АТАКА НА БАНКИ

Высокая степень проникновения информационных технологий в ключевые отрасли экономики Беларуси помимо воли приобретает и обратную сторону. Назревает актуальность общемировых трендов информационной безопасности. Эту особенность отметил Александр Панков, директор по развитию бизнеса компании Positive Technologies в Республике Беларусь.

Во многих странах мира активно применяются решения Positive Technologies для оценки уровня безопасности своих сетей и приложений. Благодаря многолетним исследованиям, специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Александр Панков поделился планами на развитие бизнеса компании в Беларуси и особо подчеркнул, что эксперты оценивают республику в качестве одного из наиболее активно развивающихся рынков среди стран СНГ как в сфере цифровизации общества, так и с точки зрения прогресса информационных технологий.

– Цели компании на ближайшие годы предусматривают активную работу с крупным бизнесом и госструктурами республики в части повышения уровня киберзащищенности коммерческих и государственных предприятий, – сказал Александр Панков. – Мы планируем поэтапно вывести на рынок все экспертные сервисы Positive Technologies – от тестов на проникновение и аудита защищенности до реагирования и расследования инцидентов безопасности, а также полный портфель продуктов компании. К сегодняшнему дню система контроля защищенности и соответствия стандартам MaxPatrol 8 и защитный экран уровня приложений PT Application Firewall уже получили подтверждение соответствия требованиям технического регламента ТР 2013/027/BY в Оперативно-аналитическом центре при Президенте Республики Беларусь. Сертификация ряда других продуктов ожидается в ближайшее время…

На пике текущего года компания Positive Technologies опубликовала крайне интересное исследование с анализом высокотехнологичных атак на банки в первой половине 2018 г. В предоставленном в редакцию обзоре «Атака на банки» эксперты Positive Technologies поделились опытом решений для предотвращения online-мошенничества.

В последние несколько лет в средствах массовой информации регулярно появляются заголовки о новых ограблениях банков. Фигурирующие в них названия преступных группировок обычно известны каждому специалисту по безопасности, а на счету некоторых из этих преступников – целый ряд многомиллионных краж. Высокие гонорары и относительно низкий на сегодняшний день риск обнаружения способствуют развитию киберпреступности: несмотря на то, что отдельные группировки задерживаются правоохранительными органами, их место занимают другие.

Преступники быстро адаптируются к меняющейся среде, неустанно следят за публикациями о новых уязвимостях и успевают эксплуатировать их гораздо быстрее, чем службы безопасности банков установят соответствующие обновления. На подпольных форумах

в интернете существует открытый доступ к ПО для проведения атаки с подробными инструкциями, есть возможность заручиться поддержкой недобросовестных сотрудников банков и преступных сообществ, специализирующихся на отмывании незаконно полученных денег. Складывается ситуация, когда злоумышленник может похитить миллионы долларов, проникнув в сеть банка, которая, казалось бы, должна иметь высокий уровень защиты.

Как на самом деле обстоит ситуация с информационной безопасностью в банковской сфере? Как хакерам удается обойти существующие системы защиты, какие недостатки в механизмах безопасности позволяют им прочно закрепиться в инфраструктуре банка и проводить мошеннические операции, до последнего момента оставаясь незамеченными службой безопасности?

В данном исследовании мы постараемся ответить на эти вопросы. В заключение оценим, с учетом выявленных уязвимостей, сколько банков сегодня могут подвергнуться атаке.

Как обирают банки

По оценкам Сбербанка, ежегодные убытки от кибератак в России уже составляют около 600 млрд руб., а во всем мире эта сумма приближается к триллиону долл. США. Мы наблюдаем атаки на системы межбанковских переводов, карточный процессинг, управление банкоматами, интернет-банкинг, платежные шлюзы.

