

Защищенность кредитно-финансовой сферы, итоги 2018 года

Оценка Positive Technologies

Содержание

Методология	3
Общие тенденции 2018 года	3
Краткая статистика: инциденты и методы атак	4
Портрет злоумышленника	6
Защищенность инфраструктуры кредитно-финансовой организации	9
Защищенность онлайн-банкинга и мобильного банкинга	12
Защищенность банкоматов, платежных терминалов	15
Защищенность платежных терминалов (POS)	17
Защищенность инвестиционных и трейдинговых приложений	18
Общие выводы, прогнозы и рекомендации Positive Technologies	19
О Positive Technologies	21

Методология

Отчет основан на данных, полученных в ходе выполненных компанией Positive Technologies в течение 2018 г. работ по анализу защищенности корпоративной инфраструктуры финансовых организаций, банкоматов, мобильных и онлайн-банков, торговых платформ. Также в выборку вошли итоги работ экспертного центра безопасности Positive Technologies (PT Expert Security Center) по расследованию киберинцидентов и ретроспективному анализу событий безопасности в инфраструктуре компаний и отслеживанию активности АPT-группировок, действующих в финансовом секторе, за 2018 год. При подготовке материала использована общедоступная информация об актуальных угрозах информационной безопасности и данные аналитических отчетов компании Positive Technologies за 2017–2018 годы.

Общие тенденции 2018 года

Кредитно-финансовые организации входят в число наиболее атакуемых киберпреступниками. В течение 2018 г. общее число атак росло при снижении количества успешных (снизился финансовый ущерб от них).

В большинстве атак на финансовые организации использовалось вредоносное ПО, часто доставляемое с использованием социальной инженерии, в частности — фишинга. Во внутренней сети уровень их защищенности мало чем отличается от компаний из других отраслей и достаточно низок. Это позволяет злоумышленникам беспрепятственно перемещаться по сети, получать доступ к критически важным системам, управлению банкоматами и карточному процессингу.

Исследования защищенности банкоматов и платежных терминалов показывают, что используемые механизмы безопасности недостаточно эффективны. Выявленные уязвимости и недостатки механизмов защиты позволяют похитить деньги или перехватить данные банковских карт. В 2018 г. были зафиксированы преимущественно атаки типа blackbox.

Главная позитивная тенденция в безопасности финансовых приложений в 2018 г. – сокращение доли уязвимостей высокого уровня риска в онлайн-банках. Однако в целом их защищенность остается низкой: кража денежных средств в 2018 г. была возможна в 54% онлайн-банков (что несколько выше показателя 2017 г., составившего 50%), в отдельных случаях уязвимости позволяли развивать атаку до проникновения в корпоративную инфраструктуру.

Преступники в будущем могут наметить себе и новые объекты атак, которые пока не привлекают их внимания. Например, большое число уязвимостей выявляется в торговых платформах, используемых в финансовых организациях. Атаки на них еще не распространены, но имеют шансы превратиться в новый тренд в ближайшее время и потенциально могут вызвать изменение цен на бирже и привести к потере денег.

Краткая статистика: инциденты и методы атак

По итогам 2017 и 2018 гг. кредитно-финансовые организации входят в число наиболее атакуемых: они входят в топ-3 по общему количеству атак.

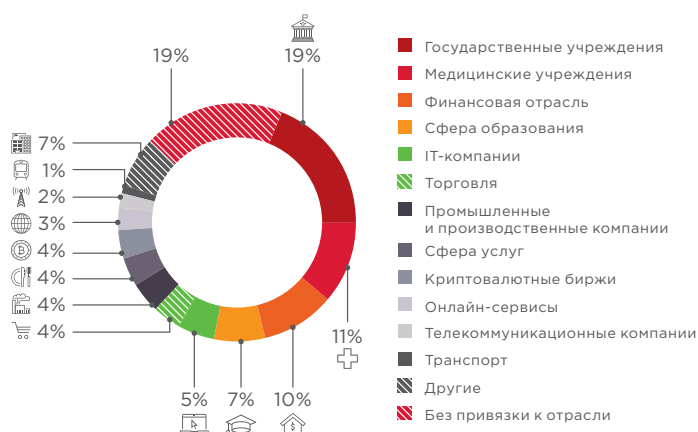


Рисунок 1. Категории жертв среди юридических лиц

Главный мотив злоумышленников — получение финансовой выгоды (65% инцидентов в 2018 г. и 92% — в 2017 г.). Доля инцидентов, нацеленных на получение информации о платежных картах, персональных данных, учетных данных пользователей для доступа к личным кабинетам, с 2017 по 2018 г. увеличилась с 8 до 31%.

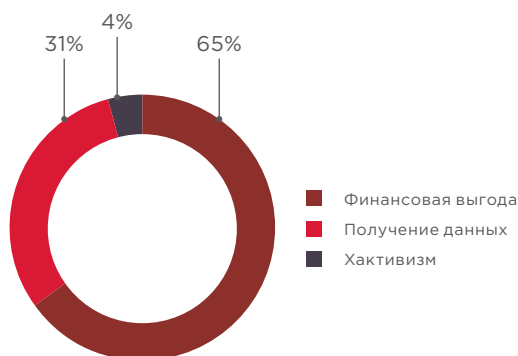


Рисунок 2. Мотивы атак на организации кредитно-финансовой сферы

Среди методов атак по итогам 2018 г. лидируют использование ВПО (58%), социальная инженерия (49%), хакинг (36%), подбор учетных данных (11%) и эксплуатация веб-уязвимостей (5%). В целом это повторяет тенденции 2017 года. Растет доля атак, в ходе которых используется вредоносное ПО. В 2017 г. мы отмечали, что ВПО применялось в 48% случаев, в 2018 г. доля таких атак составила 58%. Этому способствует то, что ВПО с каждым годом становится более доступным и, соответственно, снижается порог входа в киберпреступный бизнес.

В финансовых организациях система защиты, как правило, хорошо организована, поэтому главным вектором проникновения в инфраструктуру остается социальная инженерия, использующаяся в 49% атак. Фишинг — самый эффективный способ доставки вредоносного ПО. 90% актуальных на сегодня АРТ-группировок используют его на этапе проникновения.

