

АТАКИ НА БАНКИ



2018

СОДЕРЖАНИЕ

Введение.....	3
Как грабят банки сегодня.....	4
Примеры хищений	4
Группировки	5
Типовая схема атаки	5
Результаты тестов на проникновение.....	11
Уязвимости сетевого периметра.....	11
Уязвимости внутренней сети.....	13
Заключение.....	17

ВВЕДЕНИЕ

В последние несколько лет в СМИ регулярно появляются заголовки о новых ограблениях банков. Фигурирующие в них названия преступных группировок обычно известны каждому специалисту по безопасности, а на счете некоторых из этих преступников целый ряд многомиллионных краж. Высокие гонорары и относительно низкий на сегодняшний день риск обнаружения способствуют активному развитию киберпреступности: несмотря на то, что отдельные группировки прекращают свою деятельность, а их участники задерживаются правоохранительными органами, на их место приходят другие, использующие более совершенные техники атак.

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 любой желающий может свободно приобрести ПО для проведения атаки с подробными инструкциями по его использованию, заручиться поддержкой недобросовестных сотрудников банков и преступных сообществ, специализирующихся на отмывании незаконно полученных денег. Складывается ситуация, при которой злоумышленник, обладающий минимальными техническими знаниями, 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 отрасли? Как хакерам удастся 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 этом отчете, основанном на результатах работ по анализу защищенности информационных систем отдельных банков за последние три года, мы постараемся ответить на эти вопросы. Сделанные выводы могут не отражать актуальное состояние защищенности информационных систем в других организациях. Данное исследование проведено с целью обратить внимание специалистов по ИБ отрасли на наиболее актуальные проблемы и помочь им своевременно выявить и устранить уязвимости. В первую очередь рассмотрим примеры атак и известных группировок, которые были активны в последние три года, и составим типовую схему атаки на банковскую инфраструктуру. Затем приведем результаты, полученные нашими экспертами в ходе работ по тестированию на проникновение, и покажем, какие уязвимости распространены сегодня в банках и какие из них приводят к успешной реализации атак. В заключение оценим, с учетом выявленных уязвимостей, сколько банков сегодня могут стать жертвами преступников.

КАК ГРАБЯТ БАНКИ СЕГОДНЯ

По оценкам Сбербанка, ежегодные убытки от кибератак в России уже составляют около 600 миллиардов рублей, а во всем мире эта сумма приближается к триллиону долларов 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, преступникам удается обходить все механизмы защиты, а в СМИ продолжают появляться публикации о новых кибератаках и новых хищениях из банков.

Примеры хищений

Сто миллионов долларов

Волна атак на карточный процессинг прошла в начале 2017 года 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 из банкоматов в другой стране. (Дропы, ответственные за непосредственное снятие наличных, заранее приобретали карты по поддельным документам и выезжали за пределы страны, в которой находился банк-жертва.) 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.

Шестьдесят миллионов долларов

Осенью 2017 года злоумышленники атаковали банк Тайваня, совершив переводы на счета в Камбодже, Шри-Ланке и США.

Четыре миллиона долларов

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.

Полтора миллиона долларов

В начале декабря в публичных источниках появилась информация о группировке MoneyTaker, которая проводила атаки на финансовые организации России и США в течение полутора лет. Преступники атаковали системы карточного процессинга и межбанковских переводов, средняя сумма хищения в США составила 500 тыс. долл., а в России — 72 млн руб.

Сто тысяч долларов

В декабре 2017 года появилась информация о первой успешной атаке на систему SWIFT в российском банке. Жертвой хакеров оказался банк «Глобэкс» (дочерняя компания Внешэкономбанка). В преступлении подозревается хакерская группировка Cobalt, специализирующаяся на кибератаках на банки.

Группировки

Если рассматривать преступные группировки, которые были активны в последние три года, то наиболее заметна была деятельность группировок Cobalt (предположительно связаны с Buhtrap), Carbanak, Lazarus и Lurk.

Группировка Cobalt известна своими атаками на финансовые организации СНГ, Восточной Европы и Юго-Восточной Азии, но в 2017 году 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 году российские банки потеряли более 1,1 млрд рублей 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 году злоумышленники попытались вывести миллиард долларов из центрального банка Бангладеш, но из-за ошибки в платежном документе смогли похитить только 81 млн.

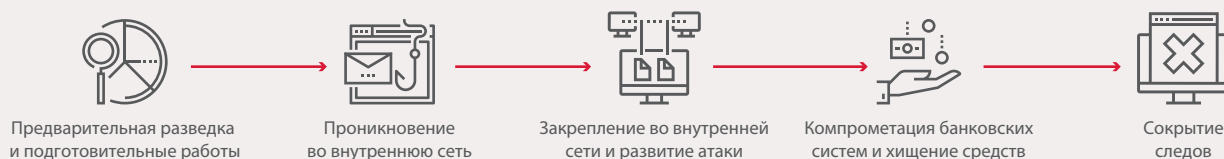
О группировке Carbanak СМИ заговорили после серии хищений в 2014–2015 годах. Отличительной чертой злоумышленников являлась широкая специализация: им удавалось похищать деньги из любых систем, к которым был получен доступ, эксплуатируя при этом исключительно недостатки защищенности корпоративных сетей. Общая сумма украденных средств превышает миллиард долларов.

