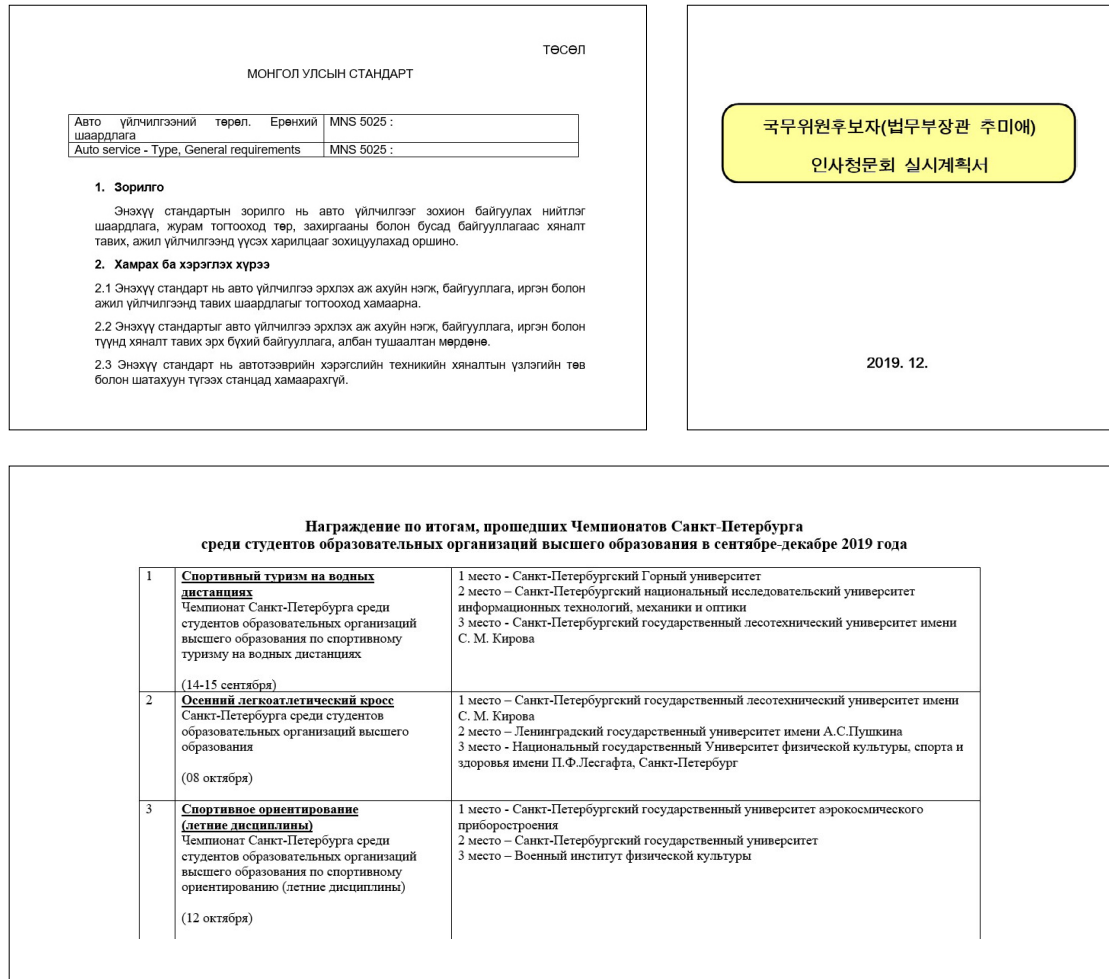


Рисунок 18. Примеры документов из рассылок группы Bisonal

Государственные учреждения атакует также группа SongXY. В PT ESC зафиксировали три атаки в течение квартала — две на украинские госучреждения и одну атаку на Россию. Как и Bisonal, группа SongXY использовала документы в формате RTF с эксплойтом для уязвимости [CVE-2018-0798](#). Вложения сгенерированы с помощью билдера 8.t.

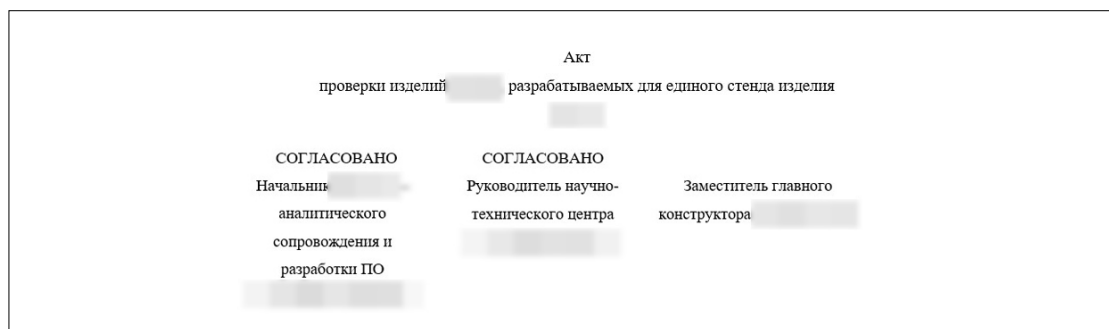


Рисунок 19. Пример вредоносного вложения группы SongXY

Службові номери керівництва України

Структурний підрозділ	Прізвище, ім'я, по-батькові	Телефон
Директор		(приймальня)
Перший заступник Директора		відсутній
Заступник Директора		(приймальня)
Заступник Директора		відсутній
Заступник Директора		(приймальня)
Заступник Директора		(приймальня)
Головний підрозділ детективів		
Керівник Головного підрозділу детективів		(приймальня)

**Розпорядження N 2098-р Директора від 26 листопада 2019 року
вакансія конкурсного оголошення про вакансії**

ЗАТВЕРДЖУЮ
Директор
(найменування посади, ініціали (ім'я), прізвище та підпис керівника державної служби у державному органі)

«26» листопада 2019 року

Розпорядженням Директора
2019 року № 2098-р оголошено конкурс на зайняття вакантних посад в
України (далі –).

