



Актуальные киберугрозы

III квартал 2019 года

Содержание

Обозначения	2
Резюме	3
Сводная статистика	4
Динамика атак	7
Методы атак	8
Использование вредоносного ПО	8
Социальная инженерия	9
Хакинг	10
Эксплуатация веб-уязвимостей	11
Подбор учетных данных	11
Категории жертв	12
Государственные организации	13
Промышленные компании	14
Финансовые организации	16
Наука и образование	18
Как защититься организации	20
Как вендору защитить свои продукты	22
Об исследовании	24
Краткое описание группировок	25

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 III квартала 2019 года мы отмечаем:

- Количество уникальных киберинцидентов растет — в III квартале мы зафиксировали на 6% больше кибератак, чем во II квартале.
- Целенаправленные атаки существенно преобладают над массовыми, их доля составила 65% против 59% во II квартале. Организации по всему миру находятся под угрозой сложных целенаправленных атак (APT-атак). Наибольший интерес для злоумышленников представляют государственные учреждения, промышленные компании, финансовый сектор и организации сферы науки и образования.
- В список целей APT-группы TA505 добавились новые отрасли, расширилась география атак.
- Доля кибератак, направленных на кражу информации, в два раза больше доли финансово мотивированных кампаний.
- Четверть от общего объема похищенной у юридических лиц информации составили персональные данные. Частные лица чаще рискуют учетными записями — логины и пароли составили 47% всего объема информации, похищенной у частных лиц.
- Растет доля заражений вредоносным ПО. Три четверти атак на юридические лица и 62% атак на частных лиц сопровождались заражениями различного рода зловредами.
- Треть всех заражений вредоносным ПО как среди юридических, так и среди частных лиц, приходится на долю шпионских троянов. Среди юридических лиц также остается высокой доля заражений шифровальщиками (27%), среди частных лиц — рекламным ПО (21%).
- В 81% случаев заражение инфраструктуры компаний вредоносным ПО начиналось с фишингового письма. Наиболее распространенный вектор заражения частных лиц — через посещение различного рода веб-ресурсов: на долю этого вектора в III квартале пришлось 35% заражений ВПО.

Сводная статистика

В III квартале 2019 года доля атак, направленных на кражу информации, выросла до 61% в атаках на юридические лица и до 64% в атаках на частных лиц (против 58% и 55% соответственно во II квартале). Доля финансово мотивированных атак для юридических и частных лиц сравнялась и составила 31%. Финансово мотивированные кампании в отношении юридических лиц преимущественно связаны с заражениями троянами-шифровальщиками, требующими выкуп за восстановление зашифрованных данных. В атаках на частных лиц киберпреступники ищут финансовую выгоду, распространяя навязчивую рекламу и мобильные приложения, подписывающие на платные услуги.

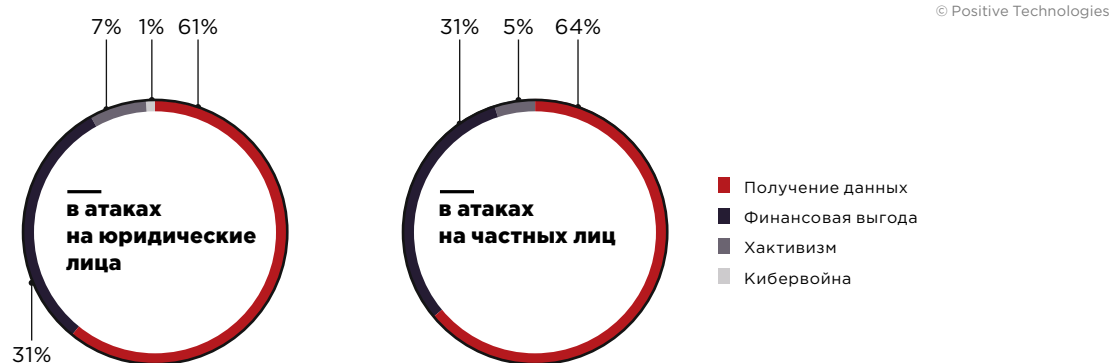


Рисунок 1. Мотивы злоумышленников

Утечка персональных данных в результате кибератаки — по-прежнему одна из актуальных угроз. В III квартале персональные данные составили четверть от общего объема похищенной у юридических лиц информации. Как известно, в 2018 году вступил в силу Общий регламент по защите данных (GDPR). В сентябре появилась информация о том, что польский ретейлер оштрафован за нарушение GDPR на 645 тыс. евро после инцидента с утечкой персональных данных более 2 млн пользователей его веб-сайтов в прошлом году.

Каждая пятая атака (19%) в III квартале была направлена против частных лиц. Почти половина (47%) всех украденных у частных лиц данных — это учетные данные. Пользователи могут сами раскрывать логины и пароли злоумышленникам в результате хитроумных фишинговых атак. Например, более 200 клиентов Народного банка в Казахстане попались на удочку кибермошенников, не заметив не большой разницы в адресе онлайн-банка, и ввели свои учетные данные на поддельном сайте, имитирующем официальный ресурс.

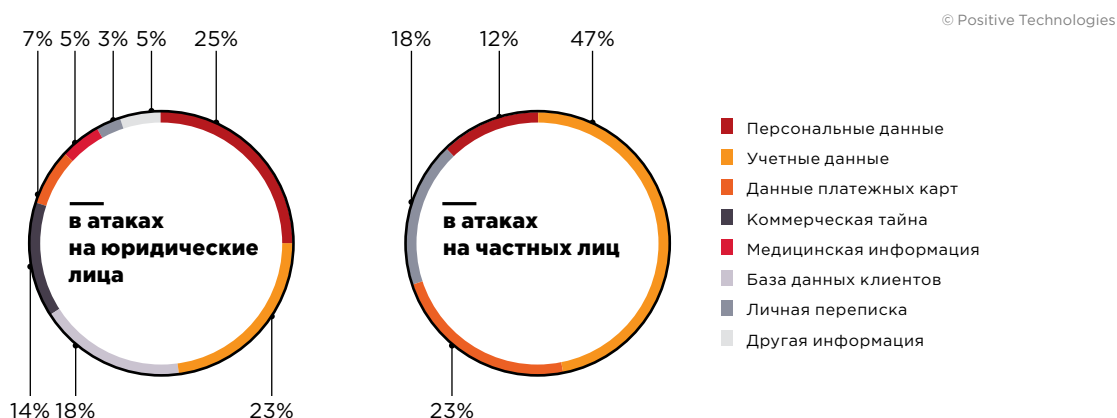


Рисунок 2. Типы украденных данных

Высокая доля целенаправленных атак — тренд, который в 2019 году мы отмечаем из квартала в квартал. В III квартале их доля составила 65% (для сравнения — 47% в I квартале, 59% во II квартале). Мы видим связь увеличения доли целевых атак с ростом активности APT-группировок. В III квартале специалисты PT Expert Security Center (PT ESC) зафиксировали кибератаки APT-групп TA505, RTM, Cobalt, Bronze Union, APT-C-35, KONNI, Gamaredon и других.

Мы вновь отмечаем высокий интерес злоумышленников к государственным учреждениям. Доля атак на правительственные ресурсы выросла до 23%, что на 4 п. п. больше, чем во II квартале. Кроме того, злоумышленники активно атакуют промышленные компании, финансовую отрасль, а также образовательные учреждения и научные институты. На некоторых из этих атак мы остановимся более подробно.