Выбор целей достаточно широк: при наличии должных знаний и технических средств доступ к таким системам может принести злоумышленникам более весомое вознаграждение, чем мошенничество в отношении клиентов банка. Для хищения денежных средств преступникам требуется проникнуть в инфраструктуру банка, безопасность которой обязана находиться на высоком уровне. Но, как мы видим, в СМИ продолжают появляться сообщения о новых инцидентах.

Волна атак на карточный процессинг прошла в начале 2017 г. в ряде стран Восточной Европы. Проникнув в инфраструктуру банка, преступники получали доступ к системам карточного процессинга и увеличивали лимит овердрафта карт, а также отключали системы антифрода, которые могли бы оповестить банк о мошеннических операциях. В ту же минуту их сообщники снимали наличные средства в банкоматах в другой стране. Средняя сумма хищения в каждом случае составила около 5 млн долл. США.

Двумя годами ранее схожую тактику применила группировка Metel. Пробравшись в инфраструктуру банка, преступники получили возможность отменять операции по картам и возвращать первоначальный баланс, в то время как их сообщники переходили от одного банкомата к другому, похищая миллионы рублей. Осенью 2017 г. злоумышленники атаковали банк Тайваня, совершив переводы на счета в Камбодже, Шри-Ланке и США.

Пока работа банков в Непале была приостановлена на время праздников, преступники осуществили вывод денег через систему межбанковских переводов SWIFT. Банкам удалось отследить транзакции и вернуть значительную часть похищенных средств лишь благодаря своевременному реагированию.

В начале декабря минувшего года в публичных источниках появилась информация о группировке MoneyTaker, которая проводила атаки на финансовые организации России и США в течение полутора лет. Тогда же появилась информация о первой атаке на систему SWIFT в российском банке «Глобэкс» (дочерняя компания Внешэкономбанка).

Группировки

Если рассматривать преступления за последние три года, то наиболее заметна деятельность группировок Cobalt (предположительно связаны с Buhtrap), Carbanak, Lazarus и Lurk.

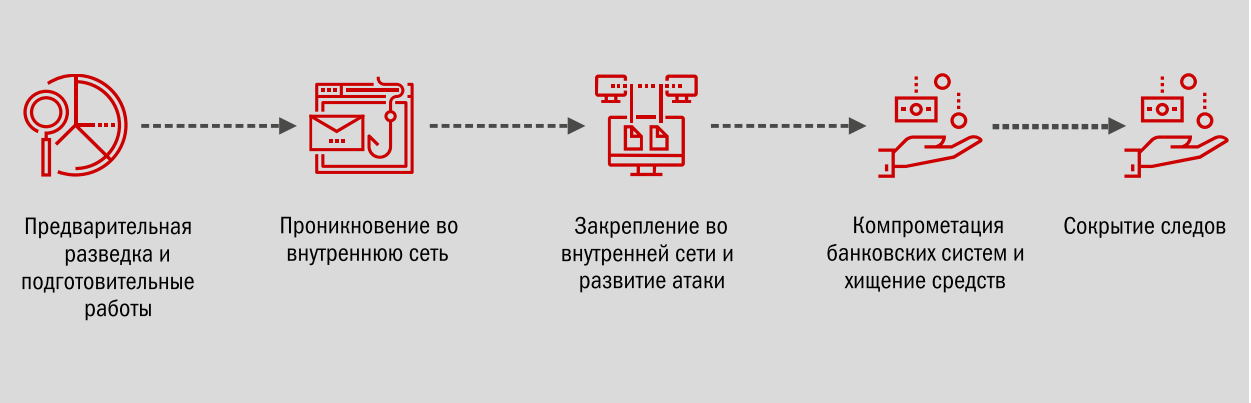

Схема основных этапов атаки

Например, преступная группа Cobalt известна своими атаками на финансовые организации СНГ, Восточной Европы и Юго-Восточной Азии, но в 2017 г. список регионов значительно расширился: были зафиксированы атаки в странах Западной Европы, Северной и Южной Америки. Большую часть атакованных финансовых организаций составляют банки, тем не менее в их число также входят фондовые биржи, инвестиционные фонды и другие специализированные кредитно-финансовые организации.