Рисунок 20. Примеры вредоносных вложений группы SongXY

Промышленные компании

© Positive Technologies

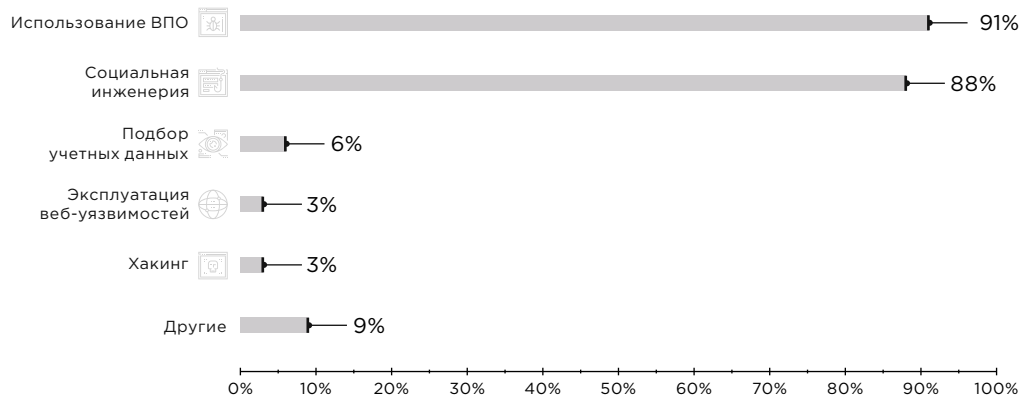


Рисунок 21. Методы атак на промышленные компании в Q4 2019

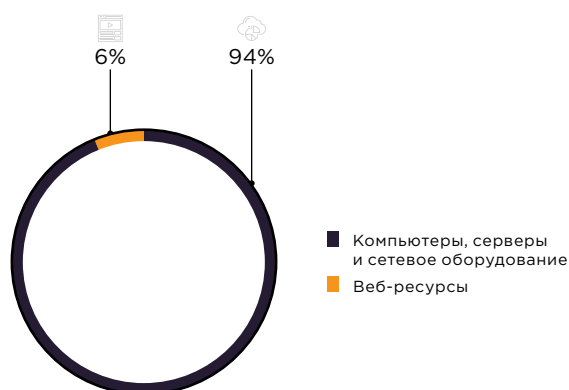


Рисунок 22. Объекты атак

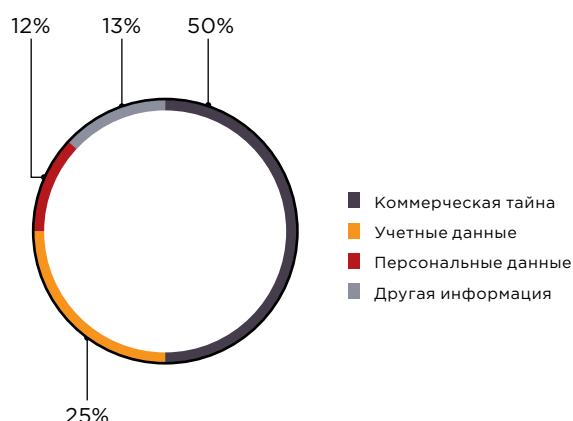


Рисунок 23. Украденные данные

Группа RTM по-прежнему активно атакует промышленные компании России и СНГ. Однако в списке адресатов их вредоносных рассылок числятся также государственные учреждения, банки и организации сферы науки и образования. Всего в течение IV квартала специалисты PT ESC зафиксировали 25 атак этой группы. Напомним, что с июня 2019 года группа RTM стала вычислять IP-адрес сервера с помощью логических операций над суммой транзакции, полученной на определенный кошелек Bitcoin. В середине декабря 2019 года группа RTM внесла небольшие изменения в алгоритм получения IP-адреса. Теперь в каждом образце ВПО присутствуют два номера кошельков Bitcoin и в вычислениях задействуются последние исходящие транзакции с первого кошелька на второй. Внесенное изменение практически не затронуло код, однако позволило злоумышленникам защититься от подмены адресов контрольных серверов для своего ВПО.

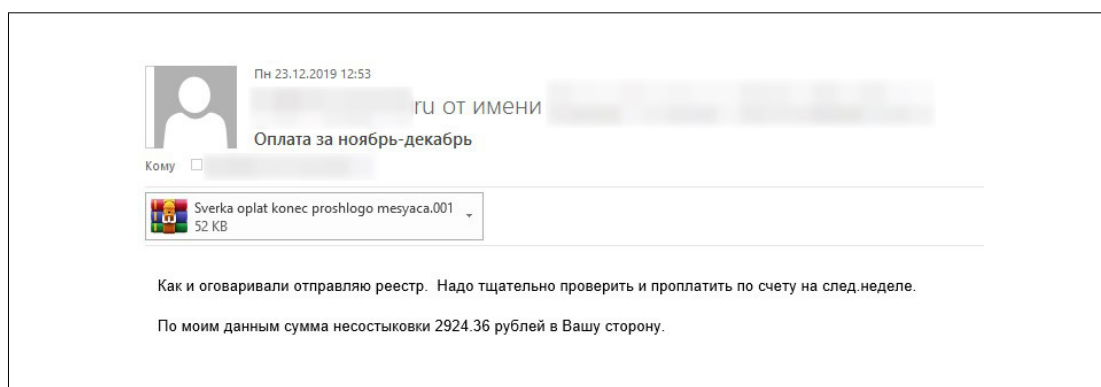


Рисунок 24. Фишинговое письмо группы RTM в адрес промышленной компании

В течение IV квартала, помимо России и СНГ, АPT-атакам подвергались промышленные компании США, Южной Кореи, Японии, Индонезии, Турции, Германии. Эксперты из команды Section 52 компании CyberX обнаружили целенаправленные атаки на промышленность, в ходе которых злоумышленники рассылали фишинговые письма, доставляющие инфостилер Seara, который, по мнению специалистов, может использоваться для кражи интеллектуальной собственности и паролей для доступа к промышленным системам.

Промышленные компании также активно атакует кибергруппировка APT33. Отличительная черта атак этой группы — техника password spraying, то есть опробование нескольких слабых паролей в атаках на большое число учетных записей. На конференции CyberwarCon эксперт Microsoft представил результаты мониторинга деятельности APT-группы. По наблюдению специалистов, в последние месяцы киберпреступники сократили число атакуемых организаций до двух тысяч, на порядок увеличив число учетных записей, которые они пытаются взломать в каждой из этих организаций.

Финансовые организации

© Positive Technologies

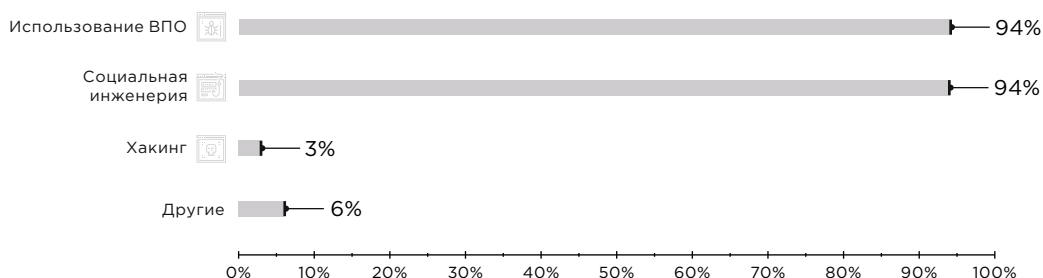


Рисунок 25. Методы атак на финансовые организации в Q4 2019

В IV квартале специалисты PT ESC зафиксировали 12 рассылок группировки Cobalt в адрес финансовых организаций.