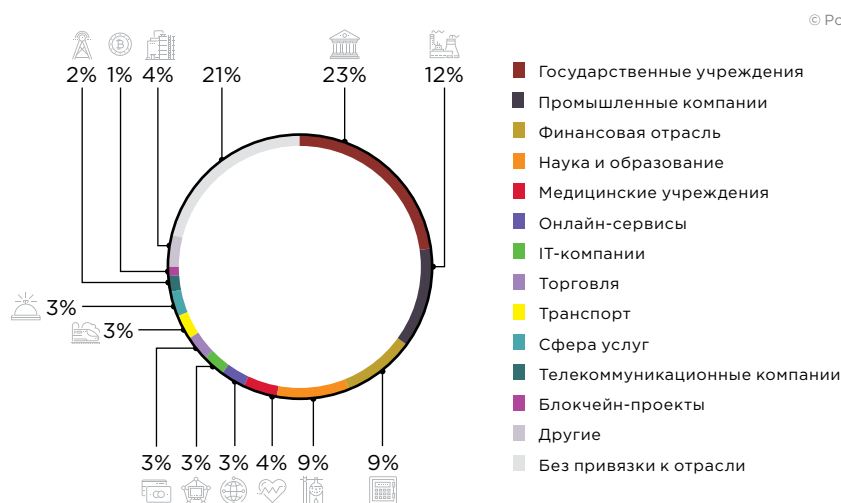


Рисунок 3. Категории жертв среди юридических лиц

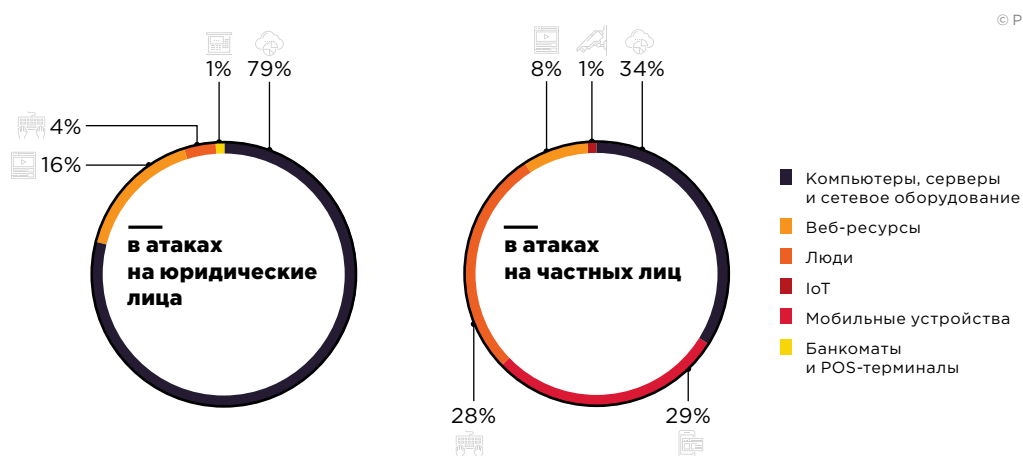


Рисунок 4. Объекты атак

Заражение вредоносным ПО вкупе с методами социальной инженерии — по-прежнему наиболее распространенные методы кибератак. В III квартале три четверти (74%) кибератак на юридические лица сопровождались заражением жертв различного рода зловредами, что на 13 п. п. больше, чем во II квартале.

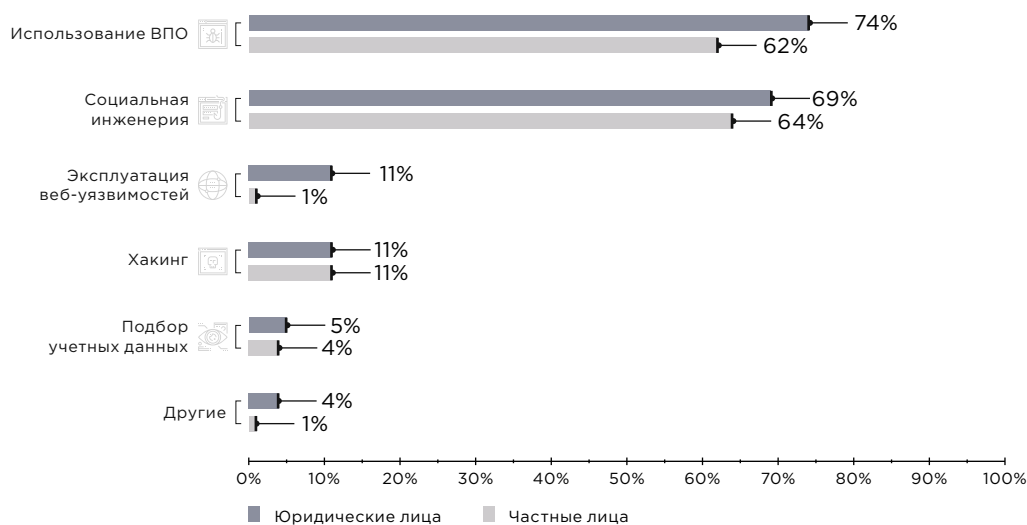


Рисунок 5. Методы атак

Отрасль

Распределение киберинцидентов по метрикам (мотивы, методы, объекты атак) внутри отраслей		Государственные учреждения	Финансовая отрасль	Промышленные компании	Медицинские учреждения	Онлайн-сервисы	Сфера услуг	IT-компании	Наука и образование	Торговля	Телекоммуникационные компании	Транспорт	Блокчейн-проекты	Другие	Без привязки к отрасли	Частные лица
Всего атак		69	28	37	11	10	8	10	29	8	7	8	4	12	65	73
Объект	Компьютеры, серверы и сетевое оборудование	52	23	34	8	3	3	8	27	6	7	5	2	7	56	25
	Веб-ресурсы	14	2	1	1	7	4	2	1	2		2	2	4	6	6
	Люди	3	1	2	2				1			1		1	3	20
	Мобильные устройства															21
	Банкоматы и POS-терминалы		2				1									
	IoT															1
Метод	Использование ВПО	52	24	34	7	1	4	5	24	3	4	6		6	56	45
	Социальная инженерия	49	24	35	8	1	4	5	23	3	4	7		6	42	47
	Подбор учетных данных	3	1			1	2	1			1	1	1	1	3	3
	Хакинг	7	1	2				3	3	1	1		3	1	12	8
	Эксплуатация веб-уязвимостей	11	1	2		6	2	1		4			1	3	4	1
	Другие	2	1	1	2	2					2			2	1	1
Мотив	Получение данных	46	27	33	5	7	7	7	9	4	5	8	1	10	28	46
	Финансовая выгода	11	1	4	5			1	20	3			3	1	36	23
	Хактивизм	9			1	3	1	2		1	2			1	1	4
	Кибервойна	3														

Градацией цвета показана доля атак внутри одной отрасли

Динамика атак

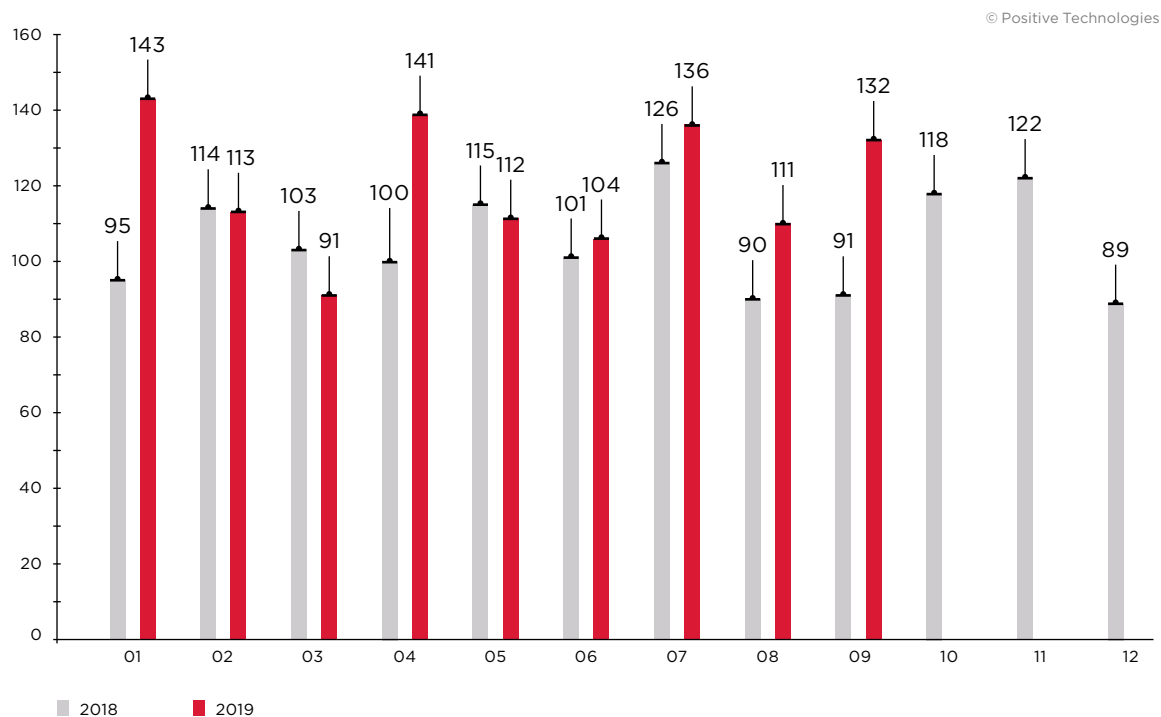


Рисунок 6. Количество инцидентов в 2018 и 2019 годах (по месяцам)