В банках целью злоумышленников является доступ к управлению банкоматами: отправляя в установленное время команды на выдачу наличных средств, преступники забирают из банкомата все содержимое без физического вмешательства в работу устройства. По оценкам ЦБ, в 2017 г. российские банки потеряли более 1,1 млрд руб. в результате действий группировки Cobalt.

Не меньшую известность получила и группировка Lazarus, которой приписывают одно из самых громких ограблений банка через систему SWIFT. В 2016 г. злоумышленники попытались вывести миллиард долларов из центрального банка Бангладеш, но из-за ошибки в платежном документе смогли похитить только 81 млн долл.

Специалистам по информационной безопасности хорошо знаком и троян Lurk, который на протяжении нескольких лет использовался для атак на системы дистанционного банковского обслуживания (ДБО). Члены преступной группировки были арестованы в 2016 г. Считается, что в общей сложности хакеры вывели из банков более 3 млрд руб.

Типовые схемы атак

Выбор цели злоумышленника во многом обусловлен технической подготовкой, имеющимися инструментами и знаниями внутренних процессов банка, которыми располагают преступники. Каждая из атак имеет свои особенности. В частности, действия преступников различаются на этапе вывода денежных средств, но присутствуют и общие черты. Злоумышленники действуют по довольно простым сценариям, состоящим из пяти основных этапов (см. схему на с. 41).

Первый этап достаточно длительный и трудоемкий: перед злоумышленниками стоит задача собрать о банке как можно больше информации, которая поможет преодолеть системы защиты. Для разведки также активно привлекаются недобросовестные сотрудники банков, готовые за вознаграждение поделиться информацией. При построении инфраструктуры и подготовке инструментов преступники могут нанимать сторонних исполнителей.

После всестороннего изучения жертвы и подготовки к атаке злоумышленники переходят ко второму этапу. Наиболее распространенным и эффективным методом проникновения в инфраструктуру банка является фишинговая рассылка электронных писем в адрес сотрудников банка, которая осуществляется как на рабочие, так и на личные адреса. Такой метод использует, например, группировка Cobalt, также его применяли Lazarus, Metel, GCMAN.

Другой вариант первичного распространения вредоносного ПО – взлом сторонних компаний, которые не столь серьезно относятся к защите своих ресурсов, и заражение сайтов, часто посещаемых сотрудниками целевого банка, как в случае с Lazarus и Lurk.

На третьем этапе развития атаки, когда преступники получают доступ к локальной сети банка, им необходимы привилегии локального администратора на компьютерах сотрудников и серверах. Успешность атак обусловлена недостаточным уровнем защищенности систем от внутреннего нарушителя.

После получения максимальных привилегий в ОС на узле преступники получают из памяти ОС учетные данные всех пользователей, подключавшихся к ней (идентификаторы, пароли или хеш-суммы паролей), и используют их для подключения к другим компьютерам в сети.

«БЕЛАРУСБАНК» И СЕТЬ АЗС «А-100» РЕАЛИЗОВАЛИ НОВЫЙ СЕРВИС

ОАО «АСБ Беларусбанк» и ОДО «Астотрейдинг» совместно с компанией АССИСТ, партнером банка по оказанию услуг интернет-платежей, реализовали возможность оплаты топлива через мобильное приложение aisDrive. Теперь держатели платежных карточек могут с помощью телефона оплатить топливо в сети АЗС «А-100», не отходя от автозаправочной колонки и автомобиля.

АЛЬФА-БАНК: АВТОМАТИЗАЦИЯ КОНТАКТ-ЦЕНТРА

Обращения в контакт-центр в Альфа-Банке переходят на частичную автоматизацию. Уже сейчас можно позвонить и узнать баланс по карточке без участия оператора. В дальнейшем возможности получения информации или совершения операций будут расширяться. В планах Банка – автоматизировать ответы на вопросы о действующих кредитах.