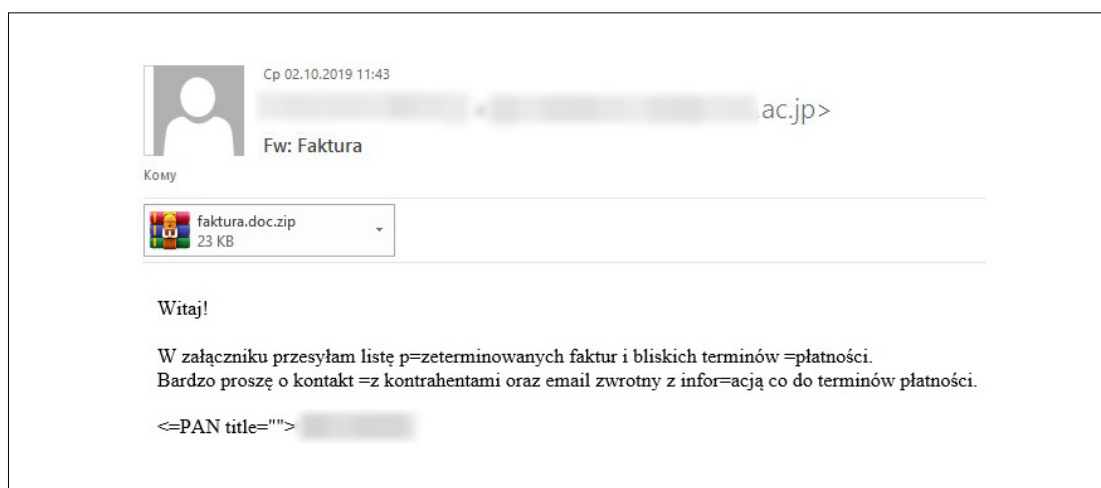
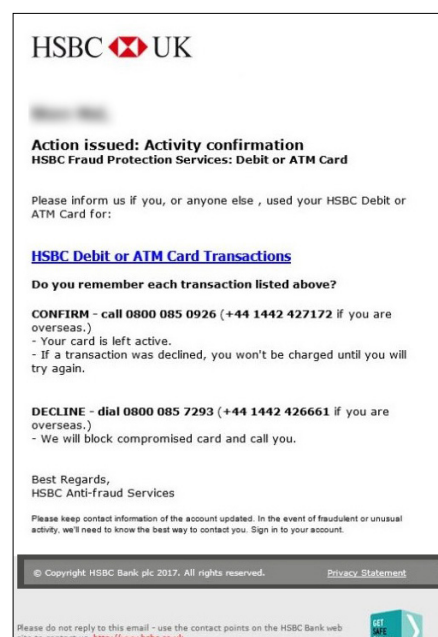


Рисунок 26. Фишинговое письмо группы Cobalt

Злоумышленники используют вредоносные вложения разных типов — документы в формате RTF с эксплойтами, офисные документы с макросами, а также файлы в формате VHD (Virtual Hard Drive). Последний является новым форматом для вредоносных рассылок Cobalt. Он эффективен только для Windows версий 7 и выше. При открытии файла в формате VHD он автоматически монтируется в систему как диск, после чего в «Проводнике Windows» открывается вредоносное содержимое, а пользователю остается лишь запустить его. В качестве полезной нагрузки в IV квартале группа использовала CoolPlants, CobInt, COM-DLL-Dropper и JScript-бэкдор.

Рисунок 27. Изображение из вредоносного вложения в формате VHD



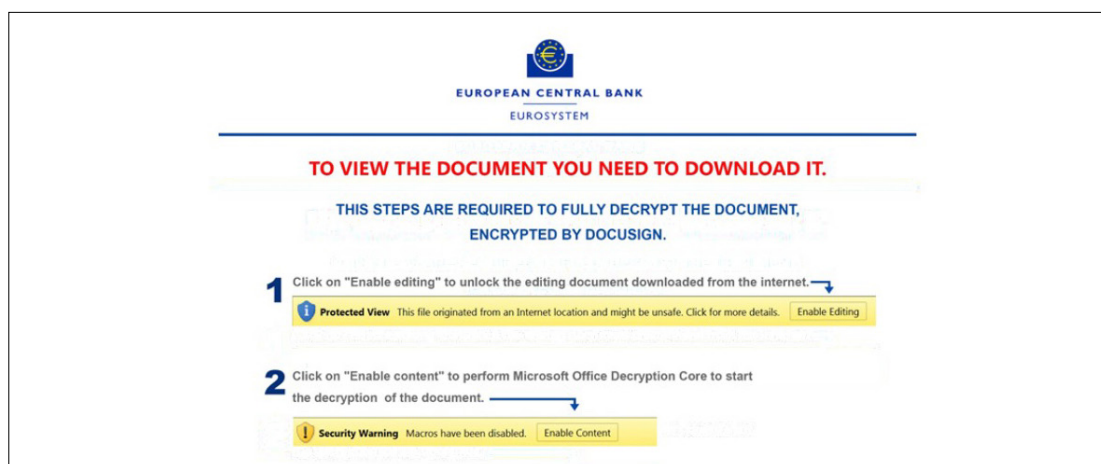


Рисунок 28. Пример документа с внедренными вредоносными макросами

Группа TA505 также атакует финансовые организации. У злоумышленников нет привязки по географическому признаку. В IV квартале специалисты PT ESC зафиксировали атаки этой группы на финансовые организации в США, Колумбии, Индии и Чехии. Во вложениях к вредоносным письмам группа TA505 доставляет загрузчик Get2, с помощью которого в дальнейшем на инфицированные компьютеры загружаются бэкдоры FlawedGrace и SDBbot, а также загрузчик Snatch.

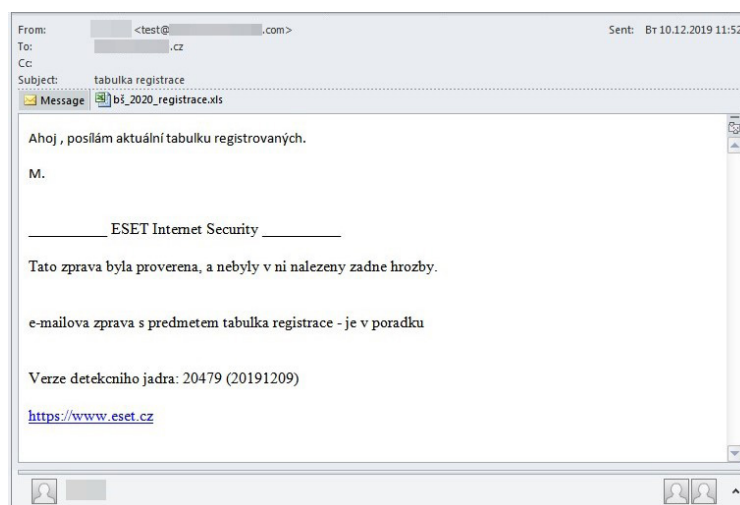


Рисунок 29. Фишинговое письмо группы TA505 в чешский банк

Помимо финансовых организаций, TA505 атаковала также IT-компании, промышленные предприятия, университеты и другие отрасли. Помимо вышеперечисленного ВПО, в арсенале группы по-прежнему шифровальщик CryptoMix, ВПО EmailStealer для фильтрации интересующих злоумышленников файлов по расширению и кражи почтовых аккаунтов, утилита для отключения Windows Defender и запуска полезной нагрузки, модифицированный бэкдор ServHelper. Кроме того, TA505 начали использовать шпионское ПО AZORult.