Поиск и эксплуатация уязвимостей в публично доступных сервисах (хакинг) применяются в 36% атак на финансовые организации, а подбор учетных данных и эксплуатация веб-уязвимостей — в 11 и 5% атак соответственно. Под угрозой в этом случае оказываются скорее банки среднего звена, не всегда готовые вкладывать крупные бюджеты в обеспечение собственной безопасности. Небольшие банки могут оказаться промежуточным звеном атаки: например, с компьютеров их сотрудников могут рассылаться фишинговые письма в адрес их коллег из более крупных банков.

Нередко злоумышленники комбинируют эти методы в ходе атаки.

Резюме: вредоносное ПО и социальная инженерия укрепляют свои позиции

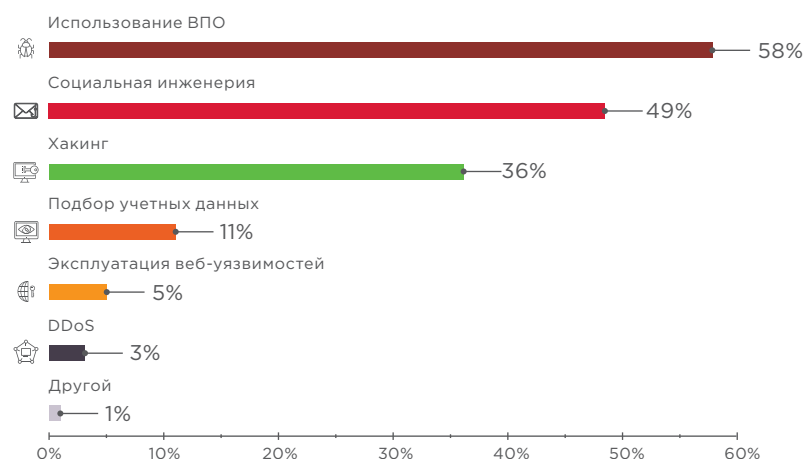


Рисунок 3. Методы атак на организации кредитно-финансового сектора

Вредоносное ПО будет и дальше широко использоваться в атаках на финансовые организации. Рынок киберуслуг и ВПО активно развивается — все больше группировок предпочитают не разрабатывать собственное ПО, а покупать готовое. Одни и те же программы, вероятно, будут использоваться разными группами киберпреступников, что существенно усложнит атрибуцию.

В тренде у преступников использование уязвимостей в продуктах Microsoft, причем все чаще применяются вновь опубликованные эксплойты (окно между появлением новой технологии и принятием ее на вооружение может исчисляться часами).

Преступники будут искать новые пути распространения вредоносного ПО и совершенствовать старые. Социальная инженерия, вероятно, останется основным путем распространения, однако рост осведомленности о различных способах мошенничества заставит преступников разрабатывать новые схемы обмана пользователей. Многоэтапные атаки (через supply chain) также не потеряют актуальности.

Портрет злоумышленника

Общий тренд:

мотив, вектор атаки,
результативность

Ключевые

группировки:

хорошо известные
и новички

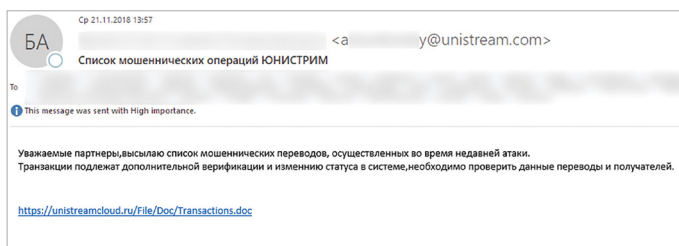
Ключевой мотив злоумышленников, атакующих организации кредитно-финансового сектора, — прямая финансовая выгода. И даже атаки, нацеленные на получение информации о платежных картах, персональных данных, учетных данных пользователей для доступа к личным кабинетам и так далее, в дальнейшем могут быть монетизированы за счет последующей кражи денег со счетов либо их перепродажи на теневом рынке. На долю такого типа информации приходится до 83% всех продаваемых и покупаемых в дарквебе данных.

Основной вектор, используемый атакующими для доступа в корпоративную сеть кредитно-финансовых организаций, — фишинг. С каждым годом качество составления фишинговых сообщений улучшается. А на стороне атакующих появляются новые игроки. Так, во втором полугодии 2018 г., помимо известных АРТ-группировок, атакующих финансовый сектор, была обнаружена новая. Злоумышленники также рассылали документы с макросами, которые загружали утилиты, предоставляющие удаленный доступ к зараженному компьютеру.

Cobalt

Группа Cobalt за 2018 г. выполнила 61 рассылку по кредитно-финансовым организациям в России и странах СНГ. Из них на I, II, III и IV кварталы пришлось по 12, 12, 24 и 13 рассылок соответственно¹. Главная цель группы — кража денежных средств со счетов финансовых организаций. Основные используемые методы — это компрометация банкоматной сети либо подделка платежных документов. Для доставки ВПО в корпоративную сеть группа пользуется фишинговыми письмами: для каждой рассылки подготавливался отдельный домен, с которого рассылались письма с заранее подготовленным убедительным содержанием. В некоторых случаях с них же загружалась полезная нагрузка.

Большую часть года группировка использовала JS-бэкдор, с августа перешла на распространение вредоносного ПО CobInt, но в октябре вернулась к использованию JS-бэкдора. Фишинговые рассылки в августе и начале сентября проводились с поддельных доменных адресов, якобы принадлежавших платежной системе Interkassa, а также банкам BBVA Compass Bancshares, Европейскому центральному банку, Unibank, АЛЬФА-БАНКу, Райффайзенбанку. В течение IV квартала рассылка проводилась от лица взломанных банков — например, от имени Unistream. Примечательно, что группировка провела вредоносную рассылку менее чем через двое суток с момента публикации информации об уязвимости нулевого дня CVE-2018-15982 (в течение 34 часов)².



1, 2 По данным PT Expert Security Center.

Рисунок 4. Пример фишингового письма, рассылаемого группировкой Cobalt

Silence

В 2018 г. группировка Silence провела 7 атак (в II квартале — 3, в IV — 4)³. Группа не очень разнообразно подходит к составлению фишинговых писем: разница между рассылками 2017 и 2018 гг. минимальна.