Специалистам по информационной безопасности хорошо знаком и троян Lurk, который на протяжении нескольких лет использовался для атак на системы ДБО. Члены преступной группировки были арестованы в 2016 году. Считается, что в общей сложности хакеры вывели из банков более 3 миллиардов рублей.

Типовая схема атаки

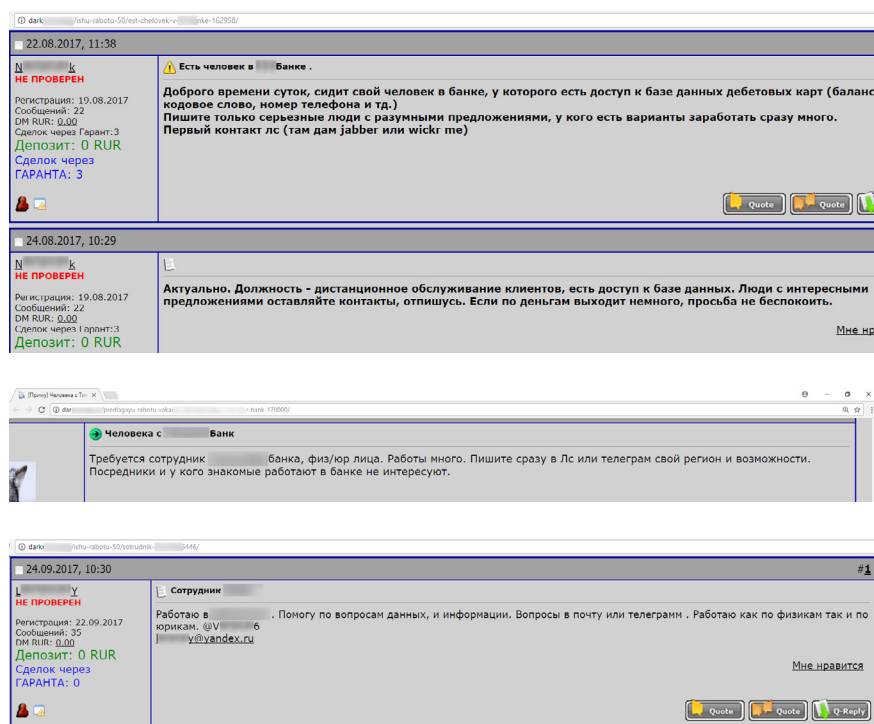
Выбор цели злоумышленника во многом обусловлен технической подготовкой, имеющимися инструментами и знаниями о внутренних процессах банка, которыми располагают преступники. Каждая из атак имеет свои особенности, в частности действия преступников различаются на этапе вывода денежных средств, но присутствуют и общие черты, которые мы постарались отметить в данном разделе. Злоумышленники действуют по довольно простым сценариям, состоящим из 5 основных этапов, представленных на схеме ниже.

Основные этапы атаки

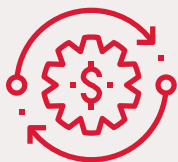


Этап 1. Разведка и подготовка

Первый этап достаточно длительный и трудоемкий: перед злоумышленниками стоит задача собрать как можно больше информации о банке, которая поможет преодолеть системы защиты, и провести предварительную организационную работу, учитывая специфику атакуемого банка. Поскольку сканирование внешних ресурсов может быть выявлено системами защиты, для того, чтобы не раскрыть себя на начальном этапе, преступники прибегают к пассивным методам получения информации, например для выявления доменных имен и адресов, принадлежащих банку. Для разведки также активно привлекаются недобросовестные сотрудники банков, готовые за вознаграждение поделиться информацией: множество объявлений об этом легко найти на соответствующих форумах в интернете.



Поиск сообщников на тематических форумах



Злоумышленник собирает информацию о банке:

- + сведения о системах на сетевом периметре и используемом ПО;
- + о сотрудниках (электронные адреса, телефоны, должности, ФИО и т. п.);
- + партнерах и контрагентах, их системах и сотрудниках;
- + бизнес-процессах.

Примеры подготовительных действий:

- + разработка или адаптация ВПО для используемых в банке версий ПО и ОС;
- + подготовка фишинговых писем;
- + организация инфраструктуры (регистрация доменов, аренда серверов, покупка эксплойтов и т. п.);
- + подготовка инфраструктуры для отмывания денег и их обналичивания;
- + поиск дропов для обналичивания денег;
- + тестирование инфраструктуры и ВПО.



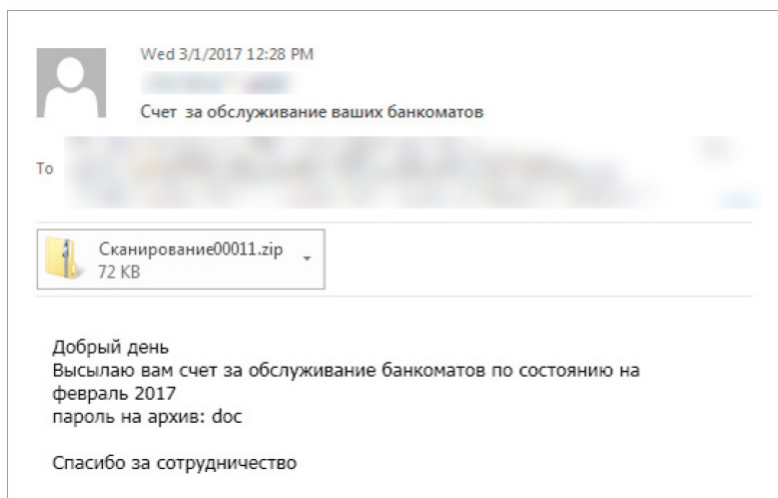
Этап 1. Разведка и подготовка

При построении инфраструктуры и подготовке инструментов для атаки злоумышленники могут как использовать собственные знания (разрабатывать эксплойты внутри группировки), так и нанимать для этого сторонних исполнителей; кроме того, они могут покупать уже готовые инструменты и адаптировать их к конкретным задачам. Если не планируется выводить деньги через банкоматы, то для крупных операций понадобятся связи с преступными сообществами для отмывания средств.