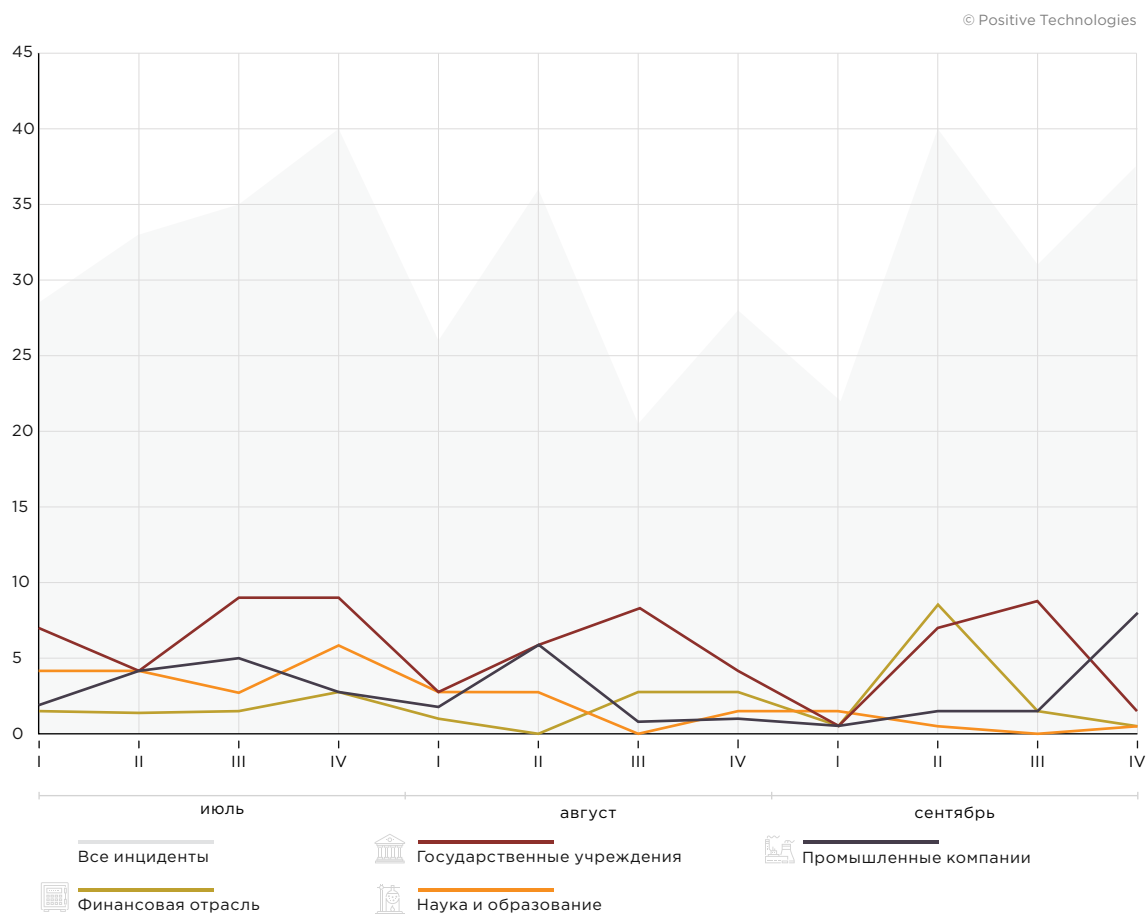


Рисунок 7. Количество инцидентов в III квартале 2019 года (по неделям)

Методы атак

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

Использование вредоносного ПО

На протяжении III квартала специалисты РТ ESC регулярно фиксировали атаки АPT-группы TA505. В арсенале группировки банковский троян Dridex, шифровальщик Cryptomix, код которого подписан сертификатами, выданными на подставные юрлица, трояны для удаленного управления ServHelper и FlawedAmmyu, а также плагин Upxxes, способный детектировать и отключать большое число антивирусных средств защиты. Злоумышленники вели активные фишинговые рассылки в организации по всему миру, атакуя финансовый сектор, промышленные компании, правительственные учреждения, научные институты, транспортные организации. На некоторых кампаниях мы остановимся подробнее в соответствующих разделах.

В III квартале наши эксперты обнаружили новую активность группы Bronze Union (она же LuckyMouse, APT27), распространяющей ВПО для удаленного управления ZxShell. Компоненты обнаруженного ВПО были подписаны с использованием скомпрометированных сертификатов различных компаний. Установленный троян ZxShell сложно обнаружить при сканировании зараженной системы классическими средствами защиты, поскольку вместе с ним злоумышленники устанавливают специальный руткит, который заменяет установочные пути модулей ВПО в момент обращения к ним на пути легитимных утилит.

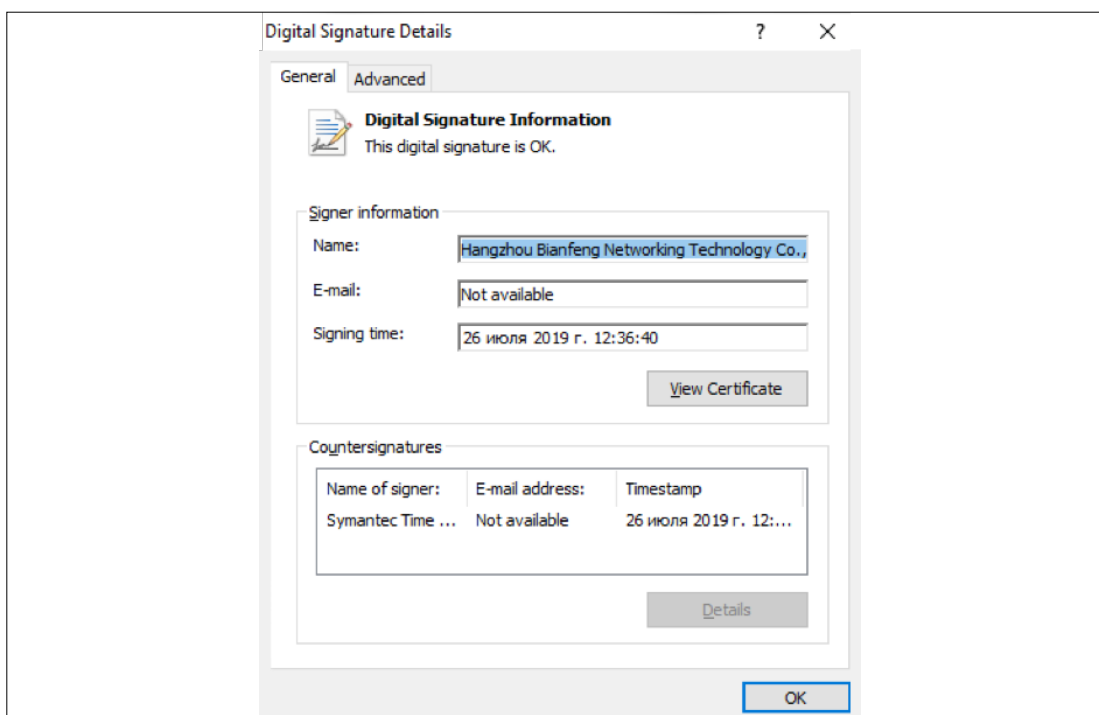


Рисунок 8. Подпись установщика ZxShell скомпрометированным сертификатом

Операторы шифровальщика Sodinokibi, о котором мы уже писали во II квартале, продолжают агрессивную политику. В результате компрометации поставщика облачных технологий PerCSoft данные его клиентов — приблизительно 400 стоматологических клиник — оказались зашифрованы. В августе жертвами этого шифровальщика стали более 20 населенных пунктов в Техасе. Злоумышленники регулярно изобретают новые способы доставки Sodinokibi на компьютеры жертв.

Доля майнеров в III квартале сократилась до 3% в атаках на юридические лица и до 2% в атаках на частных лиц. Мы связываем это с постепенным переходом злоумышленников на ВПО, которое может выполнять сразу несколько функций. Например, троян Clipse способен скрытно «майнить» криптовалюту, воровать пароли, подменять адреса криптокошельков, а также запускать брутфорс-атаки против сайтов на базе WordPress.