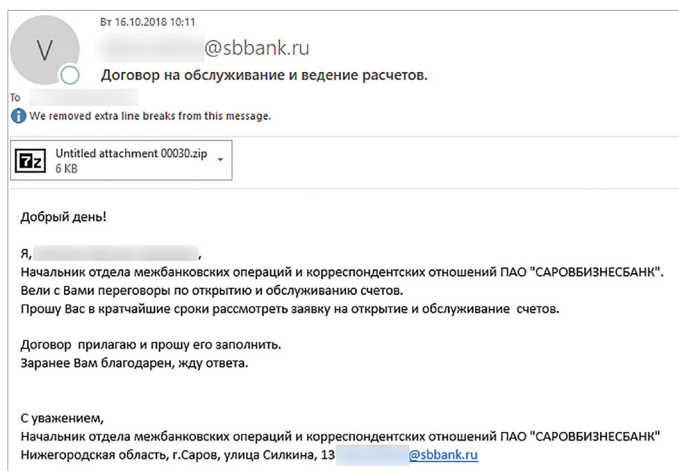


Рисунок 5. Пример фишингового письма, рассылаемого группировкой Silence

RTM

Группа RTM за 2018 г. провела 59 рассылок, в том числе нацеленных на финансовые учреждения. В I квартале группировка выполнила 5 из них, в II — 14, в III — 17 и в IV — 23 рассылки. Атакую, группа пытается получить доступ к финансовым счетам организаций, и уже с них производит кражу денег. Для получения доступа в корпоративную сеть используются фишинговые рассылки. С начала своей активности группа придерживается неизменного их формата.

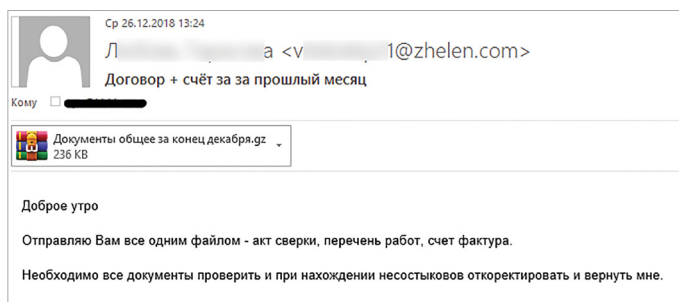


Рисунок 6. Пример фишингового письма, рассылаемого группировкой RTM

Кроме того, данная группа в качестве одного из центров управления использовала домены в зоне .bit⁴. Это специальная зона, созданная на базе технологии блокчейн 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 комьюнити о новых управляющих серверах с задержкой в минуты с начала (иногда и до) их использования злоумышленниками.

³ По данным PT Expert Security Center.

⁴ В последние годы его начали использовать операторы таких ботнетов, как Dimnie, Shifu, RTM и Gandcrab, для управления адресами C&C-серверов.

Новые игроки

Резюме: группировки сохраняют активность

Во второй половине 2018 г. была выявлена новая группировка, атакующая финансовый сектор. Злоумышленники рассылали вредоносные документы с макросами якобы от лица ФинЦЕРТ. При исполнении макроса на компьютер загружалась полезная нагрузка — [Metasploit stager](#).

Также была зафиксирована рассылка, которая проводилась через скомпрометированную учетную запись сотрудника компании «Альфа-Капитал». При анализе рассылаемого документа был обнаружен сценарий на JavaScript, который использовала группа Treasure Hunters, однако в него была добавлена функция запуска Metasploit stager. В обоих случаях письма были очень хорошо подготовлены.

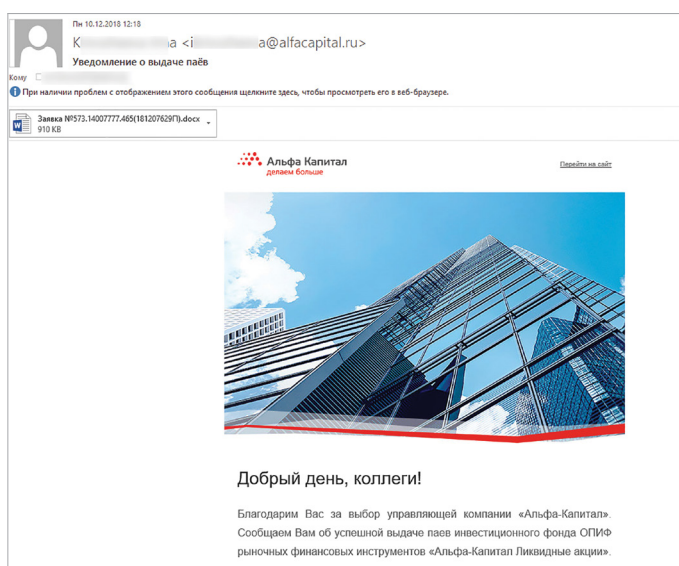


Рисунок 7. Пример фишингового письма, рассылаемого новой группировкой, атаковавшей кредитно-финансовый сектор

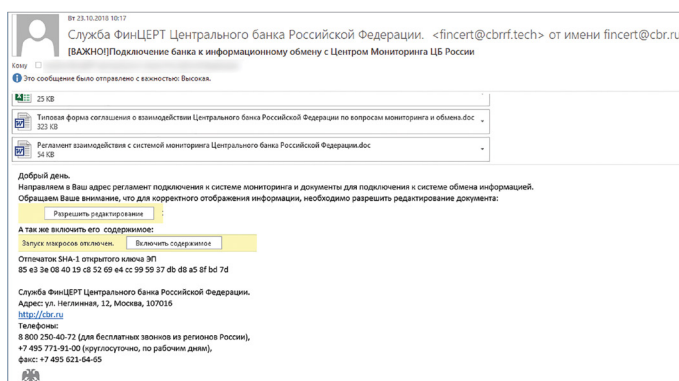


Рисунок 8. Пример фишингового письма, рассылаемого новой группировкой, атаковавшей кредитно-финансовый сектор

Несмотря на общий рост числа атак в 2018 г., финансовый ущерб значительно снизился по сравнению с предыдущим годом. Этому во многом способствует информационный обмен внутри отрасли. Затишье может быть связано и с арестом одного из руководителей группировки Cobalt в марте 2018 г., так как существенная доля успешных хищений

в российских банках годом ранее была связана именно с ее деятельностью. Впрочем данная группа продолжает свою деятельность. Не исключено, что после арестов участников Cobalt и FIN7 (Carbanak) преступники формируют новые группировки и проводят реструктуризацию. В конце 2018 г. был выявлен загрузчик группы Silence, подписанный валидным сертификатом SEVA MEDICAL LTD. Этим же сертификатом был подписан один из COM-DLL дропперов группы Cobalt. Это позволяет говорить о возможном смешении составов группировок или об использовании ими одних и тех же сервисов, что весьма вероятно, так как современные киберпреступники все чаще работают по сервисной модели. Злоумышленники разрабатывают новые инструменты, собирают информацию об уязвимостях и совершенствуют техники атак, в том числе улучшают методы доставки полезной нагрузки с помощью фишинга. Это делается и для того, чтобы преодолеть совершенствующиеся средства защиты.

