Сергей ГОЛОВАНОВ,
ведущий антивирусный эксперт,
«Лаборатория Касперского»

Киберугрозы в эпоху новых финансовых технологий

Деньги всегда были главной мотивацией подавляющего большинства киберпреступных групп. Свою охоту на чужие финансы компьютерные злоумышленники начали много лет назад, преимущественно с индивидуальных пользователей. Однако по мере развития технологий в финансовой сфере интересы киберпреступников плавно переключились на организации, у которых в случае успешной атаки можно отнять несоизмеримо больше денег.

В 2018 году самой активной оказалась киберпреступная группа Lazarus. Это название было у всех на слуху в связи с попыткой ограбления центрального банка Бангладеш. В зону приоритетов Lazarus сегодня входят банки, финтех-компании, криптовалютные биржи, POS-системы, банкоматы, а география активности охватывает десятки стран от Азии до Латинской Америки. Столь широкий разброс интересов иллюстрирует основные тенденции, которые мы наблюдаем в области развития киберугроз для финансовой отрасли.

РЫНОК КРИПТОВАЛЮТ — НОВАЯ МИШЕНЬ

Рост популярности и стоимости криптовалют, достигший своего пика около года назад, спровоцировал киберпреступников вкладывать ресурсы в разработку новых техник и атак на незнакомые им прежде цели. Во-первых, как показывают итоги 2018 года, они массово начали создавать и распространять программы-майнеры, которые, по нашим подсчетам, обошли даже самую громкую угрозу последних лет — шифровальщиков. Тренд был настолько повальным, что встречались примеры перепрофилированного вредоносного ПО, возможности которого были расширены функциями для скрытой добычи криптовалюты на зараженных компьютерах. В общей сложности, по нашим данным, в 2018 году майнерами были атакованы более 5 млн уникальных пользователей.

Компьютерные злоумышленники уже давно и очень активно интересуются традиционными биржами, и, разумеется, они не могли обойти вниманием новый их подвид — криптобиржи. Одной из наиболее интересных была атака AppleJeus (опять же дело рук Lazarus), нацеленная на трейдеров криптовалюты в Азии. Злоумышленники создали специальное ПО, которое выглядело абсолютно легитимно и обладало полезными

функциями, но в определенный момент программа загружала апдейт, который на поверку оказывался бэкдором.

НОВЫЕ ПОДХОДЫ В АТАКАХ НА БАНКОМАТЫ

Одна из главных тенденций последних лет — развитие методов атак на банкоматы. В 2018 году мы обнаружили шесть новых семейств, и в итоге сегодня их насчитывается более 20. Многие их них эволюционируют, обрастают новыми функциями и возможностями. А началось все в 2014 году с громких операций Tyupkin и Carbanak (в обоих случаях подавляющее большинство жертв находилось в Восточной Европе). Тогда злоумышленники применяли уникальное вредоносное ПО, которые было создано именно для этих ограблений и обладало техническими возможностями для маскировки.

С тех пор многое изменилось. Теперь готовые программы и инструменты для атаки на банкоматы можно найти в свободной продаже в Даркнете. Например, в 2017 году мы обнаружили, что за 5000 долларов любой желающий мог приобрести вредоносное ПО Cutlet Maker и пойти с ним грабить банкомат. Уникальность ситуации заключалась в том, что помимо готового инструментария атакующий получал в комплекте пошаговую инструкцию. Таким образом, воспользоваться Cutlet Maker мог абсолютно любой, даже технически неподкованный злоумышленник. Все, что ему было нужно, — получить доступ к USB-порту банкомата, загрузить в ОС вредоносное ПО и дальше, следуя инструкции, по очереди использовать все содержащиеся в нем компоненты. Создатели Cutlet Maker настолько позаботились о своих «клиентах», что даже снабдили его специальным приложением, которое отображало количество и номинал банкнот в кассетах банкомата, благодаря чему злоумышленники мог действовать не вслепую, по очереди снимая деньги из каждой кассеты, а сразу выбирать ячейку, содержащую самую большую сумму.