Появившийся на просторах дарквеба в апреле 2019 года новый инфостилер Рассоон набирает популярность. В IV квартале операторы этого ВПО атаковали сотрудников банковских организаций. Чтобы обойти средства защиты электронной почты, злоумышленники рассылают фишинговые письма с ранее скомпрометированной корпоративной учетной записи. В конце октября письма содержали ссылку на вредоносное изображение, размещенное в Dropbox. Рассоон распространяется по схеме malware as a service (MaaS) за 200 долл. США в месяц. Разработчики регулярно обновляют ВПО, добавляя в него новые функции.

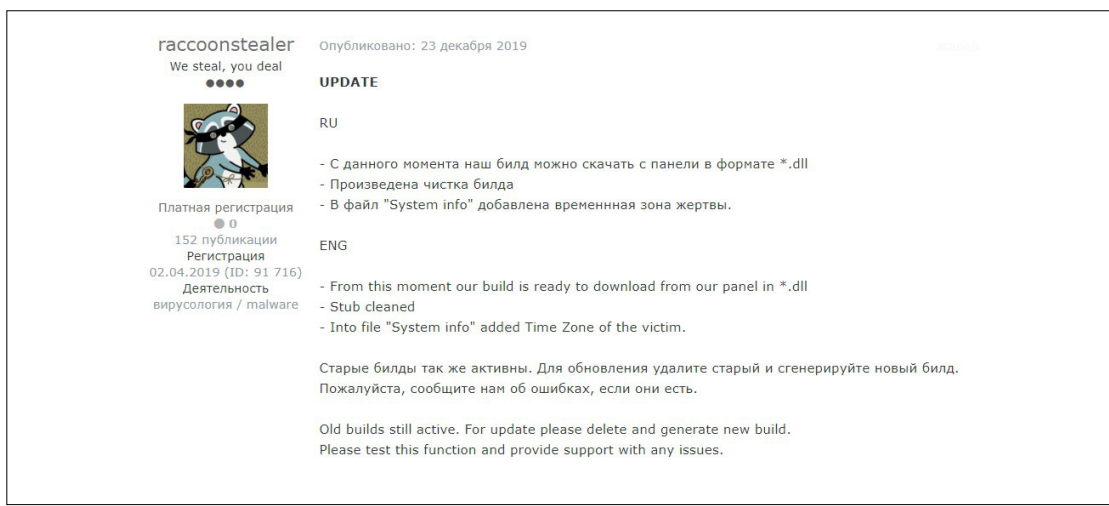


Рисунок 30. Объявление разработчиков Raccoon об обновлении ВПО

IT-компании

В IV квартале доля атак на IT-компании выросла до 8% от общего числа кибератак на юридические лица (против 3% в III квартале). Крупные IT-компании привлекательны для операторов шифровальщиков, и это неудивительно. Если скомпрометировать поставщика IT-услуг, он может потерять клиентов, ведь те будут опасаться за свою инфраструктуру. Можно предположить, что это заставит IT-компанию заплатить выкуп.

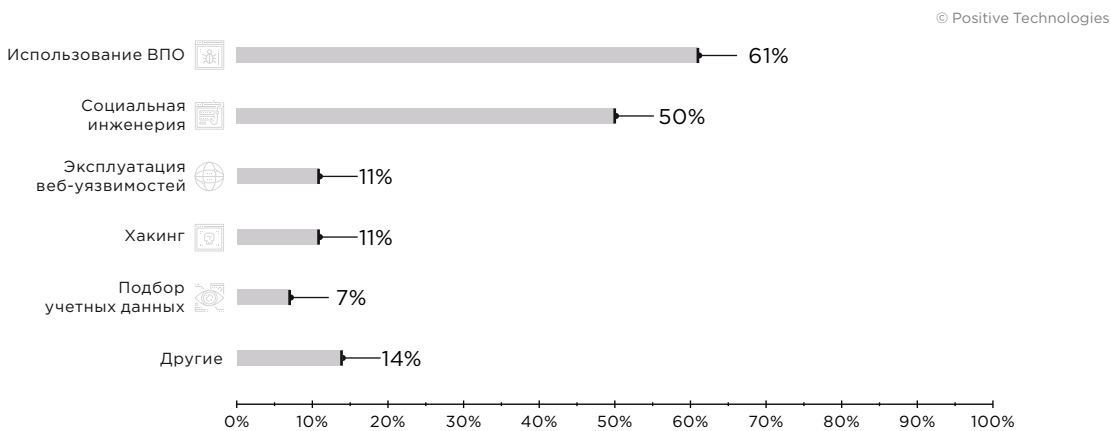


Рисунок 31. Методы атак на IT-компании в Q4 2019

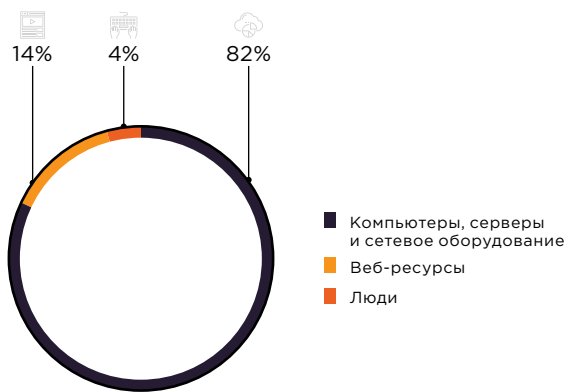


Рисунок 32. Объекты атак

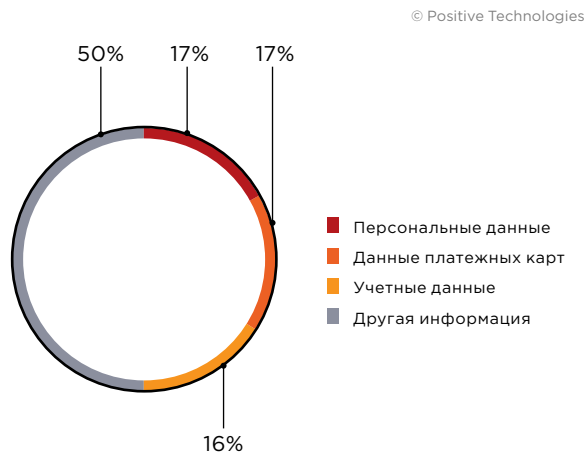


Рисунок 33. Украденные данные

Один из принципов Общего регламента по защите данных (GDPR) гласит, что персональные данные должны быть защищены от незаконной обработки, уничтожения и повреждения (принцип целостности и конфиденциальности). В IV квартале 2019 года мы наблюдали новый тренд: операторы шифровальщиков вынуждают жертв платить выкуп, аргументируя тем, что в случае разглашения персональных данных компания заплатит на порядок больше денег в соответствии с санкциями, предусмотренными GDPR. Так, один из крупнейших американских хостинг-провайдеров CyrusOne подвергся атаке шифровальщика (предположительно речь также идет о Sodinokibi), операторы которого пригрозили жертве публикацией похищенных данных в случае отказа платить выкуп.