Защищенность инфраструктуры кредитно-финансовой организации

Общий тренд: безопасность внутренней сети далека от совершенства

Основные уязвимости и недостатки механизмов защиты сетевого периметра банков, подразделяются на четыре типа:

- недостатки конфигурации серверов,
- недостатки управления учетными записями и паролями,
- недостаточная сетевая безопасность,
- уязвимости веб-приложений.

Наиболее часто встречающиеся проблемы в конфигурации серверов — несвоевременное обновление ПО (67% банков) и хранение чувствительных данных в открытом виде (58% банков). Более чем в 50% обследованных банков использовались словарные пароли. В 58% случаев использовались открытые протоколы передачи данных, а в 50% — были доступны интерфейсы удаленного доступа и управления. Среди уязвимостей веб-приложений отметим возможность внедрения SQL-кода (33% банков) и загрузки произвольных файлов (25%), способных привести к выполнению произвольных команд на сервере. При проведении тестов на проникновение в банках в 2017–2018 гг. во всех случаях преодолеть периметр удавалось из-за недостаточной защиты веб-приложений.

Защита сетевого периметра в банковской сфере значительно выше, чем в других отраслях. В ходе тестирования на проникновение (за аналогичный период) сетевой периметр организаций преодолевается в 58% случаев. В кредитно-финансовой сфере этот показатель составляет 22% и возрастает до 75% при использовании социальной инженерии.

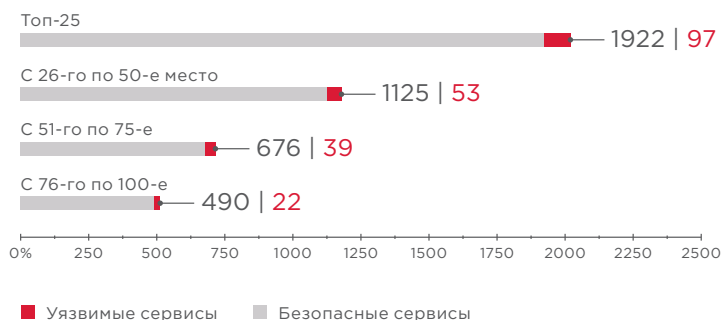


Рисунок 9. Доли уязвимых сервисов на сетевом периметре 100 крупнейших банков

Безопасность внутренней сети кредитно-финансовых организаций далека от совершенства. Полный контроль над инфраструктурой был получен во всех исследованных в 2017–2018 гг. банках. В 33% случаев, не обладая максимальными привилегиями в системе, можно получить доступ к узлам, с которых выполняется управление банкоматами, доступ к системам межбанковских переводов, карточному процессингу, платежным шлюзам.



Рисунок 10. Наиболее распространенные уязвимости во внутренней сети (доля банков)

Типовые векторы атак во внутренней сети часто базируются на слабой парольной политике и недостаточной защите от восстановления паролей из памяти ОС. Почти в 50% систем слабые пароли устанавливают пользователи, но чаще используются стандартные учетные записи, оставляемые администраторами при установке СУБД, веб-серверов, ОС или создании служебных учетных записей. Приложения часто обладают избыточными привилегиями или содержат известные уязвимости, в итоге злоумышленники имеют возможность получить административные права на узле в 1–2 шага.

Попытки использования банками корпоративных блокчейн-систем создают дополнительные риски. Компоненты этих систем, связь между ними и прочими системами финансовой организации (в том числе внутренними и внешними приложениями) открывают новые возможности для проникновения в инфраструктуру. Оценка безопасности пилотных внедрений технологии блокчейн в банковские проекты показала, что в 71% случаев содержались уязвимости в смарт-контактах, половина проектов имела уязвимости в приложениях, используемых для доступа к данным, хранящимся в блокчейне. Это связано в том числе и с тем, что практика безопасной разработки еще не наработана, а требования по безопасности к внедрению таких систем еще только предстоит сформировать.

Ввиду того, что такая система оперирует критически важными данными, для успешной атаки достаточно лишь одной уязвимости — не важно, в каком компоненте системы. Это сильная мотивация для злоумышленников. В числе последствий атак могут быть несанкционированное внесение данных в реестр, атаки на пользователей со стороны блокчейна, полная блокировка работоспособности системы, проникновение в сеть организации при помощи специально подготовленных блокчейн-транзакций, используемых как транспорт для атак на связанные системы. Гипотетически это может привести к полному контролю со стороны нарушителя над критически важными ресурсами организации.

Ключевые проблемы:

неосведомленность персонала и неготовность к оперативному выявлению угроз

Часто самым уязвимым звеном в системе защиты кредитно-финансовой организации является персонал. Оценка осведомленности показала, что в 75% кредитно-финансовых организаций сотрудники переходили по ссылке, указанной в фишинговом письме, в 25% — вводили свои учетные данные в ложную форму аутентификации, и еще в 25% 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. При этом 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, использующимися для преодоления периметра почти каждой преступной группировкой.

Другая проблема — низкий уровень защищенности внутренней сети и неготовность к оперативному выявлению угроз. Такие результаты позволяют предположить, что любая преступная группировка смогла бы получить полный контроль над доменной инфраструктурой в каждом из исследованных банков.