Этап 2. Проникновение во внутреннюю сеть

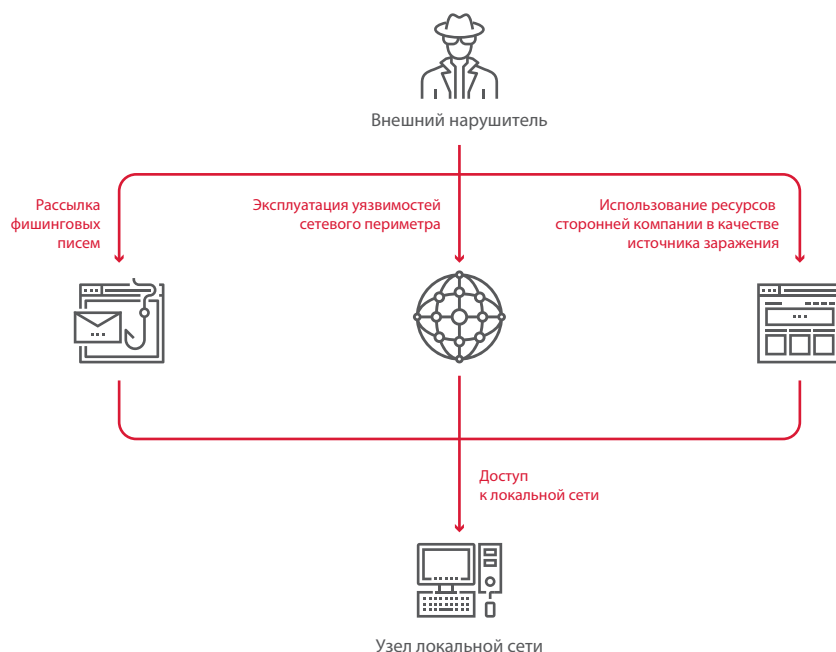
После всестороннего изучения жертвы и подготовки к атаке злоумышленники переходят в наступление.

Крупные и средние банки сегодня уделяют достаточно много внимания защите своего сетевого периметра, поэтому организовать атаку на серверы или веб-приложения не только сложно, но и рискованно, поскольку велика вероятность обнаружить себя. Наиболее распространенным и эффективным методом проникновения в инфраструктуру банка является фишинговая рассылка электронных писем в адрес сотрудников банка, которая осуществляется как на рабочие адреса, так и на личные. Такой метод используется, например, группировкой [Cobalt](#), также его применяли [Lazarus](#), [Metel](#), [GCMAN](#).



Фишинговое письмо, отправленное группировкой Cobalt

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 мы видели это в случае [Lazarus](#) и [Lurk](#).



Этап 2. Проникновение во внутреннюю сеть

Этап 3. Развитие атаки и закрепление в сети

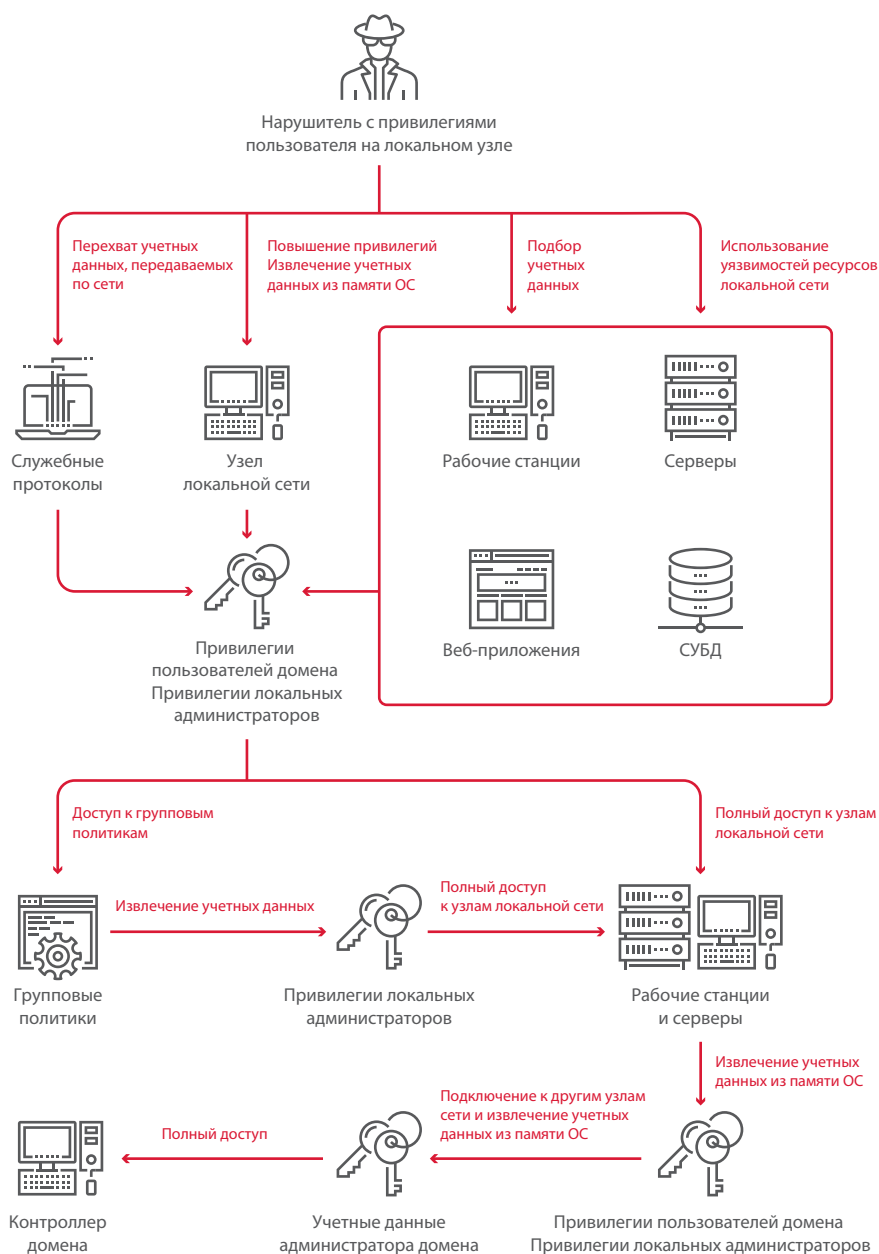
После того, как преступники получают доступ к локальной сети банка, им необходимо получить привилегии локального администратора на компьютерах сотрудников и серверах — для дальнейшего развития атаки. Успешность атак обусловлена недостаточным уровнем защищенности систем от внутреннего нарушителя. Можно выделить распространенные уязвимости:

- + использование устаревших версий ПО и отсутствие актуальных обновлений безопасности для ОС;
- + множественные ошибки конфигурации (в том числе избыточные привилегии пользователей и ПО, а также установку паролей локальных администраторов через групповые политики);
- + использование словарных паролей привилегированными пользователями;
- + отсутствие двухфакторной аутентификации для доступа к критически важным системам.

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). Эти данные используются для подключения к другим компьютерам в сети.

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

Привилегии локального администратора используются по уже классической схеме, когда злоумышленник копирует память процесса lsass.exe и использует его для извлечения паролей пользователей ОС (или их хеш-сумм) с помощью утилиты mimikatz. Подобные действия не детектируются антивирусными средствами, так как для копирования памяти используются легитимные инструменты, например `procdump`, а сама утилита mimikatz запускается на ноутбуке злоумышленника. Кроме того, злоумышленники могут использовать Responder для атак на служебные протоколы с целью перехвата учетных данных. Более подробно такие методы распространения в сети описаны в нашем отдельном [исследовании](#).



Этап 3. Развитие атаки и закрепление в сети

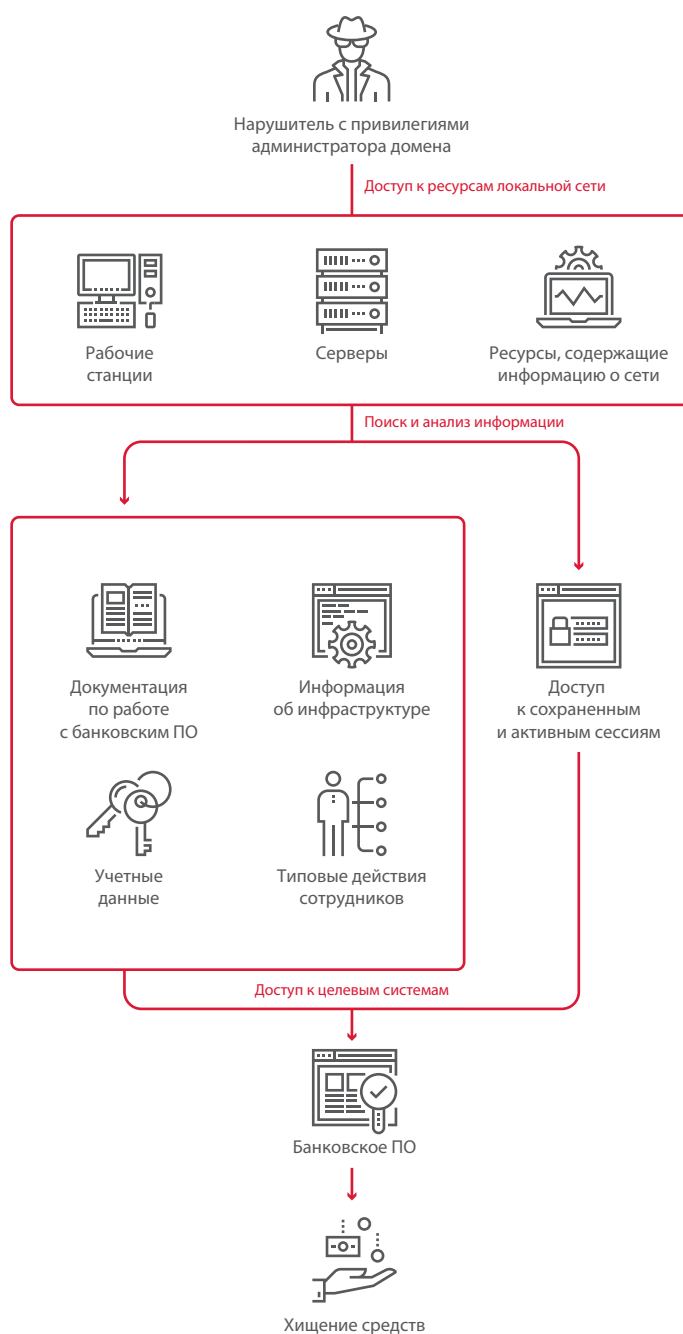
Если злоумышленникам удастся получить привилегии администратора домена, они смогут в дальнейшем беспрепятственно перемещаться по сети, контролировать компьютеры сотрудников, серверы и службы инфраструктуры банка. Обладая таким уровнем привилегий, получить доступ к бизнес-системам организации и специализированному банковскому ПО становится очень просто, для этого достаточно определить рабочие станции сотрудников, которые таким доступом обладают, и подключиться к ним. Используя технику *golden ticket*, злоумышленники могут надежно закрепиться в корпоративной системе на длительное время.