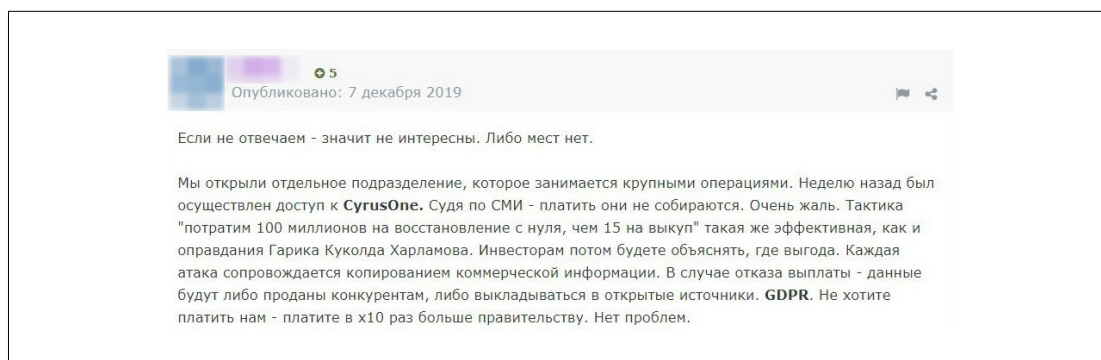


Рисунок 34. Сообщение в дарквебе об атаке на CyrusOne

От операторов Sodinokibi в IV квартале пострадали также IT-компании Synoptek и Complete Technology Solutions.

В начале квартала злоумышленники атаковали сайт Extendware, разработчика расширений для сайтов на базе CMS Magento, и внедрили на страницы продажи расширений кейлоггер. По мнению специалистов, речь может идти об атаке типа supply chain: злоумышленники могли внедрить вредоносное ПО не только на сайт Extendware, но и в сами расширения, что потенциально влечет за собой компрометацию всех клиентов жертвы. В середине 2019 года мы уже писали об атаках supply chain на IT-компании. Этот тренд сохранялся на протяжении всего года и, вероятно, сохранится и в 2020 году. Еще один пример supply chain — атака на разработчика платформы для электронной коммерции Volusion, о которой мы подробнее расскажем далее.

Торговля

© Positive Technologies

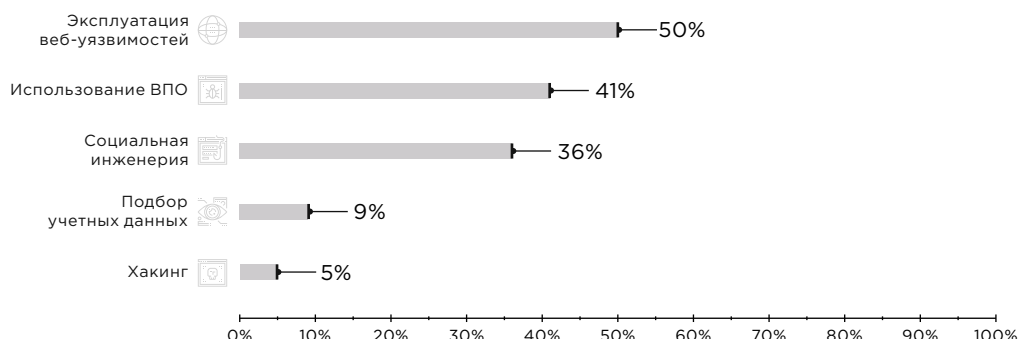


Рисунок 35. Методы атак на организации сферы торговли в Q4 2019

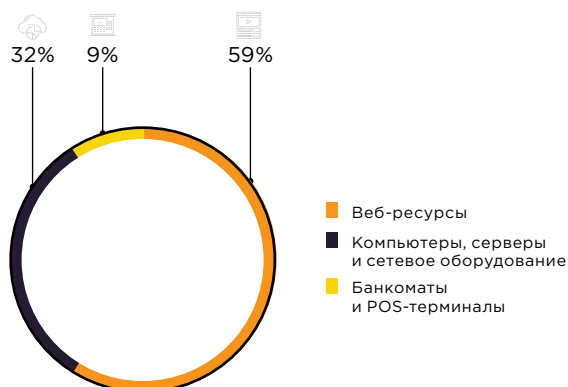


Рисунок 36. Объекты атак

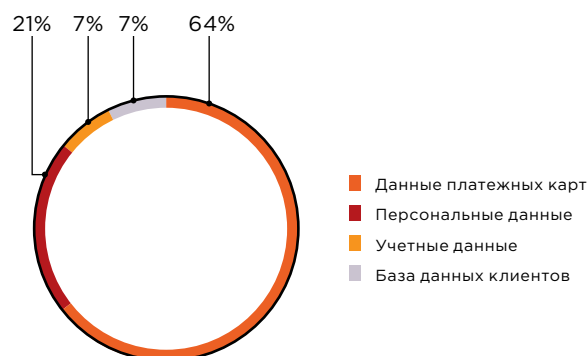


Рисунок 37. Украденные данные

В начале квартала стало известно, что злоумышленники, причастные к атакам под общим названием MageCart, скомпрометировали онлайн-магазин модной одежды Sixth June, разработанный на базе платформы Magento, и внедрили JavaScript-сниффер — небольшой скрипт, предназначенный для кражи данных платежных карт. Злоумышленники приняли меры, чтобы усложнить выявление сниффера — зарегистрировали доменное имя mogento[.]info, делая ставку на созвучие с Magento. С поддельного веб-ресурса загружались вредоносные компоненты, на него же в дальнейшем отправлялись похищаемые данные платежных карт.

Что такое MageCart

Это класс атак на онлайн-ресурсы с функцией оплаты, например интернет-магазины. Также термин MageCart используется для наименования групп злоумышленников, стоящих за этими атаками. Суть атаки заключается в компрометации сайта и внедрения скрипта на языке JavaScript (так называемого JavaScript-сниффера) на страницу оплаты. Когда пользователь вводит данные платежной карты на скомпрометированном сайте, сниффер отправляет их на сервер злоумышленников. Такой типа атак иногда называют веб-скиммингом.