Перемещение между узлами обычно осуществляется посредством легитимного ПО и встроенных функций ОС (например, PsExec или RAdmin), т. е. с помощью тех средств, которые не должны вызвать подозрений, поскольку их ежедневно пользуют администраторы. Группировка Cobalt прибегала также к фишинговым рассылкам внутри банка, отправляя письма от имени реальных сотрудников с их рабочих станций.

Если злоумышленникам удастся получить привилегии администратора домена, они смогут в дальнейшем беспрепятственно перемещаться по сети, контролировать компьютеры сотрудников, серверы и службы инфраструктуры банка.

На четвертом этапе производится компрометация банковских систем. Закрепившись в сети, преступники должны понять, на каких узлах находятся искомые банковские системы и как удобнее получить к ним доступ. Рабочие станции пользователей исследуются в поисках файлов, указывающих на работу с банковскими приложениями.

Дополнительную помощь преступникам могут оказать ресурсы, которые содержат информацию об инфраструктуре, например системы мониторинга, которые используют в своей работе администраторы, или техническая поддержка пользователей. Преступники могут долго находиться в банковской системе, оставаясь незамеченными, собирать информацию об инфраструктуре и процессах, не спеша изучать выбранные для проведения атак схемы и наблюдать за действиями сотрудников. Это означает, что кражу денег можно предотвратить, если вовремя выявить факт компрометации, даже в том случае, когда преступники уже проникли и закрепились в сети банка.

На пятом этапе преступники скрывают следы. Хотя злоумышленники переключаются на использование скриптов, выполняющихся в оперативной памяти, в системе остаются признаки их присутствия: записи в журналах событий, изменения в реестре и другие зацепки.

Волна атак вирусов-шифровальщиков, с которой мир столкнулся в 2017 г., была превосходным примером того, как легко могут быть уничтожены данные крупной компании, и теперь арсенал хакеров пополняется модификациями вирусов, которые распространяются по рабочим станциям сети и шифруют содержимое жестких дисков. Поскольку восстановить зашифрованные данные в большинстве случаев не представляется возможным, банк несет ущерб, вызванный вынужденным простоем бизнес-процессов, который может оказаться гораздо значительнее ущерба непосредственно от хищения денежных средств.

Тесты на проникновение

Рассмотрим, насколько вероятны описанные выше атаки. Тестирование на проникновение проводится для оценки реального уровня защищенности организации.

Ежегодно мы проводим десятки работ по тестированию на проникновение в различных организациях. Для этого исследования мы выбрали 12 наиболее информативных проектов, выполненных нами в банках за последние три года, в ходе которых накладывались минимальные ограничения на действия экспертов.

Основные уязвимости и недостатки механизмов защиты, которые распространены на сетевом периметре банков, можно разделить на четыре категории: уязвимости веб-приложений, недостаточная сетевая безопасность, недостатки конфигурации серверов и недостатки управления учетными записями и паролями (см. диаграмму на с. 44).

Следует учитывать, что наличие уязвимостей на периметре системы еще не означает, что их эксплуатация позволит проникнуть во внутреннюю сеть. В целом уровень защиты сетевого периметра в банковской сфере значительно выше, чем в остальных компаниях. За три года в рамках внешнего тестирования на проникновение

БАНК «РЕШЕНИЕ»: ПРЕДСТАВЛЕНА ВИРТУАЛЬНАЯ КАРТА С КЕШБЭКОМ

В июне появилась виртуальная карта, которая позволяет совершать платежи в системе «Расчет» (ЕРИП), оплачивать товары в интернет-магазинах и рассчитываться за онлайн-такси не только в Беларуси, но и за рубежом.