Возвращаясь к теме атак на корпоративные блокчейн-системы, следует отметить, что на данный момент затруднены своевременное обнаружение подобных инцидентов (из-за отсутствия общедоступного инструментария) и реагирование на них, так как существует только два варианта реагирования: hard fork блокчейна (то есть откат состояния блокчейна до момента совершения атаки и добавление новых транзакций, начиная с этого момента); и принятие последствий атаки (единственный вариант в случае использования публичного блокчейна). Оба варианта имеют побочные эффекты. При проведении hard fork все транзакции, совершенные после инцидента, будут утеряны, что потребует их добавления заново. Это особенно критично, если данные о случившемся инциденте появились спустя значительное время после атаки.

Резюме:

необходимо повысить оперативность выявления атак

Финансовые организации имеют достаточно эффективные барьеры для защиты от внешних атак, но не готовы противостоять нарушителю во внутренней сети. Зная это, злоумышленники обходят системы защиты сетевого периметра с помощью простого и эффективного метода — фишинга, который доставляет вредоносное ПО в корпоративную сеть. Преступники следят за публикацией новых уязвимостей и быстро модифицируют свои инструменты. Внутри сети злоумышленники свободно перемещаются незамеченными с помощью известных уязвимостей и легитимного ПО, не вызывающего подозрений у администраторов.

Используя недостатки защиты корпоративной сети, злоумышленники за короткое время получают полный контроль над всей инфраструктурой банка. Сейчас банки должны сосредоточиться на обеспечении безопасности во внутренней сети и внедрении средств защиты, которые позволят оперативно выявлять следы атак в инфраструктуре.

Блокчейн — относительно новая технология, и необходимо особое внимание к построению и эксплуатации основанных на ней систем, в том числе с точки зрения безопасности. Обеспечение безопасности используемых блокчейн-систем требует от кредитно-финансовых организаций внедрения методологии безопасной разработки смарт-контрактов; детального анализа архитектуры и конфигурации инфраструктуры информационной системы, построенной на базе блокчейна; обязательного анализа исходного кода информационной системы и смежных компонентов; регулярной независимой оценки безопасности как самой блокчейн-системы в целом (включая тестирование на проникновение), так и отдельных ее компонентов (смарт-контрактов, веб- и мобильных приложений).

Защищенность онлайн-банкинга и мобильного банкинга

Общий тренд: пароли, финансовая информация и персональные данные пользователей остаются в зоне риска

К числу ключевых тенденций 2018 г. в области защищенности онлайн-банкинга относится сокращение доли уязвимостей высокого уровня риска (с 32% в 2017 г. до 15% в 2018 г.).

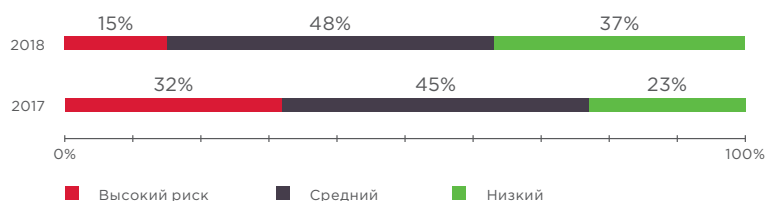


Рисунок 11. Доля уязвимостей различного уровня риска

Теряет актуальность критически опасная уязвимость «Недостаточная аутентификация»: в 2018 г. не зафиксировано ни одного приложения, в котором бы она оставалась.

Однако по-прежнему во многих системах операции повышенной важности совершаются без дополнительного (второго) фактора аутентификации. При этом продолжают оставаться под угрозой личная информация клиентов и банковская тайна: риск несанкционированного доступа к личным данным клиентов и банковской тайне (к выпискам по счету или платежным поручениям других пользователей) существует в каждом исследованном в 2018 г. онлайн-банке (по итогам 2017 г. этот показатель составил 94%). Из-за ошибок в логике работы онлайн-банка остается риск мошеннических операций и кражи денежных средств: например, в результате так называемых атак на округление суммы денежных средств при конвертации валюты.

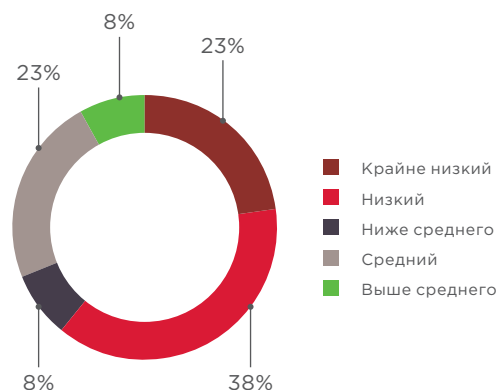


Рисунок 12. Уровень защищенности онлайн-банков (доля систем)

Ключевые проблемы:
ошибки бизнес-логики
систем и уязвимости кода

В мобильных приложениях уязвимости высокого уровня риска обнаружены в 38% приложений для iOS и 43% приложений для платформ под управлением Android (в 2017 г. уязвимости такого типа обнаружены в 25 и 56% приложений соответственно). Большинство проблем безопасности — общие для обеих платформ. Небезопасное хранение данных — основной недостаток, он выявлен в 76% мобильных приложений (что на 11% выше показателя 2017 г.). Под угрозу попадают пароли, финансовая информация, и персональные данные пользователей. Злоумышленнику редко требуется физический доступ к смартфону, чтобы украсть данные: 89% уязвимостей могут быть использованы с использованием ВПО.

Онлайн-банки

На первое место вышли ошибки в реализации механизмов двухфакторной аутентификации: в некоторых онлайн-банках не применяются одноразовые пароли (one-time password, OTP) для критически важных действий (аутентификация, смена учетных данных и другое) или пароли имеют слишком большой срок действия. Это может быть связано с тем, что банки стремятся найти баланс между безопасностью и удобством использования приложений. Так, ради удобства применения и возможности сэкономить на SMS-сообщениях для OTP в системах ДБО сегодня часто используют механизмы адаптивной аутентификации, в частности риск-ориентированную модель аутентификации (risk-based authentication). Однако отказ даже от части мер безопасности в пользу удобства повышает риск совершения мошеннических операций. Так, если нет необходимости подтверждать операцию с помощью одноразового пароля, злоумышленнику больше не требуется доступ к мобильному телефону жертвы, а слишком большой срок действия пароля повышает шанс его успешного подбора.