Чтобы скрыть свое присутствие, злоумышленники часто используют бестелесный вредоносный код, который выполняется только в оперативной памяти, а для сохранения канала удаленного управления после перезагрузки компьютера добавляют ВПО в автозагрузку ОС.

Этап 4. Компрометация банковских систем и хищение денег

Закрепившись в сети, преступники должны понять, на каких узлах находятся искомые банковские системы и как будет удобнее получить к ним доступ. Преступники исследуют рабочие станции пользователей в поисках файлов, указывающих на то, что с данной рабочей станции осуществляется работа

с банковскими приложениями. Для хранения паролей к критически важным системам в корпоративных сетях обычно используется специальное ПО. Нарушитель с привилегиями локального администратора ОС может скопировать дампы памяти этого процесса, извлечь пароли для доступа к приложению или зашифрованным базам, а затем получить в открытом виде пароли для доступа ко всем критически важным системам банка — АБС, SWIFT, рабочим станциям для управления банкоматами и др. Такой сценарий атаки весьма эффективен и неоднократно применялся в ходе тестирования на проникновение. Дополнительную помощь преступникам могут оказать ресурсы, которые содержат информацию об инфраструктуре, например системы мониторинга, которые используют в своей работе администраторы, или ресурсы технической поддержки пользователей. Используя полученные данные, нарушители будут более уверенно ориентироваться в структуре внутренней сети и смогут учесть особенности бизнес-процессов банка при проведении атаки, чтобы не вызвать подозрений у службы безопасности и срабатывания систем выявления атак.



Этап 4. Компрометация банковских систем и хищение денег

Преступники могут находиться в инфраструктуре банка долго, оставаясь незамеченными, собирать информацию об инфраструктуре и процессах, не спеша изучать выбранные для проведения атак системы 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.

Основными способами хищений являются:

- + перевод средств на подставные счета через системы межбанковских платежей;
- + перевод денежных средств на криптовалютные кошельки;
- + управление банковскими картами и счетами;
- + управление выдачей наличных средств в банкоматах.

Этап 5. Скрытие следов

С целью затруднить расследование инцидента преступники принимают меры для уничтожения следов пребывания в системе. Несмотря на то, что 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. Поэтому неудивительно, что некоторые нарушители предпочитают обезопасить себя настолько, насколько это возможно и не просто удаляют отдельные следы, а полностью выводят из строя узлы сети, стирая загрузочные записи и таблицы разделов жестких дисков. Волна атак вирусов-шифровальщиков, с которой мир столкнулся в 2017 году, была превосходным примером того, как легко могут быть уничтожены данные крупной компании, и теперь арсеналы хакеров пополняются 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. Так как к заключительному моменту атаки преступники с высокой долей вероятности обладают максимальными привилегиями в системе и досконально изучили ее, остановить их действия на этом этапе уже вряд ли удастся.

РЕЗУЛЬТАТЫ ТЕСТОВ НА ПРОНИКНОВЕНИЕ

Мы рассмотрели, как на сегодняшний день злоумышленники атакуют банки. В этом разделе мы расскажем, с какими уязвимостями сталкиваемся на практике при проведении тестов на проникновение, и разберем, насколько вероятны описанные выше атаки.

Тестирование на проникновение проводится для оценки реального уровня защищенности организации, при этом моделируются действия потенциального нарушителя. В зависимости от исходного уровня привилегий нарушителя различают внешнее тестирование, в рамках которого проверяется возможность преодоления сетевого периметра, и внутреннее, целью которого является получение полного контроля над инфраструктурой или доступ к критически важным системам. 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.