Веб-скимминг достиг таких масштабов, что разные группы злоумышленников MageCart независимо друг от друга проводят атаки на одни и те же ресурсы. Так, эксперты PerimeterX пришли к выводу, что снифферы, аналогичные тому, что были на Sixth June, установлены еще на пяти веб-ресурсах, включая интернет-магазин PEXSuperstore.com. В то же время на сайте PEXSuperstore.com был выявлен второй сниффер, который, по мнению экспертов, был установлен другой группой киберпреступников.

Как и в прошлом квартале, наблюдаются атаки MageCart типа supply chain. Так, одна из групп скомпрометировала хранилище Google Cloud платформы для электронной коммерции Volusion и внедрила сниффер, который автоматически попал в интернет-магазины на базе Volusion. Число жертв по разным оценкам достигает от 6500 до 20 000 интернет-ресурсов.

Компрометируя онлайн-ресурсы и устанавливая JavaScript-снифферы, злоумышленники стараются минимизировать риск их обнаружения. Например, в случае с Volusion злоумышленники использовали доменное имя volusion-cdn[.]com, маскируя нелегитимную передачу данных под взаимодействие с серверами Volusion. Этот же прием использовался в описанных выше атаках на интернет-магазины на базе CMS Magento. Еще один тренд в сокрытии JavaScript-снифферов — минимизация объема внедряемого кода. Так, в IV квартале специалисты Malwarebytes выявили атаки, в ходе которых внедрялась всего одна строка кода, которая отвечала за загрузку JavaScript-сниффера с адреса payment-mastercard[.]com, принадлежащего злоумышленникам.

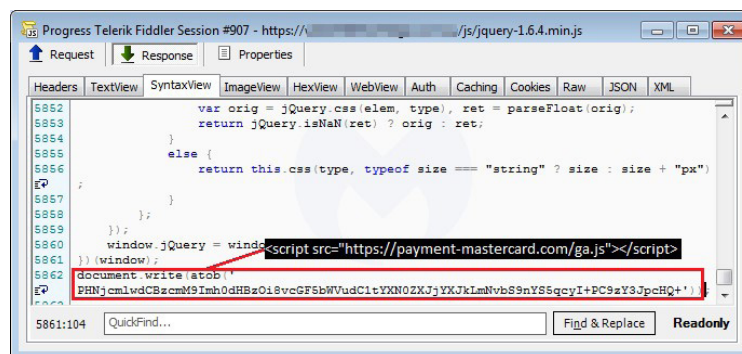


Рисунок 38. Ссылка на поддельную форму ввода платежных данных, внедренная на страницу скомпрометированного сайта

Специалисты также установили, что доменное имя payment-mastercard[.]com использовалось и для других атак. С него загружалась поддельная страница ввода платежных данных, имитирующая форму ввода легитимного провайдера платежных услуг. После ввода платежной информации в фишинговую форму данные отправлялись на сервер злоумышленников, а покупатель перенаправлялся на оригинальную страницу провайдера.

Торговым компаниям не стоит забывать, что им, так же как и другим отраслям, угрожают атаки шифровальщиков. К примеру, дилерской компании Arrigo Automotive Group в IV квартале подобная атака стоила 250 тыс. долл. США.

Кроме того, сферу торговли атакуют и АPT-группы. Например, специалисты PT ESC выявили АPT-атаки группы TA505 на торговые компании в Японии.

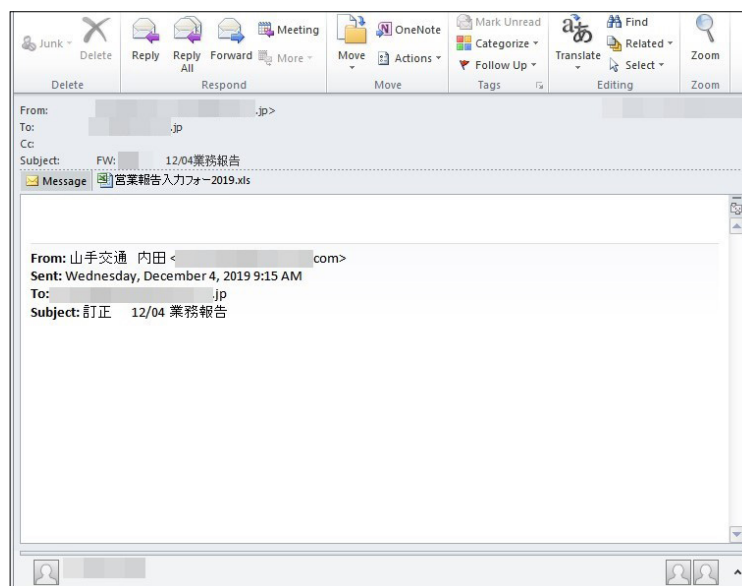


Рисунок 39. Письмо группы TA505 в адрес японской торговой компании

Как защититься организации



Используйте эффективные технические средства защиты

- Системы централизованного управления обновлениями и патчами для используемого ПО. Для правильной приоритизации планов по обновлениям необходимо учитывать сведения об актуальных угрозах безопасности.
- Системы антивирусной защиты со встроенной изолированной средой («песочницей») для динамической проверки файлов, способные выявлять и блокировать вредоносные файлы в корпоративной электронной почте до момента их открытия сотрудниками и другие вирусные угрозы. Наиболее эффективным будет использование антивирусного ПО, построенного на решениях одновременно нескольких производителей, способного обнаруживать скрытое присутствие вредоносных программ и позволяющего выявлять и блокировать вредоносную активность в различных потоках данных — в почтовом, сетевом и веб-трафике, в файловых хранилищах, на веб-порталах. Важно, чтобы выбранное решение позволяло проверять файлы не только в реальном времени, но и автоматически анализировало уже проверенные ранее, это позволит выявить не обнаруженные ранее угрозы при обновлении баз сигнатур.
- SIEM-решения — для своевременного выявления и эффективного реагирования на инциденты информационной безопасности. Это позволит своевременно выявлять злонамеренную активность, попытки взлома инфраструктуры, присутствие злоумышленника и принимать оперативные меры по нейтрализации угроз.
- Автоматизированные средства анализа защищенности и выявления уязвимостей в ПО.
- Межсетевые экраны уровня приложений (web application firewalls) — в качестве превентивной меры защиты веб-ресурсов.
- Системы глубокого анализа сетевого трафика — для обнаружения сложных целевых атак как в реальном времени, так и в сохраненных копиях трафика. Применение такого решения позволит не только увидеть не обнаруженные ранее факты взлома, но и в режиме реального времени отслеживать сетевые атаки, в том числе запуск вредоносного ПО и хакерских инструментов, эксплуатацию уязвимостей ПО и атаки на контроллер домена. Такой подход позволит существенно снизить время скрытного присутствия нарушителя в инфраструктуре, и тем самым минимизировать риски утечки важных данных и нарушения работы бизнес-систем, снизить возможные финансовые потери от присутствия злоумышленников.
- Специализированные сервисы анти-DDoS.