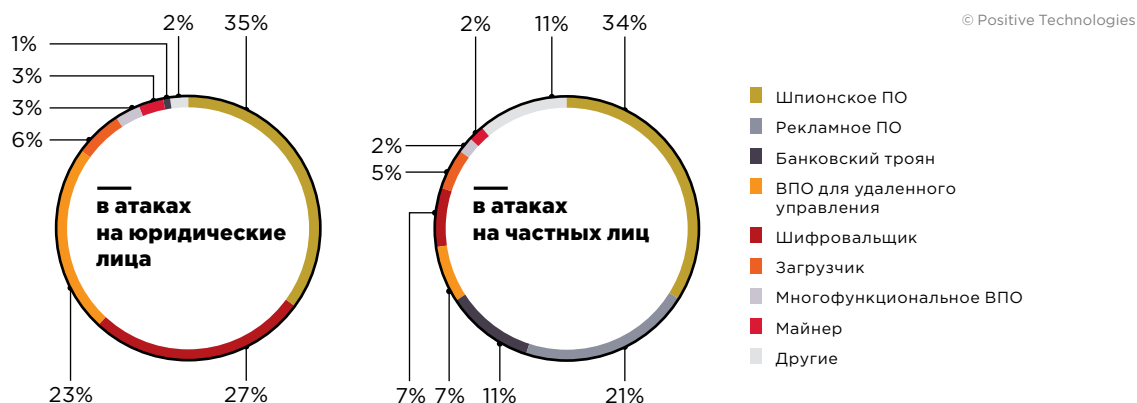


Рисунок 9. Типы вредоносного ПО

В конце августа Emotet (один из крупнейших ботнетов в мире) возобновил активность после нескольких месяцев затишья. Операторы ботнета работают по схеме malware as a service (MaaS) и предоставляют киберпреступникам доступ к компьютерам, зараженным Emotet, для их дальнейшего инфицирования другими вредоносами. С сентября злоумышленники проводят вредоносные рассылки под видом счетов на оплату, финансовых документов и даже под видом бесплатной версии новой книги Эдварда Сноудена. Вложения к таким письмам заражают жертву трояном Emotet, посредством которого операторы ботнета могут загружать на скомпрометированные устройства другие злоумышленники, например банковский троян Trickbot или вымогатель Ryuk, которые нередко находят одновременно на зараженных узлах.

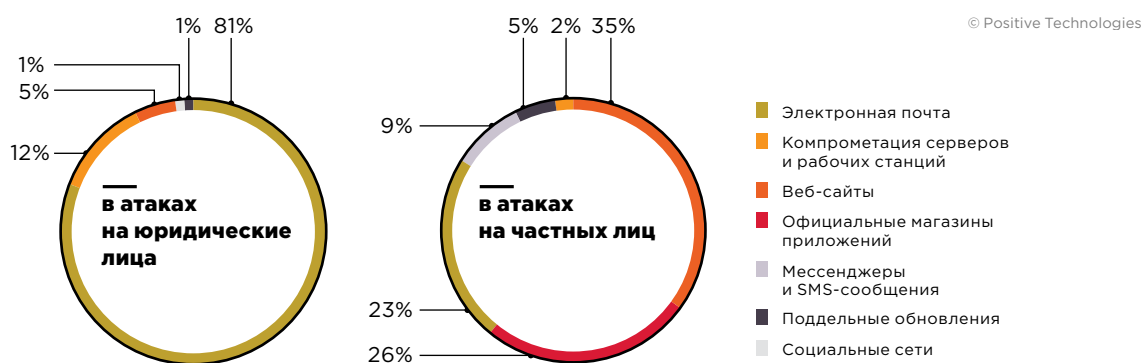


Рисунок 10. Способы распространения ВПО

Социальная инженерия

Методы социальной инженерии популярны у злоумышленников. В III квартале их доля в атаках на юридические лица выросла почти вдвое и составила 69% против 37% в прошлом квартале. Киберпреступники продолжают зарабатывать огромные суммы, подделывая либо используя скомпрометированные корпоративные адреса электронной почты (business email compromise, BEC) для рассылки фишинговых писем. Преступники выдают себя за представителя доверенной компании, например контрагента, и просят оплатить счет, подменив банковские реквизиты. Так, в администрацию округа Кабаррус (Северная Каролина, США) пришло оповещение

о том, что реквизиты строительного подрядчика якобы изменились. Не заподозрив неладное, очередной платеж на сумму 2,5 млн долл. США администрация перевела уже не подрядчику, а киберпреступникам. Жертвой аналогичной атаки стала компания Toyota Boshoku Corporation, лишившаяся внушительной суммы в 37,5 млн долл. США. По данным американского Центра приема жалоб на киберпреступления (Internet Crime Complaint Center, IC3), мировые убытки от ВЕС-мошенничества за последние три года составили более 26 млрд долл. США.

Вредоносная ссылка, даже если она отправлена с доверенного адреса, может быть заблокирована средствами защиты электронной почты. Однако киберпреступники успешно обходят системы борьбы с фишингом. Например, в III квартале злоумышленники рассылали банковским рабочим письма со ссылкой на скомпрометированный ресурс SharePoint. Там злоумышленники разместили документ с другой ссылкой, перейдя по которой жертва попадала на поддельную страницу ввода логина и пароля. Если бы фишинговая ссылка была добавлена непосредственно в тело письма, средства защиты могли бы его заблокировать, однако ссылки на SharePoint были включены в белые списки и не блокировались.

© Positive Technologies

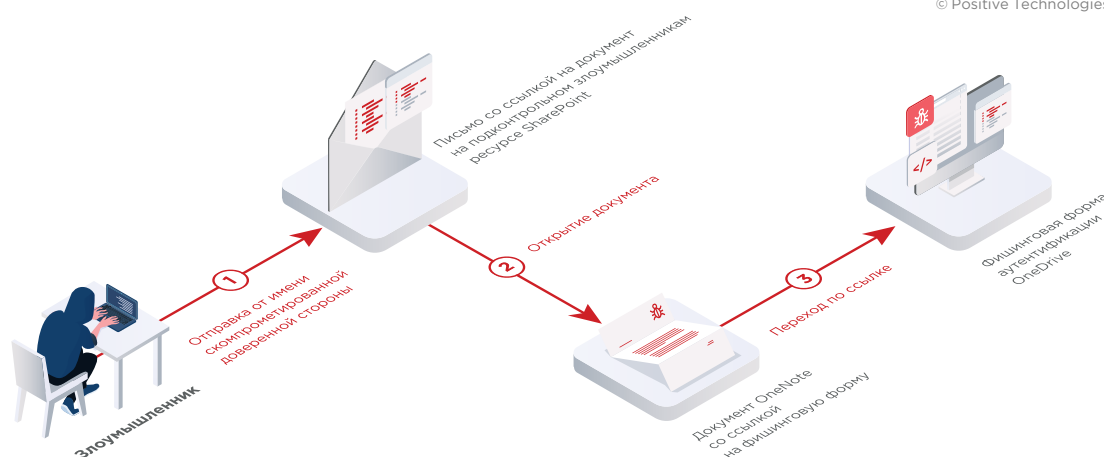


Рисунок 11. Схема фишинговой атаки с использованием скомпрометированных ресурсов SharePoint

Хакинг

Мы регулярно напоминаем читателям о необходимости своевременного обновления ПО. Когда об уязвимости в программном продукте становится известно широкому кругу людей, в первую очередь под удар кибератак попадают те организации и частные лица, которые своевременно не установили обновления. Так, в III квартале группа злоумышленников eGobbler, внедряющих на страницы веб-сайтов вредоносную рекламу, продолжает эксплуатировать уязвимость CVE-2019-5840 в браузере Chrome для iOS, которая была исправлена еще в июне. Однако вскоре после выхода обновления злоумышленники eGobbler выявили новую уязвимость — на этот раз в движке WebKit. Брешь позволяет показывать всплывающие окна с рекламой каждый раз, когда пользователь использует клавиатуру для навигации по сайту. В настоящее время уязвимость исправлена в iOS 13 и Safari 13.0.1.

В прошлом квартале мы писали о критически опасной уязвимости в службе RDS CVE-2019-0708, более известной под названием BlueKeep. В августе специалисты Microsoft исправили еще две ошибки в службе RDS; эти новые критически опасные уязвимости CVE-2019-1181 и CVE-2019-1182 похожи на BlueKeep, однако им подвержены более поздние версии Windows, включая серверные.