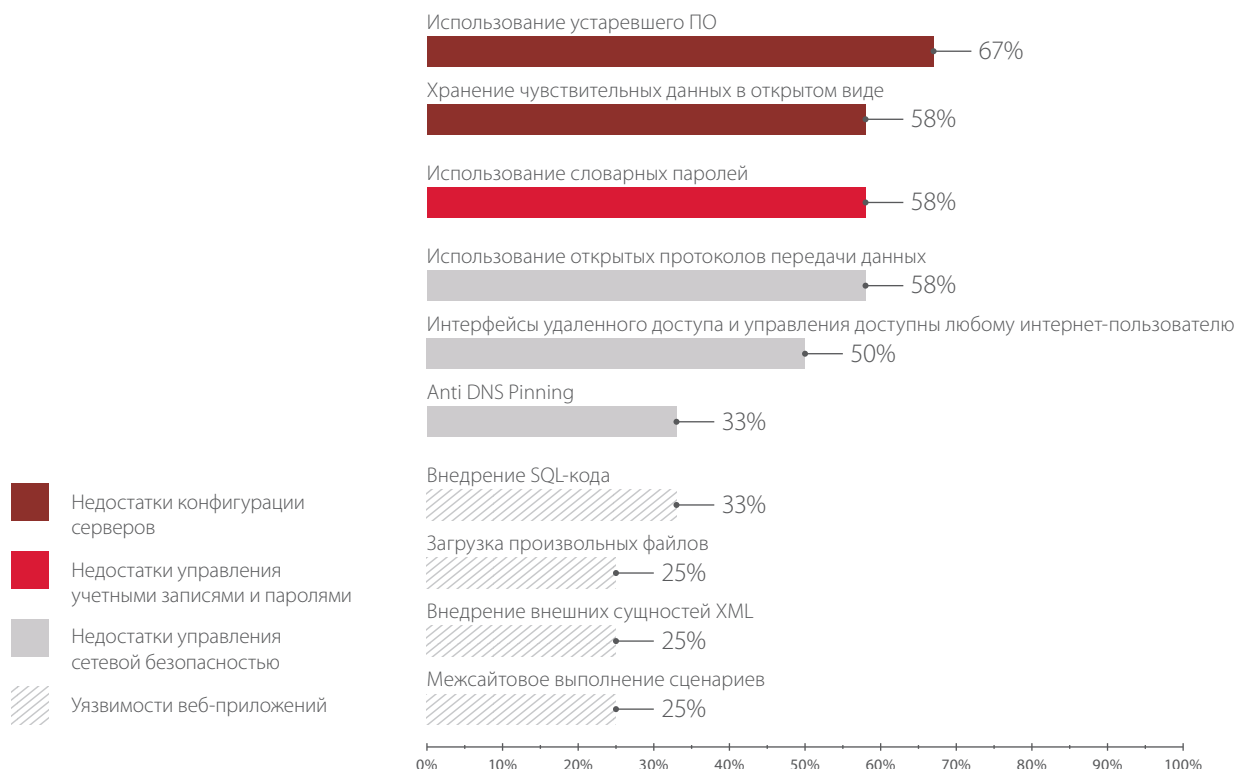
Уязвимости сетевого периметра

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.

В 100% банков выявлены:

- + уязвимости веб-приложений,
- + недостатки сетевой безопасности,
- + недостатки конфигурации серверов.

В 58% банков выявлены недостатки управления учетными записями и паролями



Десятка самых распространенных уязвимостей на сетевом периметре (доля банков)

В 22% банков удалось преодолеть сетевой периметр в рамках внешнего тестирования на проникновение

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 доступ ко 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.

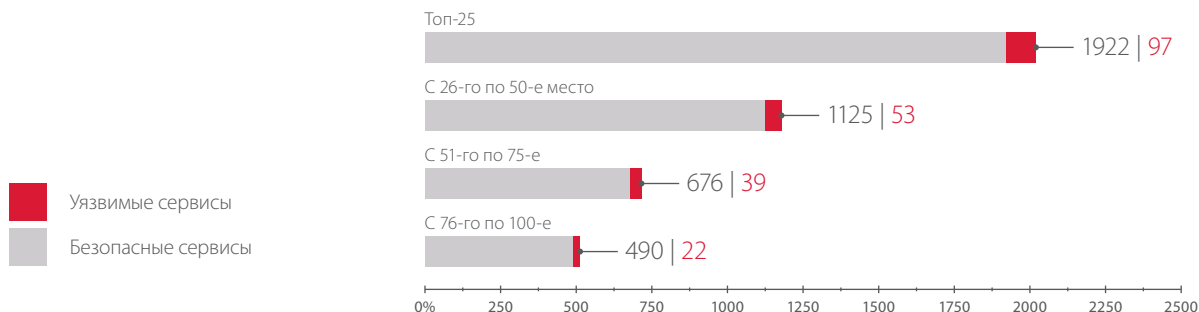
Следовательно, преступные группировки, планирующие проникнуть во внутреннюю сеть банка путем эксплуатации уязвимостей на сетевом периметре, смогли бы достичь цели в 22% банков. Подобные способы проникновения использовали в своей деятельности, например, группировки [ATMitch](#) и [Lazarus](#).

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](#)).

На внешнем периметре сети наблюдаются и недостатки, связанные с сетевой безопасностью. Наибольшую опасность представляют интерфейсы удаленного доступа и управления, которые зачастую доступны для подключения любому внешнему пользователю. Среди наиболее распространенных — протоколы SSH и Telnet, которые встречаются на периметре сети в 58% банков, а также протоколы доступа к файловым серверам (в 42% банков).

Приведем и результаты [исследования](#), проведенного нашими специалистами в 2017 году. Изучив с помощью Shodan сервисы, доступные на периметре ста наиболее крупных банков, и сопоставив их с собственной базой уязвимостей,

эксперты установили, что около 5% сервисов потенциально уязвимы. Наличие потенциально опасного сервиса еще не означает, что уязвимости действительно можно эксплуатировать, тем не менее даже один уязвимый ресурс может позволить злоумышленнику провести успешную атаку.



Доли уязвимых сервисов на сетевом периметре 100 крупнейших банков

75% банков

уязвимы к атакам методами социальной инженерии

Как мы уже отметили, большинство банков имеет достаточно высокий уровень защиты сетевого периметра, но персонал обычно является самым уязвимым звеном в системе защиты любой организации.