Однако киберпреступники пошли еще дальше. В 2018 году в рамках серии киберограблений KoffeyMaker они опустошали банкоматы в странах Восточной Европы, имея в своем арсенале лишь ноутбуки и пару легальных программ. Одной из них оказалась модифицированная версия утилиты для тестирования работы диспенсера, выдающего деньги, — KDIAG (ранее той же самой версией этой программы пользовались киберпреступники из группы Carbanak). Все необходимые инструменты и инструкции для ограбления можно было скачать на специализированных сайтах. Для проведения атаки злоумышленнику было необходимо вскрыть банкомат и напрямую подключить свой ноутбук к диспенсеру через USB. После этого ноутбук оставался в корпусе банкомата, а грабитель закрывал его и уходил. Далее он удаленно запускал измененную версию KDIAG — в заданный момент она позволяла выдать все содержащиеся в диспенсере деньги, надо было лишь подойти и забрать их. К слову, ноутбук, остававшийся на время ограбления в корпусе банкомата, преступник по завершении операции забирал. Так никаких улик и следов преступления не оставалось.

КОМПЬЮТЕРНЫЕ ЗЛОУМЫШЛЕННИКИ ДАВНО И ОЧЕНЬ АКТИВНО ИНТЕРЕСУЮТСЯ ТРАДИЦИОННЫМИ БИРЖАМИ, И, РАЗУМЕЕТСЯ, ОНИ НЕ МОГЛИ ОБОЙТИ ВНИМАНИЕМ НОВЫЙ ИХ ПОДВИД — КРИПТОБИРЖИ

ВСЕОБЩАЯ МОБИЛИЗАЦИЯ

По нашим наблюдениям, в последнее время часть банковских троянцев перестала атаковать пользователей онлайн-банкинга на традиционных ПК и переключилась на мобильные платформы. К примеру, за прошедший год количество мобильных банковских троянцев выросло более чем в два раза. Пик заражений пришелся на второй квартал 2018 года. Почему так произошло, неизвестно, но основным виновником сложившейся ситуации оказался мобильный банковский троянец Asacub. Вообще у него долгая история — стоящая за ним группировка орудует уже больше трех лет, а сам Asacub эволюционировал из SMS-троянца. В свое время его создатели усложнили логику зловреда и занялись его массовым распространением. Вектор при этом был выбран тот же, что и в самом начале, — социальная инженерия через SMS. А источником действующих номеров, владельцы которых зачастую ждали сообщений от незнакомых абонентов, стали популярные доски объявлений. Далее срабатывала лавинная техника распространения, и уже устройства жертв троянца сами становились распространителями заразы — Asacub рассылал себя сам по всей телефонной книге жертвы. По нашим данным, в 2018 году каждый день с этим троянцем сталкивалось около 40 тысяч пользователей, а 98% случаев заражения пришлось на Россию.

ФИШИНГ ПО-НОВОМУ

В прошлом году мы зафиксировали хорошо спланированную волну рассылок фишинговых писем, с помощью которых были атакованы по меньшей мере 400 промышленных компаний, преиму-

щественно на территории России. Как правило, рассылавшиеся мошенниками письма имели вид рабочей переписки на тему оплаты услуг, проведения платежей, сверки документов и других финансовых вопросов. При этом киберпреступники обращались к каждому сотруднику по фамилии, имени и отчеству, формировали индивидуальные письма и учитывали специфику атакуемых организаций.

Выяснилось, что основная цель киберпреступников — кража денежных средств со счетов организаций. Если получатель их письма открывал вложение или переходил по предложенной ссылке, то на его компьютере устанавливалось модифицированное ПО для удаленного администрирования, которое давало злоумышленникам контроль над зараженными системами. Далее киберпреступники находили и изучали документы о проводимых закупках и ПО для осуществления бухгалтерских операций. Полученная информация помогала им, в частности, подменять реквизиты платежных поручений, по которым должна была производиться оплата выставленных счетов, и средства уходили в конечном итоге сторонним получателям.