В 2018 г. до 31% выросла (в 2017 г. — 6%) доля приложений, в результате атак на которые злоумышленник может повлиять на бизнес-логику системы (в 2017 г. — 6%). Вероятно, это связано с ростом числа уязвимостей в коде приложений, разработанных банками самостоятельно. В 2018 г. доля таких уязвимостей достигла 59%, в то время как в 2017 г. она составляла 39%. Системы ДБО, разработанные банками самостоятельно, уязвимее готовых решений: среднее число уязвимостей в приложениях собственной разработки в три раза больше, чем в системах, предлагаемых вендорами (в 2017 г. оба показателя были близки по своему значению).

Большинство уязвимостей и у вендоров, и в собственных разработках относятся к уязвимостям кода. Но вендоры чаще допускают ошибки на этапе проектирования, а в собственных решениях банков уязвимости закладываются на этапе написания кода. К этой группе относятся, например, «Межсайтовое выполнение сценариев» и «Внедрение SQL-кода».

Разработчики систем ДБО сосредоточены на функциональных возможностях больше, чем на безопасности. Как следствие, 75% уязвимостей в покупных решениях связаны с недостатками механизмов защиты. Примеры уязвимостей в механизмах защиты — «Недостаточная защита от подбора учетных данных», «Недостаточная авторизация».

К числу наиболее распространенных уязвимостей конфигурации относятся раскрытие чувствительных данных в сообщениях об ошибках и версий используемого ПО в заголовках ответов веб-сервера.

Мобильный банкинг

Общий уровень защищенности клиентских частей мобильных приложений для Android и iOS примерно одинаков. Около трети всех уязвимостей в клиентских частях мобильных приложений для обеих платформ имеют высокий уровень риска. Аутентификационные данные небезопасно хранятся в 53% мобильных приложений.

Серверные части мобильных приложений в равной степени содержат уязвимости в коде самого приложения и в механизмах его защиты. В числе последних стоит отметить недостатки реализации двухфакторной аутентификации, позволяющие злоумышленнику совершать операции от имени законного пользователя, например переводить деньги с его счета на свой.

В среднем каждая серверная часть содержит пять уязвимостей кода и одну уязвимость конфигурации. Недостаточная авторизация выявлена в 43% серверных частей в 2018 г. (в 2017 г. — в 50%). Это один из самых распространенных недостатков высокого уровня риска, его доля составила 45% от всех критически опасных уязвимостей.

Большинство недостатков связаны с ошибками в механизмах защиты: 74% (в 2017 г. — 75%) и 57% (66%) — для приложений на iOS и Android соответственно, 42% (75%) — для серверных частей. Такие уязвимости возникают на этапе проектирования, а их устранение требует внесения существенных изменений в код.

Резюме:

общий уровень защищенности приложений для банкинга остается недостаточным

Несмотря на сокращение доли уязвимостей высокого уровня риска, защищенность онлайн-банков остается низкой. Одно из серьезнейших последствий атаки на них — кража денежных средств. В 2018 г. эта угроза отмечалась в 54% онлайн-банков (в 2017 г. этот показатель был на 4% ниже). Угроза несанкционированного доступа к информации клиентов и банковской тайне актуальна для каждого исследованного онлайн-банка, а в отдельных случаях уязвимости позволяли развивать атаку до проникновения в корпоративную инфраструктуру.

При разработке мобильных приложений безопасности уделяется недостаточно внимания, и основная проблема связана с небезопасным хранением данных; злоумышленники могут получить данные банковских карт и персональные данные пользователей.

Мобильные и онлайн-банки — популярные каналы для атаки на клиентов финансовых организаций. Общее повышение уровня защищенности финансовых организаций, а также то, что атаки на онлайн-банки не требуют такой высокой квалификации и подготовки, как атаки на инфраструктуру, может привести к переключению внимания части злоумышленников с финансовых организаций на их клиентов. В первую очередь под угрозой юридические лица, поскольку у них можно украсть более крупные суммы денег.

Защищенность банкоматов, платежных терминалов

Общий тренд:

blackbox продолжают лидировать

Логические атаки на банкоматы набирают популярность с 2009 г., когда был обнаружен троян Skimer, позволяющий похищать деньги и данные платежных карт. Skimer продолжает развиваться и по сей день, а наряду с ним появляются все новые семейства вредоносных программ — GreenDispenser, Alice, Ripper, Radpin, Ploutus и другие, продающиеся на форумах дарквеба. Цены на них начинаются от 1500 долл. США, но потенциальная прибыль значительно превышает расходы. В 2017 г. было обнаружено ПО CutletMaker, свободно продававшееся вместе с подробной инструкцией по использованию за 5000 долл. США.

В начале 2018 г. в США прошла волна «джекпоттинга»: преступники устанавливали на банкоматы вредоносное ПО Ploutus-D, позволявшее управлять выдачей наличных. В арсенале преступников присутствовал медицинский эндоскоп — с его помощью они проходили физическую аутентификацию без доступа к сейфу.

Хотя доля атак на банкоматы и POS-терминалы за год сократилась с 3 до 1% от общего числа инцидентов, они по-прежнему остаются в тренде. По данным Европейской ассоциации безопасных транзакций (The European Association for Secure Transactions, EAST), в 2018 г. было зафиксировано 157 логических атак на банкоматы, причем 156 из них относились к типу blackbox.

Ключевые проблемы:

blackbox и доступ к банкомату изнутри локальной сети

Все уязвимости, встречающиеся при анализе защищенности банкоматов, делятся на четыре группы:

1. Недостатки сетевой безопасности, позволяющие злоумышленнику, который получил доступ к сети банкомата, проводить атаки на сетевое оборудование, на доступные сетевые службы, перехватывать и подменять трафик. Такие атаки могут позволить подменить ответы процессингового центра или получить контроль над банкоматом. В исследуемых системах часто выявлялись недостатки межсетевого экранирования (88% банкоматов) и недостаточная защита данных, передаваемых между банкоматом и процессинговым центром (шифрование передаваемых данных отсутствовало в 58% банкоматов).
2. Недостатки защиты периферийных устройств, например отсутствие аутентификации между периферийным оборудованием и ОС банкомата (96% банкоматов), позволяют преступнику обращаться к этим устройствам после заражения банкомата вредоносным ПО или напрямую подключать свое оборудование к диспенсеру или картридеру. Это может привести к краже денег или перехвату данных платежных карт.