Эксплуатация веб-уязвимостей

Во второй половине сентября в сети появился эксплойт для уязвимости нулевого дня в форумном движке vBulletin. Новость о критически опасной уязвимости удаленного выполнения кода CVE-2019-16759, для эксплуатации которой не требуется авторизация на уязвимом форуме, быстро распространилась, хотя некоторые специалисты в области информационной безопасности утверждают, что узнали о ней несколько лет назад. В конце сентября брешь в vBulletin стала причиной взлома форумов Comodo. Как стало известно, данные 170 тысяч пользователей уже продаются в дарквебе.

Для пользователей, оплачивающих товары или услуги через интернет, по-прежнему представляют угрозу JavaScript-снифферы MageCart — небольшие сценарии на языке JavaScript, которыми злоумышленники заражают сайты с функцией онлайн-платежей. В III квартале 2019 года исследователи Trend Micro обнаружили вредоносные скрипты на сайтах двух крупных сетей отелей. Атакам подверглись постояльцы, которые оплачивали проживание через мобильные устройства. Специалистам удалось выяснить, что отели стали жертвами атак supply chain. Снифферы MageCart попали на сайты через зараженную JavaScript-библиотеку. Ее использовала компания, у которой обе жертвы заказывали разработку сайтов.

Пробелы с веб-безопасностью бывают не только у онлайн-сервисов и интернет-магазинов. Уязвимость в функции загрузки файлов в программном обеспечении SuperINN Plus для онлайн-бронирования позволила злоумышленникам взломать приложение, загрузив на сайт веб-шелл — скрипт на языке PHP для управления сервером. Помимо этого, киберпреступники нашли возможность выполнять внедрение SQL-кода. В руки злоумышленников попали зашифрованные номера платежных карт, персональные данные и контактная информация более 43 тысяч человек. Предположительно, злоумышленникам удалось получить и ключ шифрования. Этот инцидент еще раз напоминает о необходимости регулярного анализа защищенности веб-приложений. К слову, загрузка произвольных файлов — распространенная критически опасная уязвимость, которую в 2018 году наши специалисты находили в каждом четвертом исследованном веб-приложении.

Подбор учетных данных

От подбора учетных данных не застрахована ни одна компания. Credential stuffing — это метод взлома, при котором атакующие пытаются получить доступ к системе, используя базу ранее украденных логинов и паролей, которые они приобрели, например, в дарквебе. От такого рода атаки в III квартале 2019 года пострадала организация, управляющая транспортной системой Лондона, Transport for London, сайт которой пришлось временно закрыть. Жертвой атаки credential stuffing стала и компания State Farm, предоставляющая финансовые и страховые услуги. К слову, исследование Akamai свидетельствует, что в период с ноября 2017 года по апрель 2019 года 6,1% атак методом подбора учетных данных пришлось на финансовый сектор.

Категории жертв

Г Далее мы подробнее остановимся на анализе атак на отдельные отрасли, которые нам показались наиболее интересными в III квартале 2019 года.

Государственные организации

© Positive Technologies

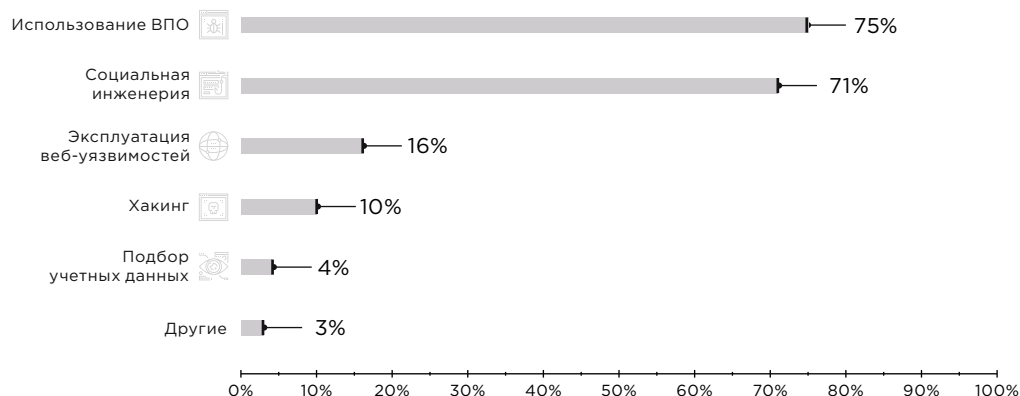


Рисунок 12. Методы атак на государственные организации в Q3 2019

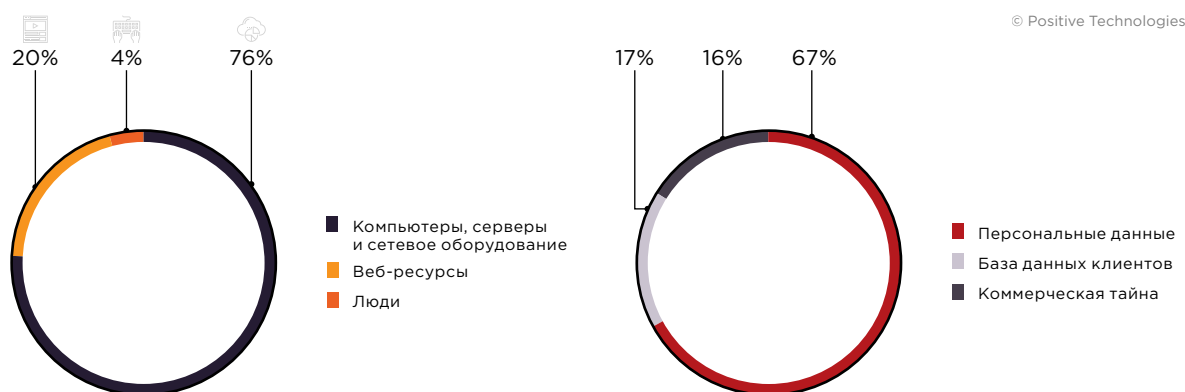


Рисунок 13. Объекты атак

Рисунок 14. Украденные данные

Интерес злоумышленников к государственным организациям растет. Министерства, ведомства, администрации городов постоянно находятся под угрозой сложных целенаправленных атак. Мы отмечаем, что некоторые кибергруппировки, конечная цель которых — кража денег из организации, предпринимают попытки кибератак на госучреждения. Так, в III квартале 2019 года специалисты PT ESC обнаружили фишинговые рассылки группы TA505 в адрес правительственных организаций Южной Кореи, Китая, Канады и Великобритании.

Группировка RTM также обратила внимание на госучреждения. В III квартале эксперты PT ESC обнаружили фишинговые письма в адрес правительственных организаций в России и Белоруссии.

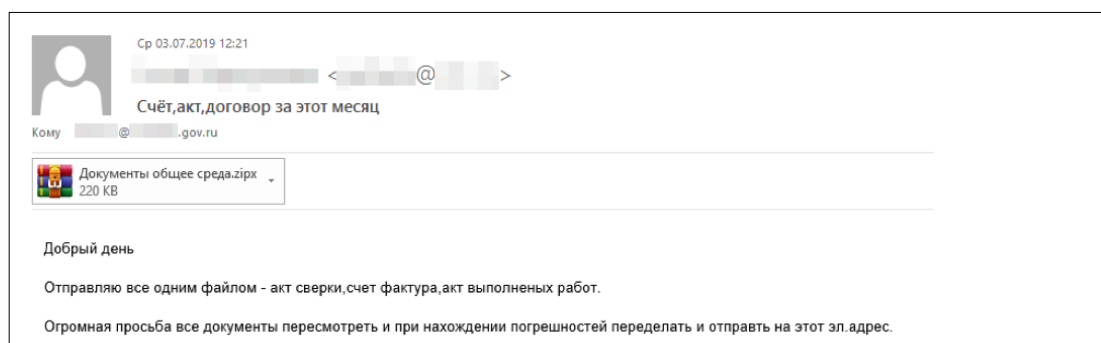


Рисунок 15. Фишинговое письмо группы RTM в адрес российской правительственной организации

Специалисты PT ESC отмечают атаки на госучреждения со стороны группы Gamaredon. Атакующих интересуют только украинские госструктуры, поэтому на их контрольных серверах настроена фильтрация обращений по географическому признаку. В своих атаках группа использует цепочку скриптов, которые загружают на компьютер жертвы утилиту для удаленного управления Ultra VNC.