В ходе оценки осведомленности в 75% банков сотрудники переходили по ссылке, указанной в фишинговом письме, в 25% банков сотрудники вводили свои учетные данные в ложную форму аутентификации, и еще в 25% банков хотя бы один сотрудник запускал на своем рабочем компьютере вредоносное вложение. В среднем в банках по фишинговой ссылке переходили около 8% пользователей, 2% запускали вложенный файл, но свои учетные данные вводили менее 1% пользователей.

Хотя уровень осведомленности в вопросах ИБ среди банковских сотрудников все же выше, чем в других отраслях, достаточно, чтобы всего один пользователь выполнил нежелательное действие, — и нарушитель получит доступ к корпоративной сети. Таким образом, три четверти банков уязвимы к атакам методами социальной инженерии, которые используются для преодоления периметра практически каждой преступной группировкой, в том числе группировками Cobalt, Lazarus, Carbanak.

Регулярное проведение тренингов по безопасности с контрольной проверкой уровня осведомленности приносит отличные результаты. В этом плане показателен пример одного банка. В ходе работ по оценке осведомленности в вопросах ИБ за 2016 год часть пользователей ввела свои учетные данные в фишинговую форму аутентификации: таким образом преступники могли бы получить данные для доступа к ресурсам банка. Через год ситуация изменилась кардинально: учетные данные не ввел ни один сотрудник.

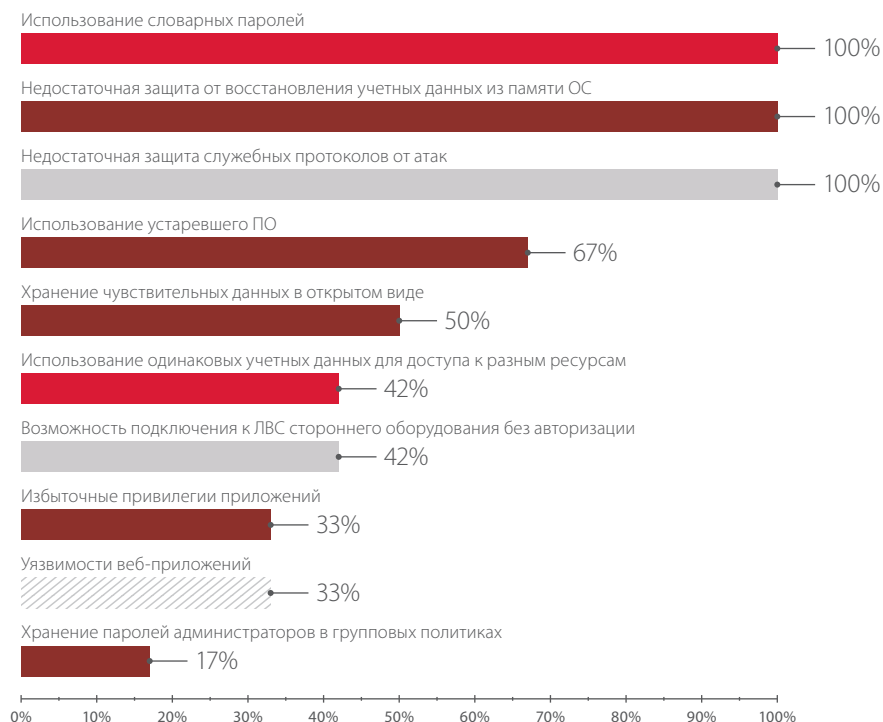
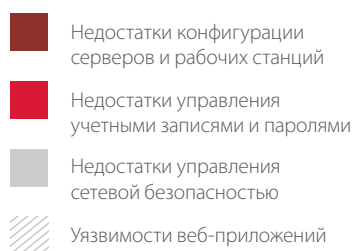
Уязвимости внутренней сети

В 100% банков

получен полный контроль над инфраструктурой

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, доступ к системам межбанковских переводов, карточному процессингу, платежным шлюзам.

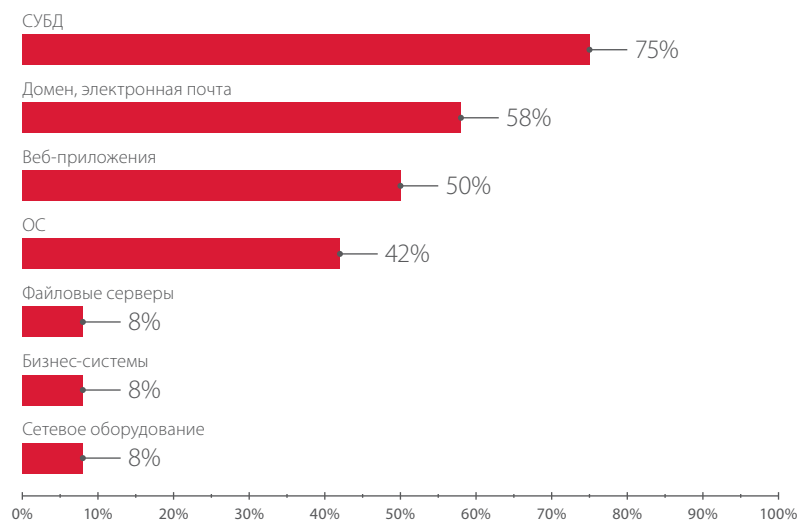
Какие недостатки безопасности позволяют злоумышленникам развивать атаку вглубь банковской инфраструктуры? На рисунке ниже представлены уязвимости, эксплуатация которых способствовала получению полного контроля над доменной инфраструктурой в ходе работ по внутреннему тестированию на проникновение. Указаны доли систем, в которых присутствовали уязвимости данного типа.