Виртуальную карту V-BANKING, эмитентом которой является Банк «Решение», можно оформить удаленно через мобильное приложение v-banking.

БАНК МОСКВА-МИНСК ЗАПУСТИЛ НОВУЮ ВЕРСИЮ МОБИЛЬНОГО ПРИЛОЖЕНИЯ MMBANK-ONLINE

Теперь его пользователи могут свободно настраивать рабочий стол и задействовать подсказки из истории операций, а владельцы iPhone X – еще и проходить аутентификацию посредством Face ID.

При выборе депозита приложение позволяет воспользоваться фильтром, а при оформлении карточки сразу предлагает определиться с пакетом обслуживания. С помощью геолокации мобильный банк также подсказывает ближайшее отделение, в котором можно забрать карточку.

Уязвимости, использовавшиеся для доступа к банковскому ПО

доступ к внутренней сети был получен в 58 % систем, а для банков этот показатель составил лишь 22 %. Во всех случаях получению доступа способствовали уязвимости в веб-приложениях, причем злоумышленнику потребовался бы всего один шаг для достижения цели. В одном банке было выявлено два вектора проникновения, причем оба заключались в эксплуатации уязвимостей веб-приложения и недостатков конфигурации веб-сервера. Следовательно, преступные группировки смогли бы достичь цели в 22 % банков. Подобные способы проникновения использовали в своей деятельности, например, ATMitch и Lazarus.

22%

Указанный процент может быть несколько выше. В рамках тестирования не эксплуатируются уязвимости, которые могут нанести ущерб инфраструктуре заказчика. Например, использование устаревшего ПО в 67 % банков потенциально может позволить преодолеть периметр, однако эксплуатация этих уязвимостей может вызвать отказ в обслуживании (например, CVE-2012-2386, CVE-2013-6420, CVE-2015-5343).

67%

Уязвимости внутренней сети

В то время как банки сосредоточены на защите сетевого периметра, безопасность внутренней сети далека от совершенства. Здесь встречаются все те же проблемы, что и во внутренних сетях других компаний. Полный контроль над инфраструктурой был получен во всех исследуемых банках. При этом в 33 % банков, даже не обладая максимальными привилегиями в системе, возможно получить доступ к узлам, с которых осуществляется управление банкоматами, системам межбанковских переводов, карточному процессингу, платежным шлюзам.

Какие недостатки безопасности позволяют злоумышленникам развивать атаку вглубь банковской инфраструктуры? Типовые векторы атак базируются на двух основных недостатках – слабой парольной политике и недостаточной защите от восстановления паролей из памяти ОС.

Если на сетевом периметре словарные пароли встречаются почти в половине банков, то во внутренней сети от слабой парольной политики страдает каждая исследованная система, и в этом

БСБ БАНК: НОВАЯ ВЕРСИЯ СИСТЕМЫ «ИНТЕРНЕТ-БАНК»

Вышла новая версия системы «Интернет-Банк» (Bank-iT/ibank) БСБ Банка, которая дает возможность работать с валютной картотекой, а также отправлять реквизиты на почту контрагента. В меню «Валютный Маклер» появился новый раздел, позволяющий заключать сделки на внебиржевом рынке и договариваться с Банком о курсах по операциям с валютой в режиме онлайн.

НОВЫЕ ВОЗМОЖНОСТИ АИС «РАСЧЕТ-ЖКУ»

ОАО «НКФО "ЕРИП"» разработан программный комплекс «SC-Аналитика-light» (генератор отчетов) для расширения функциональных возможностей АИС «Расчет-ЖКУ». Генератор отчетов позволяет самостоятельно проектировать и хранить различные шаблоны отчетов, необходимых организациям, осуществляющим учет, расчет и начисление платы за жилищно-коммунальные услуги, а также поставщикам данных услуг.