Рисунок 16. Фишинговое письмо группы Gamaredon якобы от ОБСЕ

В течение III квартала эксперты PT ESC фиксировали атаки группы APT-C-35 (она же Donot). В ходе фишинговых рассылок жертвы получали офисный документ со ссылкой на файл в формате RTF с эксплойтом для уязвимости [CVE-2018-0802](#) в Microsoft Equation. На скомпрометированные компьютеры устанавливались модули вредоносного ПО [uty](#).

Операторы шифровальщиков также нацелены на госучреждения. Они совершают атаки в надежде получить солидные суммы выкупа за восстановление зашифрованных файлов, причем их аппетиты все время растут. Помимо атак Sodinokibi на органы самоуправления штата Техас, о которых мы писали выше, в III квартале по городам США прокатилась волна атак шифровальщика Ryuk. Известно, что администрация города Ла Порт в штате Индиана [заплатила](#) киберпреступникам выкуп в размере 130 тыс. долл. США. От администрации города Нью-Бедфорд, штат Массачусетс, злоумышленники [потребовали](#) выкуп в размере 5,3 млн долл. США, однако сделка не состоялась.

В 2018 году [мы писали об атаках](#) на интернет-портал Click2Gov, который используют во многих американских городах для оплаты муниципальных услуг. В III квартале 2019 года [наблюдалась вторая волна атак](#) на сервис. В августе жертвами стали восемь городов, шесть из которых ранее уже становились жертвами атак на Click2Gov.

Промышленные компании

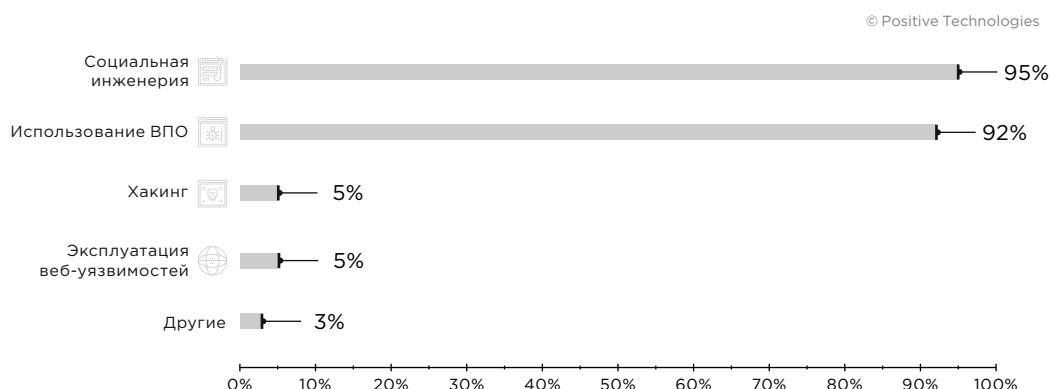


Рисунок 17. Методы атак на промышленные компании в Q3 2019

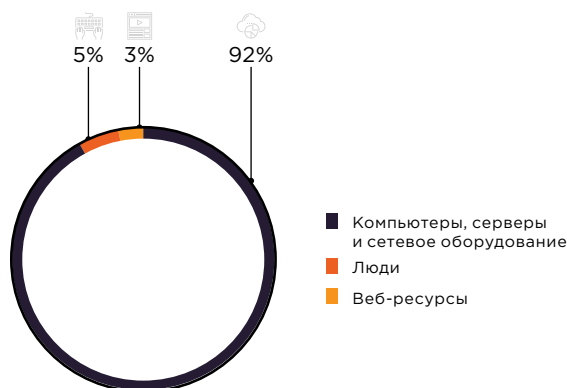


Рисунок 18. Объекты атак

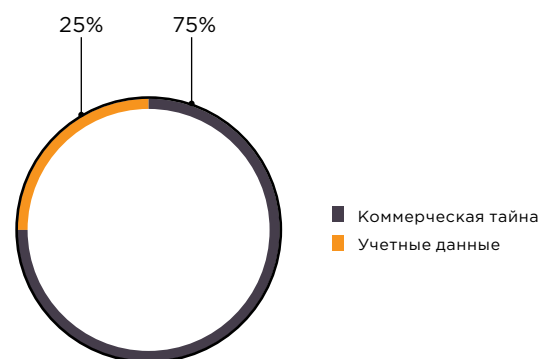


Рисунок 19. Украденные данные

В III квартале специалисты PT ESC фиксируют атаки APT-группы TA505 на американские компании пищевой промышленности, фармацевтические компании, на поставщиков медицинского оборудования. Кроме того, группировка атаковала промышленные и энергетические компании в Южной Корее и на Тайване, а также высокотехнологичные инженеринговые компании в ряде европейских стран. Злоумышленники рассылали фишинговые письма с офисными документами, которые заражали компьютеры жертв ВПО для удаленного управления FlawedAmmyu. Кроме того, в июле наши эксперты обнаружили рассылки в адрес промышленных компаний в Южной Корее, в ходе которых жертвы заражались трояном ServHelper. Вредоносное ПО злоумышленники маскировали под файлы с расширением .iso. Эксперты PT ESC выделяют две модификации ServHelper: первая может использоваться как полноценное ВПО для удаленного управления, вторая выполняет роль загрузчика легитимного ПО для администрирования NetSupport Manager.

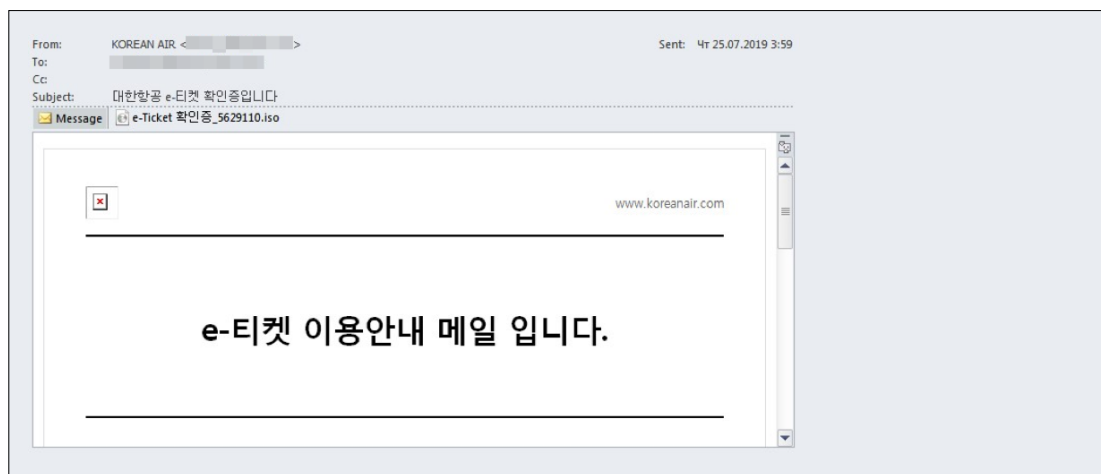


Рисунок 20. Фишинговое письмо TA505 в адрес корейской промышленной компании

Группировка RTM продолжает атаковать промышленный и топливно-энергетический комплексы России и стран СНГ. Формат фишинговых рассылок не претерпел изменений: это по-прежнему письма, якобы содержащие служебные записки, договоры, акты сверки. В течение квартала группа периодически меняла способ доставки трояна. В начале июля мы зафиксировали несколько рассылок с загрузчиком, скачивающим основной троян с удаленного сервера. Далее вплоть до конца августа вложения из фишинговых писем выполняли роль дроппера: основной троян устанавливался без загрузчика. Однако с конца лета группа RTM вновь использует загрузчик. С его помощью на скомпрометированный компьютер доставляются инфостилер Pony и основной троян RTM.

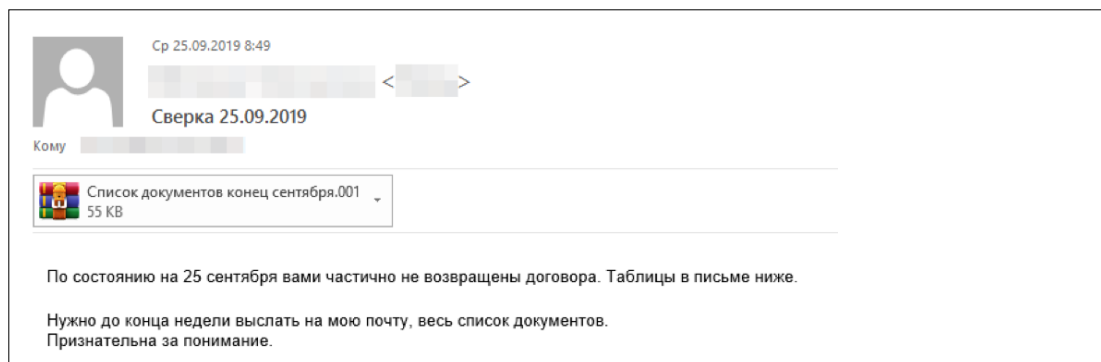


Рисунок 21. Фишинговое письмо группы RTM в адрес российской топливно-энергетической компании

В августе стало известно об атаке шпионского трояна LokiBot на американскую промышленную компанию. Зловред был доставлен в инфраструктуру предприятия в электронном письме якобы от представителя контрагента.