Г Защищайте данные:

- не храните чувствительную информацию в открытом виде или в открытом доступе;
- регулярно создавайте резервные копии систем и храните их на выделенных серверах отдельно от сетевых сегментов рабочих систем;
- минимизируйте, насколько это возможно, привилегии пользователей и служб;
- используйте разные учетные записи и пароли для доступа к различным ресурсам;
- применяйте двухфакторную аутентификацию там, где это возможно, например для защиты привилегированных учетных записей.

Г Не допускайте использования простых паролей:

- применяйте парольную политику, предусматривающую строгие требования к минимальной длине и сложности паролей;
- ограничьте срок использования паролей (не более 90 дней);
- смените стандартные пароли на новые, удовлетворяющие строгой парольной политике.

Г Контролируйте безопасность систем:

- своевременно обновляйте используемое ПО по мере выхода патчей;
- проверяйте и повышайте осведомленность сотрудников в вопросах информационной безопасности;
- контролируйте появление небезопасных ресурсов на периметре сети; регулярно проводите инвентаризацию ресурсов, доступных для подключения из интернета; анализируйте защищенность таких ресурсов и устраняйте уязвимости в используемом ПО; хорошей практикой является постоянный мониторинг публикаций о новых уязвимостях: это позволяет оперативно выявлять такие уязвимости в ресурсах компании и своевременно их устранять;
- эффективно фильтруйте трафик для минимизации доступных внешнему злоумышленнику интерфейсов сетевых служб; особое внимание стоит уделять интерфейсам удаленного управления серверами и сетевым оборудованием;
- регулярно проводите тестирование на проникновение для своевременного выявления новых векторов атак на внутреннюю инфраструктуру и оценки эффективности принятых мер по защите;
- регулярно проводите анализ защищенности веб-приложений, включая анализ исходного кода, с целью выявления и устранения уязвимостей, позволяющих проводить атаки, в том числе на клиентов приложения;
- отслеживайте количество запросов к ресурсам в секунду, настройте конфигурацию серверов и сетевых устройств таким образом, чтобы нейтрализовать типичные сценарии атаки (например, TCP- и UDP-флуд или множественные запросы к БД).



Позаботьтесь о безопасности клиентов:

- повышайте осведомленность клиентов в вопросах ИБ;
 - регулярно напоминайте клиентам о правилах безопасной работы в интернете, разъясняйте методы атак и способы защиты;
 - предостерегайте клиентов от ввода учетных данных на подозрительных веб-ресурсах и тем более от сообщения такой информации кому бы то ни было по электронной почте или во время телефонного разговора;
 - разъясняйте клиентам порядок действий в случае подозрений о мошенничестве;
 - уведомляйте клиентов о событиях, связанных с информационной безопасностью.
-

Как вендору защитить свои продукты

- Применяйте все те же меры защиты, что рекомендованы для обеспечения безопасности организации.
 - Внедрите процессы обеспечения безопасности на протяжении всего цикла разработки ПО.
 - Проводите регулярный анализ защищенности ПО и веб-приложений, включая анализ исходного кода.
 - Используйте актуальные версии веб-серверов и СУБД.
 - Откажитесь от использования библиотек и фреймворков, имеющих известные уязвимости.
-

Как защититься обычному пользователю

Г Не экономьте на безопасности:

- используйте только лицензионное ПО;
- используйте эффективные средства антивирусной защиты на всех устройствах;
- своевременно обновляйте используемое ПО по мере выхода патчей.

Г Защищайте ваши данные:

- наиболее важные файлы храните не только на жестком диске компьютера, но и на съемных носителях, внешних жестких дисках или в облачном хранилище;
- для повседневной работы в ОС используйте учетную запись без привилегий администратора;
- используйте двухфакторную аутентификацию там, где это возможно, например для защиты электронной почты.

Г Не используйте простые пароли:

- используйте сложные пароли, состоящие из незначущих комбинаций букв, цифр и знаков, длиной не менее 8 символов. Для создания и хранения паролей можно воспользоваться менеджером паролей (защищенным хранилищем с функциями генерации новых паролей);
- не используйте один и тот же пароль для разных систем (для сайтов, электронной почты и др.);
- меняйте все пароли хотя бы раз в полгода, а лучше — каждые два-три месяца.

Г Будьте бдительны:

- проверяйте все вложения, полученные по электронной почте, с помощью антивирусного ПО;
- с осторожностью относитесь к сайтам с некорректными сертификатами и учитывайте, что введенные на них данные могут быть перехвачены злоумышленниками;
- будьте предельно внимательны при вводе учетных данных на сайтах и во время работы с онлайн-платежами;
- не переходите по ссылкам на незнакомые подозрительные ресурсы, особенно когда браузер предупреждает об опасности;
- не переходите по ссылкам из всплывающих окон, даже если рекламируемые компания или продукт вам знакомы;
- не загружайте файлы с подозрительных веб-ресурсов или из других неизвестных источников.

Об исследовании

Данный отчет содержит информацию об актуальных угрозах информационной безопасности, основанную на собственной экспертизе компании Positive Technologies, результатах многочисленных исследований, а также на данных авторитетных источников.

В рамках отчета каждый массовый инцидент (например, вирусная атака, в ходе которой злоумышленники проводят многоадресные фишинговые рассылки) рассматривается как одна уникальная угроза информационной безопасности. В исследовании мы используем следующие термины:

Киберугроза — это совокупность факторов и условий, создающих опасность нарушения информационной безопасности. В нашем исследовании мы рассматриваем киберугрозы с точки зрения действий злоумышленников в киберпространстве, направленных на проникновение в информационную систему с целью кражи данных, денежных средств или с иными намерениями, которые потенциально ведут к негативным последствиям для государства, бизнеса или частных лиц. Действия злоумышленников могут быть направлены на IT-инфраструктуру компании, рабочие компьютеры, мобильные устройства, другие технические средства и, наконец, на человека как на элемент киберпространства.

Кибератака — несанкционированное воздействие на информационные системы со стороны киберпреступников с использованием технических средств и программного обеспечения с целью получения доступа к информационным ресурсам, нарушения нормальной работы или доступности систем, кражи, искажения или удаления информации.

Объект атаки — объект несанкционированного воздействия со стороны киберпреступников. Если методы социальной инженерии направлены на получение информации непосредственно от частного лица, клиента или сотрудника компании, то объектом атаки является категория «Люди». Если же методы социальной инженерии применяются с целью доставки ВПО в инфраструктуру компании или на компьютер частного лица, то в качестве объекта атаки выбирается категория «Компьютеры, серверы и сетевое оборудование».

Мотив атаки — первостепенная цель киберпреступников. Например, если в результате атаки похищены данные платежных карт, мотивом в этом случае является получение данных.