По информации пресс-служб, официальных сайтов банковских организаций и других интернет-источников

отношении банки не отличаются от любой другой компании. Приблизительно в половине систем слабые пароли устанавливают пользователи, однако еще чаще мы сталкиваемся со стандартными учетными записями, которые оставляют администраторы при установке СУБД, веб-серверов, ОС или создании служебных учетных записей. Приложения зачастую либо обладают избыточным привилегиями, либо содержат известные уязвимости, и в результате у злоумышленников появляется возможность получить административные права на узле всего в один-два шага.

В четверти банков было установлено использование пароля P@ssw0rd, также к распространенным паролям относятся admin, комбинации типа Qwerty123, пустые и стандартные пароли (например, sa или postgres).

Недостаточные меры безопасности, а нередко и полное их отсутствие наблюдаются в отношении защиты служебных протоколов. Защита от атак на протокол NBNS отсутствовала в каждом исследованном банке, а на протокол LLMNR – в 70 % банков. Атакам ARP Poisoning оказались подвержены 80 % банков. В то же время перехват учетных данных, передаваемых по сети, может вполне успешно применяться нарушителями в процессе сбора сведений о системе. Например, в ряде банков в рамках тестирования на проникновение удалось перехватить несколько NetNTLMv2-хеш-сумм паролей пользователей домена в формате Challenge-Response. Затем по этим суммам методом перебора были подобраны пароли доменных учетных записей.

Исходя из приведенных результатов, мы предполагаем, что, хотя банки достаточно хорошо защищены извне, злоумышленник с высокой долей вероятности сможет успешно атаковать банковские системы при наличии доступа к внутренней сети. Такой доступ можно получить разными путями: к примеру, устроиться на работу в банк в качестве сотрудника, обладающего только физическим доступом к сетевым розеткам или минимальным уровнем привилегий в сети (уборщик, охранник).

25 %

В 25 % банков были скомпрометированы узлы, с которых осуществляется управление банкоматами, а значит, из этих банков смогла бы вывести деньги группировка Cobalt.

17 %

В 17 % банков недостаточно защищены системы карточного процессинга, позволяющие манипулировать балансом на карточных счетах злоумышленников, как мы это видели в начале 2017 г. в атаках на банки Восточной Европы.

Группировка Carbanak, отличающаяся своим умением успешно проводить атаки на любые банковские приложения, смогла бы похитить средства из всех 58 % банков.

Заключение

На сегодняшний день банки выстроили достаточно эффективные барьеры для защиты от внешних атак, однако основная проблема в том, что они не готовы противостоять нарушителю во внутренней сети.

Зная это, злоумышленники легко обходят системы защиты сетевого периметра с помощью простого и эффективного метода – фишинга, который доставляет вредоносное ПО в корпоративную сеть. Преступники внимательно следят за публикацией новых уязвимостей и быстро модифицируют свои инструменты. Например, в 2017 г. хакеры из группировки Cobalt использовали уязвимости в Microsoft Office CVE-2017-0199 и CVE-2017-11882 в расчете на то, что банки не успели установить соответствующие обновления безопасности.

Нужно понимать, что злоумышленник не сможет достичь своей цели и похитить деньги, если атака будет вовремя выявлена и остановлена, а это возможно на любом ее этапе при соответствующих мерах защиты. Необходимо проверять почтовые вложения в изолированном окружении, не полагаясь исключительно на антивирусные решения, установленные на рабочих станциях пользователей. Крайне важно своевременно получать уведомления систем защиты и незамедлительно реагировать на них. Для этого необходим постоянный мониторинг событий безопасности силами внутреннего или внешнего подразделения SOC, а также наличие SIEM-решений, которые могут существенно облегчить и повысить эффективность обработки событий информационной безопасности.

Чтобы эффективно противостоять активно развивающейся киберпреступности, важно не скрывать произошедшие инциденты, а участвовать в обмене информацией об атаках внутри отрасли, чтобы вовремя узнавать об индикаторах компрометации и сообщать о них другим.