3. Недостатки конфигурации систем и устройств, то есть пробелы в защите, которыми злоумышленник может воспользоваться, имея доступ в сервисную зону, — например, отсутствие шифрования жесткого диска (92% банкоматов), недостаточная защита от выхода из режима «киоска» (85%), возможность подключения произвольных устройств (81%);
4. Уязвимости и недостатки конфигурации приложений класса Application Control: они направлены на предотвращение выполнения постороннего кода в системе, однако на проверку оказались недостаточно эффективными в 88% случаев. Уязвимости могут изначально содержаться в их коде или появиться как результат неправильной конфигурации.

Основные типы атак, которые были зафиксированы в России в 2018 г., — это blackbox и доступ к банкомату изнутри локальной сети банка. Атака blackbox подразумевает возможность напрямую подключить к диспенсеру свое устройство, запрограммированное на отправку команд для выдачи купюр.

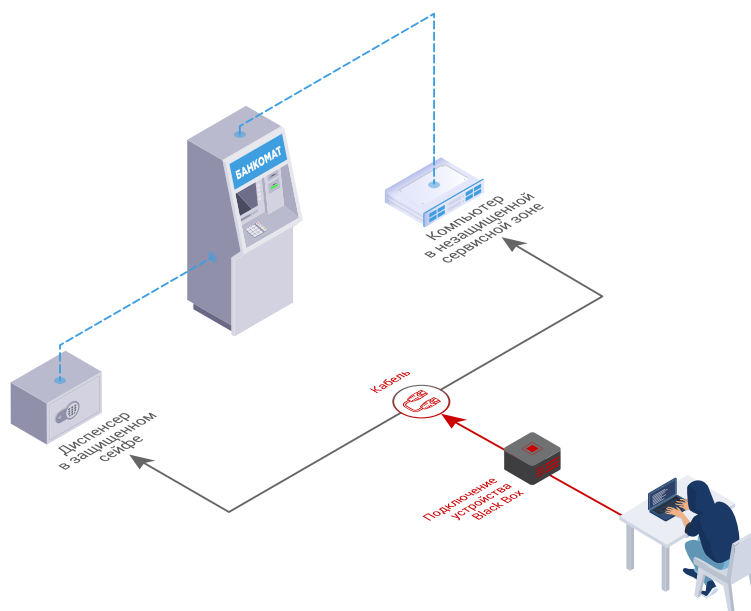


Рисунок 13. Атака blackbox

Результаты работ по анализу защищенности банкоматов, проведенных в 2017–2018 гг., показывают, что к такой атаке уязвимы 69% банкоматов. Причина этого в 50% случаев — использование недостаточно надежного шифрования между диспенсером и ОС, а еще в 19% — отсутствие каких-либо мер защиты против blackbox. На некоторых моделях банкоматов для проведения атаки преступнику требуется всего 10 минут.

При проведении тестов на проникновение доступ к управлению банкоматами из внутренней сети удалось получить в 25% банков. Это связано с общим низким уровнем защищенности во внутренней сети банков.

Во всех исследуемых банкоматах был возможен перехват данных с магнитной полосы карты из-за отсутствия аутентификации и шифрования данных при взаимодействии с картридером, а в 58% банкоматов — из-за отсутствия шифрования при передаче данных между банкоматом и процессингом.

Резюме: велик риск новых атак со стороны кибергруппировок и неквалифицированных злоумышленников

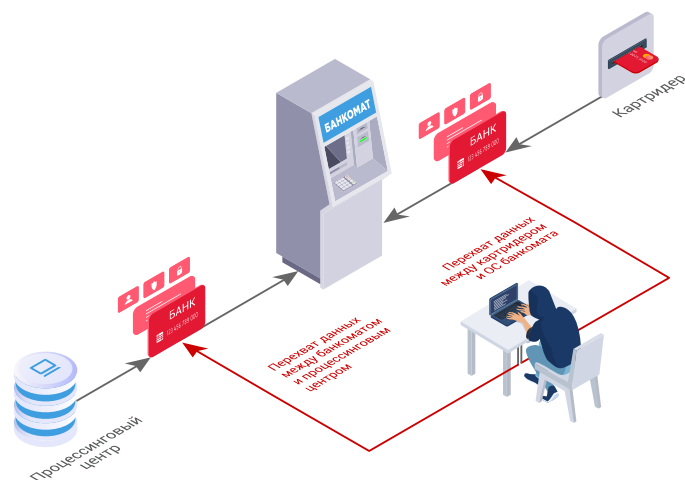


Рисунок 14. Варианты атак, направленных на перехват карточных данных

Уязвимости, связанные с сетевой безопасностью, недостатками конфигурации, недостаточной защитой периферийных устройств, в совокупности позволяют похитить деньги из банкомата или перехватить данные банковских карт. Используемые механизмы безопасности не являются серьезным препятствием для атаки: почти во всех случаях была выявлена возможность обхода установленных средств защиты. Часто одна и та же конфигурация используется на множестве банкоматов, поэтому успешная атака на один банкомат позволяет преступникам провести серию аналогичных с использованием одного сценария. На теневом рынке спрос на ВПО для банкоматов остается высоким, а значит, следует готовиться к новым атакам как со стороны крупных преступных группировок, так и изкоквалифицированных хакеров.

Защищенность платежных терминалов (POS)

Общий тренд:
mPOS'ы защищены
недостаточно

Ключевые проблемы:
от выполнения произвольных операций
до перехвата данных

В последние годы число операций, выполняемых с помощью mPOS-терминалов, существенно возросло. Острая конкуренция среди поставщиков mPOS привела к упрощению получения платежного терминала. Как и обычные POS-терминалы, они являются конечным звеном платежной инфраструктуры. Это делает их интересными и легко доступными для злоумышленников. Больше 50% исследованных mPOS-терминалов уязвимы для атак, при этом в целом уязвимыми оказались все проанализированные поставщики mPOS-терминалов. Зарегистрированы многочисленные серьезные проблемы безопасности, в частности уязвимость для выполнения произвольных команд, подделки суммы и выполнения удаленного кода. Аппаратные механизмы защиты терминалов в большинстве случаев надежны и развиты. Однако другие аспекты защищены гораздо слабее.