Метод атаки — совокупность приемов, которые использовались для достижения цели. Например, злоумышленник может провести разведку, выявить доступные для подключения уязвимые сетевые службы, проэксплуатировать уязвимости и получить доступ к ресурсам или информацию; такой процесс мы называем хакингом. При этом подбор учетных данных и использование уязвимостей веб-приложений мы выделили в отдельные категории для большей детализации.

Категория жертв — сфера деятельности атакованной организации (или частные лица, если в результате атаки пострадали люди независимо от места их работы). Так, к сфере услуг мы относим организации,

которые предоставляют услуги на коммерческой основе (консалтинговые организации, гостиницы, рестораны и др.). Категория «Онлайн-сервисы» включает интернет-площадки, позволяющие пользователям решать их задачи онлайн (например, сайты-агрегаторы для покупки билетов, бронирования номеров в гостиницах, блоги, соцсети, мессенджеры и иные социальные медиаресурсы, видеохостинги, онлайн-игры). Масштабные кибератаки, преимущественно вредоносные эпидемии, которые не ограничиваются воздействием на какую-то одну отрасль, мы отнесли к категории «Без привязки к отрасли».

По нашей оценке, большинство кибератак не передается огласке из-за репутационных рисков, в связи с этим оценить точное число угроз не представляется возможным даже для организаций, занимающихся расследованием инцидентов и анализом действий хакерских групп. Данное исследование проводится с целью обратить внимание организаций и обычных граждан, интересующихся современным состоянием информационной безопасности, на наиболее актуальные методы и мотивы кибератак, а также с целью выявить основные тенденции в изменении ландшафта киберугроз.

Краткое описание группировок

APT-C-35 (Donot, SectorE02) активна с 2016 года и атакует организации в странах Южной Азии: Пакистан, Бангладеш, Шри-Ланку, Мальдивы, Мьянму, Непал и страны Шанхайской организации сотрудничества. Злоумышленники выдают себя за представителей государственных учреждений, военных ведомств и телекоммуникационных компаний.

APT28 (Fancy Bear, Sofacy) — кибершпионская группа, которая проводит атаки как минимум с 2004 года. Стала широко известна в 2016 году после серии атак в преддверии выборов президента в США. В 2017 и 2018 годах проводила атаки на международные организации, военно-промышленные комплексы и правительственные организации в Европе и Южной Америке. В арсенале группы множество различных инструментов, в том числе собственной разработки.

APT40 (Leviathan, TEMP.Jumper, TEMP.Periscope) известна кибершпионскими кампаниями с 2013 года. Атакует транспортные и государственные организации, сферу науки и образования, а также IT-компании в Западной Европе, Северной Америке и Юго-Восточной Азии.

Bisonal известна одноименным ВПО собственной разработки. Известна с 2014 года. Атакует организации преимущественно в России, Южной Корее и Японии.

Bronze Union, также известная как TG-3390, LuckyMouse, APT27, Emissary Panda, проводит кибератаки с целью кибершпионажа с 2010 года. Для проникновения в сеть хакеры часто применяют стратегию watering hole: взламывают сайты, посещаемые целевыми пользователями, и размещают на них ВПО, которое будет автоматически заражать компьютеры посетителей. В настоящее время группировка атакует государственные организации и компании, относящиеся к промышленности, оборонному производству, энергетике, аэрокосмической и другим высокотехнологичным отраслям по всему миру.

Cloud Atlas известна с 2014 года благодаря атакам на различные организации в России, Центральной Азии и Европе (особенно в Португалии).

Cobalt известна с 2016 года своими атаками на организации кредитно-финансовой сферы. Начиная с кражи денег из банков в странах СНГ. С 2017 года расширила географию атак на банки Восточной Европы и Юго-Восточной Азии. Свое название получила по инструменту для проведения тестов на проникновение Cobalt Strike, который использовала при развитии атак внутри сети. Основной способ проникновения в сеть компании-жертвы — фишинговые рассылки с вредоносными вложениями разных форматов (исполняемые файлы, документы Microsoft Office с макросами или эксплойтами, LNK-файлы, запароленные архивы с исполняемыми файлами).

Gamaredon активна с 2013 года. Атакующих интересуют только украинские госструктуры, поэтому на их контрольных серверах настроена фильтрация обращений по географическому признаку. В своих атаках злоумышленники используют цепочку скриптов, которые загружают на компьютер жертвы утилиту для удаленного управления UltraVNC. Группа использует также Pteranodon — фреймворк собственной разработки, который позволяет полноценно управлять зараженным узлом: собирать сведения о системе и ее пользователях, красть пароли, выполнять скрипты и команды, а также передавать собранную информацию на удаленные серверы.

RTM известна с 2016 года. При атаках группа пытается получить доступ к банковским счетам организаций и производит кражу денег. Для получения доступа в корпоративную сеть используются фишинговые рассылки. С начала своей активности группа придерживается неизменного формата этих писем. По данным Positive Technologies, только за 2018 год группа провела 59 рассылок, в том числе нацеленных на финансовые учреждения. Также в 2019 году группировка стала использовать блокчейн биткойна. В число атакуемых попадают в большинстве своем организации финансовой отрасли, также известны случаи рассылок, нацеленных на промышленные, государственные и IT-организации. Кроме того, данная группа в качестве доменов для некоторых своих центров управления использовала домены в зоне .bit. Это специальная зона, созданная на базе технологии блокчейна Namecoin, защищенная от цензуры и принудительного изъятия доменов альтернатива традиционным регистраторам DNS. Из-за особенностей архитектуры блокчейна специалисты PT Expert Security Center смогли разработать алгоритм отслеживания регистрации новых доменов группировки RTM (или смены их IP-адресов). Это позволило уведомлять кредитно-финансовые организации и сообщества экспертов по ИБ о новых управляющих серверах с задержкой в считанные минуты после начала их использования злоумышленниками (а иногда и до начала).

SongXY обнаружена в 2017 году экспертами Positive Technologies. Среди пострадавших организаций насчитывается не менее 17 компаний из России, Японии, Монголии, Белоруссии, США, Таджикистана, Узбекистана, Киргизии, Казахстана и Украины. Группа атакует оборонные и промышленные предприятия. С помощью электронных писем злоумышленники рассылают ВПО Lurid и Gh0st, которое способно похищать информацию, делать скриншоты, записывать звук с микрофона.

TA505 активна с 2014 года, среди целей — крупнейшие финансовые, производственные и транспортные компании, государственные структуры. Группировка атакует организации из Великобритании, Канады, США, Южной Кореи и десятков других стран. Для проникновения в сети компаний-жертв группа использует фишинговые письма. С каждой новой волной атак злоумышленники привносят качественные изменения в свой инструментарий, сегодня их отличает использование более сложных техник сокрытия своего присутствия. С 2014 года в их арсенале числятся банковский троян Dridex, ботнет Neutrino, а также несколько семейств шифровальщиков — Locky, Jaff, Globelmposter и др. С весны 2018 года группа использует remote access trojan — FlawedAmmyu, а с конца 2018 года применяет новый бэкдор ServHelper.

О компании

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.