Восстановление инфраструктуры после целенаправленной атаки на промышленное предприятие может потребовать больших временных и финансовых затрат. В конце квартала немецкий концерн Rheinmetall — крупный производитель военного оборудования — объявил, что стал жертвой кибератаки. Это повлекло за собой нарушение бизнес-процессов крупных заводов компании в Бразилии, Мексике и США. Финансовые потери из-за простоя оцениваются в несколько миллионов евро в неделю; на восстановление, по оценкам специалистов Rheinmetall, потребуется от двух до четырех недель.

Финансовые организации

© Positive Technologies

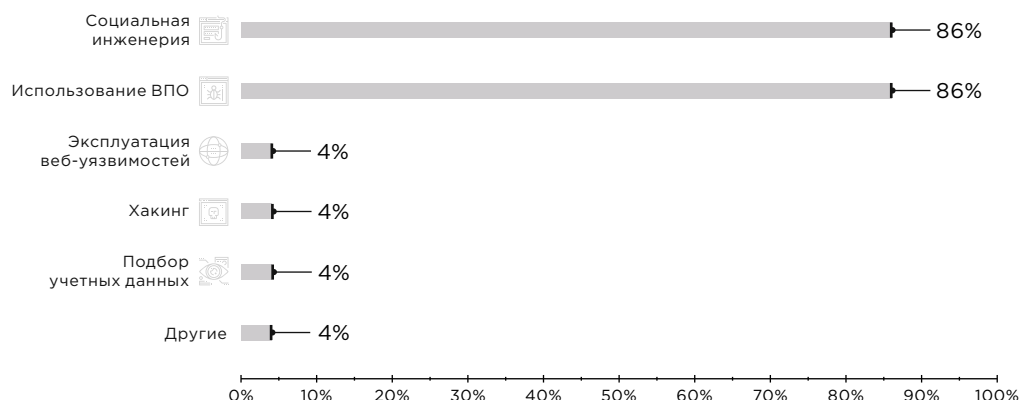


Рисунок 22. Методы атак на финансовые организации в Q3 2019

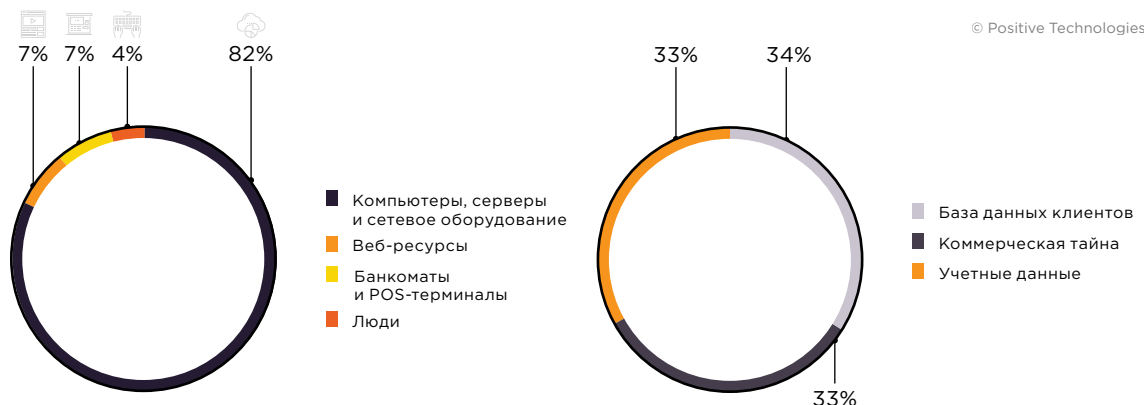


Рисунок 23. Объекты атак

Рисунок 24. Украденные данные

Финансово мотивированная АРТ-группа Cobalt по-прежнему активна. Специалисты Check Point в III квартале отметили атаки Cobalt на банки в Казахстане. Эксперты РТ ESC зафиксировали фишинговые рассылки в адрес российских и европейских банков. Письма носят целенаправленный характер (spear phishing), тщательно подготовлены и оформлены. Например, в июле группировка делала рассылку со взломанного электронного адреса сотрудника одного из московских аэропортов.



Рисунок 25. Вредоносное вложение из фишингового письма Cobalt

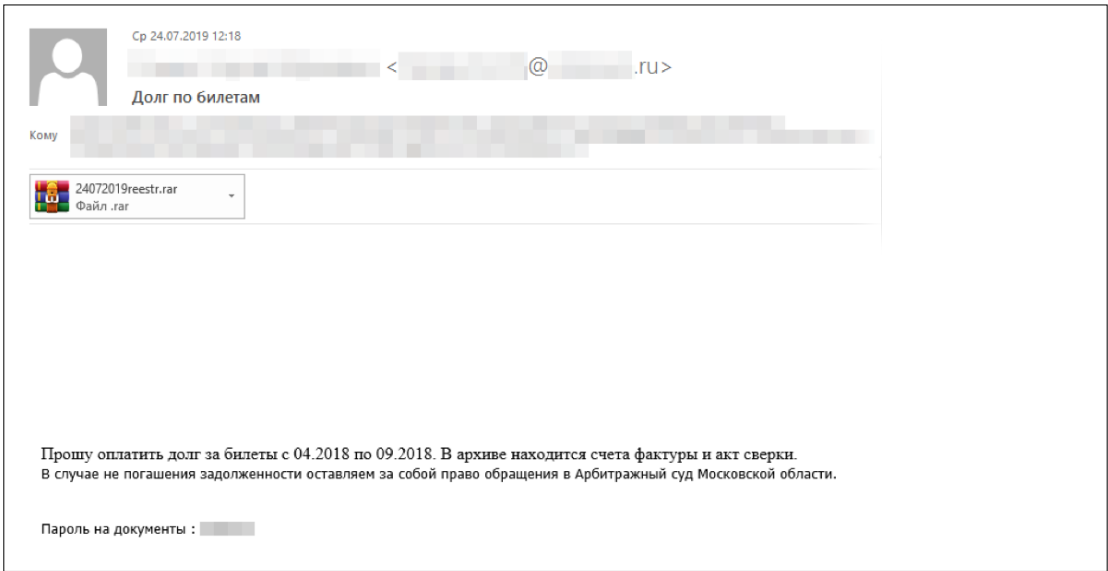


Рисунок 26. Фишинговое письмо Cobalt якобы от лица сотрудника аэропорта

В первой половине сентября эксперты РТ ESC зафиксировали фишинговые рассылки АРТ-группы TA505 в европейские и африканские банки. В качестве вложения к письмам злоумышленники использовали офисные документы с макросами. Они извлекают, записывают в систему и запускают файл в формате DLL — новый загрузчик вредоносного ПО FlawedAmmyu.