КОЕ-ЧТО ЕЩЁ…

В последние полтора года мы наблюдали принципиально новый вид атак на банки в Восточной Европе — вредоносное ПО проникало в корпоративную сеть с неизвестного устройства, в буквальном смысле подброшенного злоумышленниками. На сегодня известно по крайней мере о восьми банках, которые были ограблены таким образом, а примерный ущерб от произошедших инцидентов составил несколько десятков миллионов долларов. Эта волна операций получила название DarkVishnya.

В каждом зафиксированном случае, чтобы начать атаку, киберпреступники подбрасывали свое устройство в здание финансовой организации и физически подключали его к корпоративной сети компании. Злоумышленники использовали три вида гаджетов: ноутбук (как правило, недорогой нетбук), Raspberry Pi (одноплатный компьютер размером с кредитную карту) и Bash Bunny (специально разработанный инструмент для автоматизации и проведения USB-атак). В ходе атак киберпреступники пытались получить доступ к общим сетевым папкам, веб-серверам и так далее. После успешного закрепления в инфраструктуре финансового учреждения злоумышленники использовали легитимное ПО для удаленного управления. Поскольку киберпреступники применяли бесфайловые методы и PowerShell, они обходили белые списки и доменные политики. Украденные данные использовались для подключения к серверам и рабочим станциям, предназначенным для осуществления платежей или содержащим другую полезную для злоумышленников информацию. А похищенные денежные средства выводились, например, через банкоматы.

КАК ОТ ВСЕГО ЭТОГО ЗАЩИТИТЬСЯ

Поскольку угроз много и они подступают по разным фронтам, то и защищаться от них имеет смысл сразу по нескольким направлениям. Ключевые слова в кибербезопасности сегодня — комплексность и многоуровневость. Это касается и подходов к организации защиты, и собственно самих защитных технологий и решений.

Если речь идет об отдельных пользователях, то здесь важны знания и навыки в распознавании киберугроз. Не стоит забывать, что излюбленный метод компьютерных злоумышленников — социальная инженерия. А значит, не нужно реагировать на сомнительные сообщения в электронной почте, соцсетях и мессенджерах. Не надо открывать вложения или переходить по ссылкам, если что-то вызывает у вас подозрение. Если странное сообщение пришло от вашего знакомого, всегда можно с ним связаться проверенным способом и уточнить детали.

Знания — это прекрасный инструмент защиты и на уровне корпоративной сети любой организации. Тренинги и повышение осведомленности сотрудников о киберугрозах помогут существенно снизить риск киберинцидентов по причине человеческого фактора (а это почти половина всех случаев).

Что касается защитных технологий, то, естественно, они должны быть актуальными и способными отразить не только распространенные, но и еще не известные угрозы. Хорошие защитные решения должны выявлять и блокировать любые попытки фишинга, вредоносной активности приложений, неавторизованного подключения к сети. Системы контроля доступа в сеть и функции контроля устройств помогут предотвратить инциденты, подобные DarkVishnya. А для противодействия ограблениям банкоматов необходимо надежно защитить часть соединения диспенсера и компьютера банкомата — никто посторонний не должен получить к ним доступ. Если позволяют технические возможности, следует настроить шифрование между диспенсером и компьютером — эта мера поможет избежать подмены управляющего центра банкомата.

ЗА ПРОШЕДШИЙ ГОД КОЛИЧЕСТВО МОБИЛЬНЫХ БАНКОВСКИХ ТРОЯНЦЕВ ВЫРОСЛО БОЛЕЕ ЧЕМ В ДВА РАЗА. ПИК ЗАРАЖЕНИЙ ПРИШЕЛСЯ НА ВТОРОЙ КВАРТАЛ 2018 ГОДА