Наиболее распространенные уязвимости во внутренней сети (доля банков)

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 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 при создании служебных учетных записей. Приложения зачастую либо обладают избыточными привилегиями, либо содержат известные уязвимости, и в результате у злоумышленников появляется возможность получить административные права на узле всего в один-два шага.



Компоненты внутренней сети, для которых используются словарные пароли (доля банков)

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).

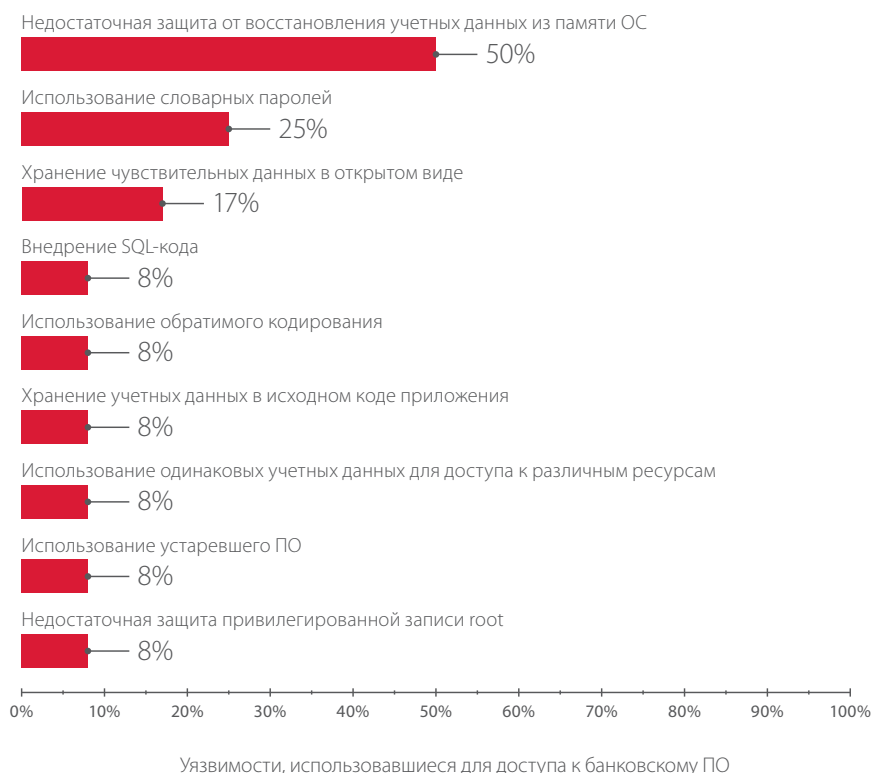
Недостаточные меры безопасности, а нередко и полное их отсутствие наблюдаются в отношении защиты служебных протоколов. Защита от атак на протокол NBNS отсутствовала в каждом исследованном банке, а защита от атак на протокол LLMNR — в 70% банков. Атакам ARP Poisoning оказались подвержены 80% банков. В 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.

В 58% банков
получен доступ
к банковским системам

На этапе распространения и закрепления в сети действия злоумышленников достаточно схожи, потому что они эксплуатируют недостатки защищенности, характерные для любой корпоративной системы. Исходя из приведенных результатов, мы предполагаем, что любая преступная группировка смогла бы получить полный контроль над доменной инфраструктурой в каждом из исследованных банков. Поэтому, хотя банки достаточно хорошо защищены извне, злоумышленник с высокой долей вероятности сможет успешно атаковать банковские системы при наличии доступа ко внутренней сети. Такой доступ можно получить разными путями; к примеру, участник преступной группы может устроиться на работу в банк в качестве сотрудника, обладающего только физическим доступом к сетевым розеткам или с минимальным уровнем привилегий в сети (уборщик, охранник).

Получить доступ к банковским приложениям удалось в 58% банков. Необходимо учитывать, что во всех остальных банках развитие атаки на критически важные узлы не проводилось, учитывая заданные границы работ. Тем не менее привилегии администратора домена позволили бы злоумышленнику прочно закрепиться в системе и осуществлять атаки на целевые ресурсы.

Ниже представлены уязвимости, благодаря которым был получен доступ непосредственно к банковскому ПО.



4 шага

требуется злоумышленнику
для получения доступа
к банковскому ПО

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

Перевести средства на собственные счета через системы межбанковских переводов, на которые нацелены Lazarus и MoneyTaker, было бы возможно в 17% банков.

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

В среднем злоумышленнику, проникшему во внутреннюю сеть банка, требуется всего четыре шага для получения доступа к банковским системам.

ЗАКЛЮЧЕНИЕ

На сегодняшний день банки выстроили достаточно эффективные барьеры для защиты от внешних атак, однако основная проблема состоит 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 году 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. Внутри сети злоумышленники свободно перемещаются незамеченными с помощью известных уязвимостей и легитимного ПО, которое не вызывает подозрений у администраторов. Пользуясь недостатками защиты корпоративной сети, злоумышленники за короткое время получают полный контроль над всей инфраструктурой банка.

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, если принимаются соответствующие меры 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.

О компании

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.