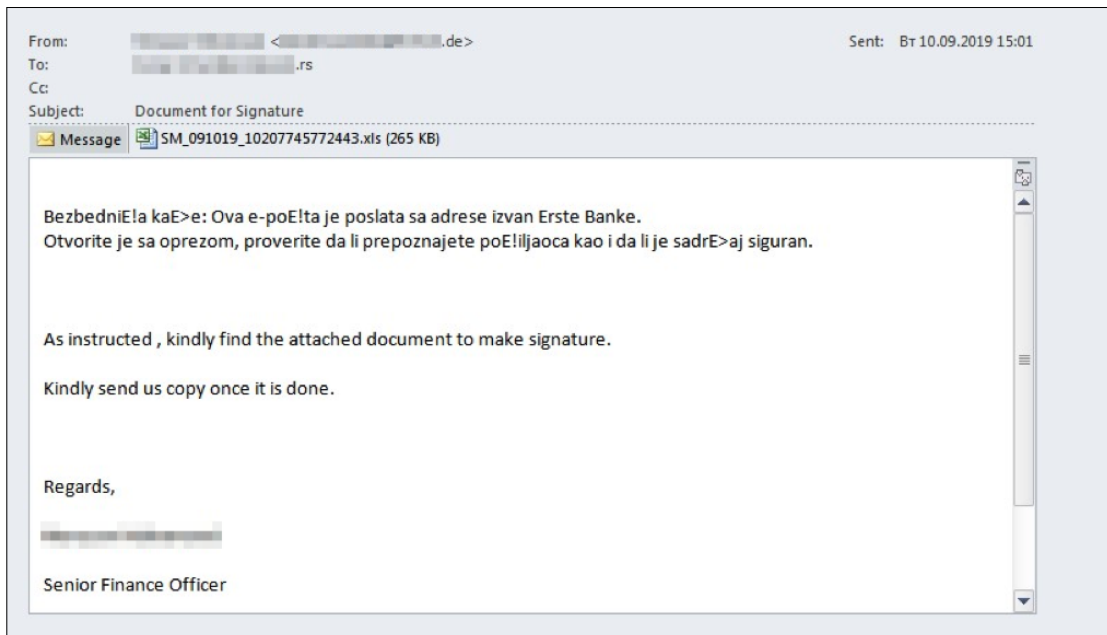


Рисунок 27. Фишинговое письмо группы TA505 в один из сербских банков

Группа RTM, действия которой преимущественно направлены на промышленный сектор, регулярно предпринимает попытки атаковать финансовые организации. В III квартале специалисты PT ESC зафиксировали фишинговые рассылки этой группы в банки России и Белоруссии.

Наука и образование

© Positive Technologies

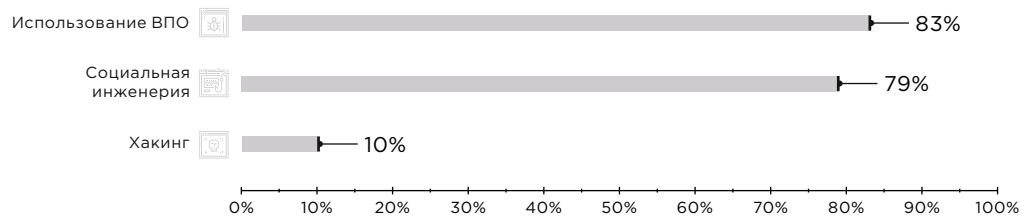


Рисунок 28. Методы атак на научные и образовательные организации в Q3 2019

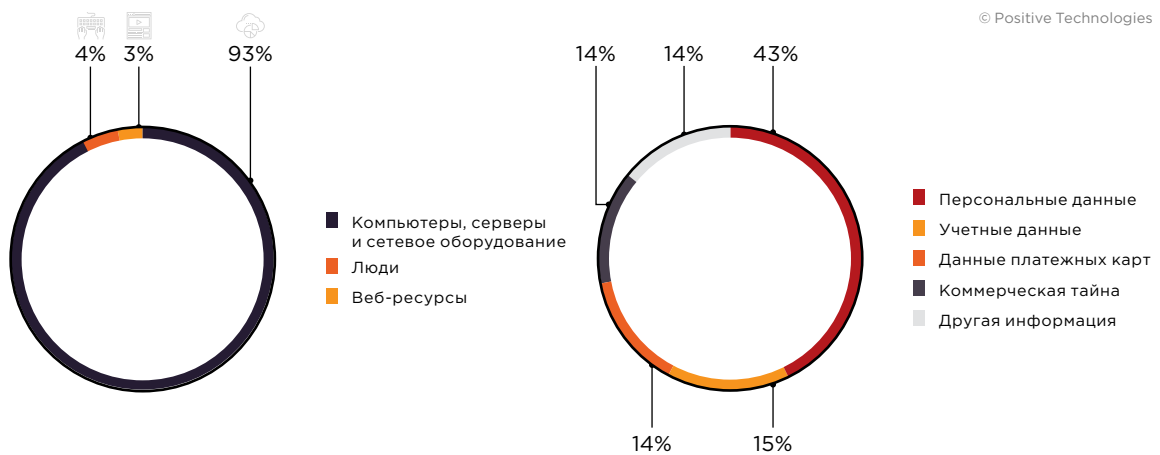


Рисунок 29. Объекты атак

Рисунок 30. Украденные данные

В III квартале 2019 года доля атак на научные и образовательные организации выросла до 9% против 6% во II квартале. Одна из возможных причин — начало учебного года. Мы отмечаем многочисленные атаки троянов-шифровальщиков на школы. Так, из-за серии кибератак в американском штате Луизиана было решено вести чрезвычайное положение.

Возобновила свою деятельность АPT-группа Cobalt Dickens, которая ведет охоту за интеллектуальной собственностью. Эксперты Secureworks сообщили, что среди адресатов, которым группа регулярно отправляет фишинговые письма, числятся 60 различных учебных заведений. В фишинговых письмах злоумышленники заманивали жертв на фальшивые сайты библиотек, где пользователям предлагалось авторизоваться. В результате ввода учетных данных в поддельную форму логины и пароли попадали в руки злоумышленников.

Летом 2019 года специалисты Microsoft обнаружили новое вредоносное ПО, получившее название Nodersok. Большая часть заражений этим ВПО (42%) приходится на сферу образования. Специалисты отмечают, что заражения происходят через сайты с вредоносной рекламой. Компрометация начинается с загрузки файла в формате HTA, после чего в результате многоступенчатой атаки на компьютер жертвы устанавливается ВПО, превращающее его в прокси-сервер для передачи вредоносного трафика.

Как защититься организации

Г 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).

Г 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.

Г Об исследовании

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

В рамках отчета массовые инциденты (например, вирусные атаки, в ходе которых злоумышленники проводят многоадресные фишинговые рассылки) рассматриваются 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.

Методы 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 или 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 исследованием 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: в Пакистане, Бангладеш, на Шри-Ланке, Мальдивах, в Мьянме, Непале и странах Шанхайской организации сотрудничества. Злоумышленники выдают себя за представителей государственных учреждений, военных ведомств и телекоммуникационных компаний.

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.

Cobalt известна с 2016 года атаками на организации кредитно-финансовой сферы. Начиная с хищений 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 атаки внутри сети. Основной способ проникновения в сеть компании — фишинговые рассылки с вредоносными вложениями разных форматов: исполняемые файлы, документы Microsoft Office с макросами или эксплойтами, LNK-файлы, архивы с паролями, внутри которых исполняемые файлы.

Cobalt Dickens известна с 2017 года. В 2019 году группа атаковала по меньшей мере 380 вузов в более чем 30 странах с целью получения доступа к интеллектуальной собственности. Сотрудникам университетов и учащимся злоумышленники рассылали фишинговые письма от имени библиотек. Письма содержали ссылки на фишинговые страницы, предназначенные для перехвата учетных данных, которые затем использовались хакерами для доступа к научным работкам пользователей.

eGobbler, известная с начала 2019 года, эксплуатировала уязвимость CVE-2019-5840 браузера Chrome для показа вредоносной рекламы пользователям мобильных устройств на базе iOS. Во второй половине 2019

года группировка расширила свои цели до пользователей всех браузеров на движке WebKit, в том числе десктопных версий, работающих под Windows, Linux и macOS. Так, в период с 1 августа по 23 сентября злоумышленникам удалось показать потенциальным жертвам около 1,16 миллиарда заманчивых предложений, ведущих на мошеннические и фишинговые сайты.

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

KONNI активна минимум с 2014 года. Свое название получила в честь вредоносной программы KONNI, которую злоумышленники использовали в своих атаках. ВПО позволяет хакерам красть файлы с чувствительной информацией, перехватывать и сохранять пароли, вводимые пользователями, снимать скриншоты и выполнять команды на зараженном компьютере. Основной мотив группировки — шпионаж и получение доступа к данным.

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 одного из центров управления использовала домены в зоне .bit. Это специальная зона, созданная на базе технологии блокчейн-на Namecoin: защищенная от цензуры и принудительного изъятия доменов альтернатива традиционным регистраторам DNS. Особенности архитектуры блокчейна позволили специалистам PT Expert Security Center разработать алгоритм отслеживания регистрации новых доменов группировки RTM (или смену 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 (а иногда и до) их использования злоумышленниками.

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, GlobeImposter и др. С весны 2018 года группа использует remote access trojan — FlawedAmmyy, 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.