Злоумышленник может подключиться к устройству через bluetooth и осуществлять произвольные операции. Для этого ему нужна информация о bluetooth-сервисах, запущенных на устройстве, а также соответствующих характеристиках и функциях. Эту информацию можно получить с помощью реверс-инжиниринга до проведения атаки. Злоумышленнику требуется лишь доступ к mPOS-терминалу, телефон, который поддерживает регистрацию событий интерфейса хост-контроллера (HCI), и мобильное приложение. Этот вектор атаки может использоваться совместно с эксплуатацией других уязвимостей, чтобы предложить клиенту менее безопасные типы операций, например по магнитной полосе.

Исследования показали наличие риска перехвата HTTPS-трафика между мобильным приложением и сервером платежной системы с последующим изменением суммы транзакции. Недобросовестный продавец может обманным путем заставить владельца карты подтвердить операцию на гораздо большую сумму.

Часть протестированных терминалов уязвима для удаленного выполнения кода, что может обеспечить злоумышленнику полный доступ к ОС терминала. После получения полного доступа к операционной системе злоумышленник сможет перехватить данные Track2 до шифрования или включить незашифрованный режим (для отправки команды) на клавиатуре терминала для перехвата PIN-кода.

Резюме: упрощение входа на рынок карточных платежей не снимает ответственности за их безопасность

Разработчики mPOS-терминалов подчеркивают простоту регистрации и использования устройств. Это ключевые элементы бизнес-модели, но она не учитывает, что снижение барьеров входа на рынок карточных платежей должно сопровождаться существенным увеличением безопасности. Нет сомнений в том, что мошеннические действия продавцов останутся серьезной проблемой поставщиков mPOS-терминалов. Необходимо разработать серьезный подход к проблеме безопасности, включая проверку в ходе регистрации и строгий мониторинг платежей.

Защищенность инвестиционных и трейдинговых приложений

Общий тренд: существенный риск проведения несанкционированных операций

Выбирая торговую платформу, трейдеры руководствуются функциональностью, облегчающей их задачи. Однако не все задумываются о безопасности этих приложений. Если хакер получит доступ к какой-то из функций — скажем, сможет изменить параметры автоматического закрытия сделки, — трейдер потерпит убытки. Кроме того, в личных кабинетах пользователей хранится конфиденциальная информация: данные о сделках, история операций, информация о доступных средствах на балансе. Исследования показали, что популярные торговые терминалы не защищены от атак: уязвимости найдены в каждом исследованном приложении, при этом 72% приложений содержали хотя бы одну критически опасную уязвимость. Во всех случаях недостатки защиты позволяли атаковать пользователей.

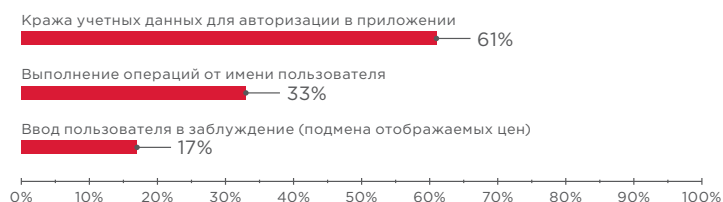


Рисунок 15. Угрозы, представляющие наибольшую опасность для трейдеров

33% изученных приложений имели уязвимости, позволяющие проводить финансовые операции от имени других пользователей. Такие атаки могут вызвать изменение цен на рынке, отразиться на большом количестве пользователей, затронуть частных трейдеров и крупные компании — банки, международные торговые корпорации, финансово-инвестиционные организации; вызвать беспорядки на бирже и привести к потере денег.

Ключевые проблемы:

недостатки шифрования,
небезопасное хранение дан-
ных, риск перехвата данных

Мы выделяем два вероятных сценария атак:

1. Трейдер с одного и того же устройства пользуется торговым терминалом и посещает сайты в Интернете. На одном из посещаемых им сайтов хакер разместил вредоносный JavaScript-код, который, не требуя дополнительных действий со стороны пользователя, атакует его терминал и покупает или продает активы. Антивирус не отреагирует на выполнение вредоносного кода, поскольку для атаки не нужно загружать файл на компьютер пользователя или выполнять команды в ОС.
2. Злоумышленник находится в одной сети с трейдером; например, трейдер подключен к сети по wi-fi или через оборудование, которое контролирует злоумышленник. Так злоумышленник сможет перехватывать и изменять трафик пользователя. Атака возможна и в том случае, если канал связи недостаточно защищен и перехват трафика происходит на стороне провайдера.

Уязвимости, обнаруженные в десктопных приложениях, преимущественно заключались в отсутствии шифрования передаваемых данных (42%) и возможности выполнения произвольных команд (29%). Атаки на десктопные приложения могут привести к тому, что злоумышленник получит контроль над компьютером трейдера и сможет развивать атаку на инфраструктуру организации.

В мобильных приложениях большинство уязвимостей (57%) были связаны с небезопасным хранением данных. При анализе веб-приложений были обнаружены уязвимости в коде и конфигурации, во всех приложениях отсутствовали HTTP-заголовки, обеспечивающих дополнительную защиту от некоторых видов атак (например от атак типа Clickjacking и «Межсайтовое выполнение сценариев»). Атаки на веб-приложения могут носить массовый характер и оказывать существенное влияние на изменение цен.

Сегодня атаки на приложения для трейдинга еще не распространены, злоумышленники, возможно, только изучают потенциальные способы атак. Однако в силу слабой защищенности трейдинговых приложений и традиционного стремления злоумышленников к легкой масштабируемости и быстрой монетизации атаки на пользователей трейдинговых систем имеют все шансы превратиться в массовые в ближайшее время.

Резюме:

атаки на пользователей
трейдинговых систем
могут стать реальностью

Общие выводы, прогнозы и рекомендации Positive Technologies

В 2018 г. на фоне увеличения общего количества кибератак на кредитно-финансовые организации наблюдалось значительное снижение финансового ущерба. Уменьшение числа успешных атак во многом связано с деятельностью ФинЦЕРТ, но еще один немаловажный фактор — это арест участников крупных преступных группировок. В ближайшее время возможно появление ряда новых группировок и инструментов, что спровоцирует новую волну атак.

Защита сетевого периметра финансовых организаций находится на достаточно высоком уровне, поэтому основным методом проникновения в инфраструктуру финансовых организаций останется доставка вредоносного ПО путем фишинговых рассылок. Стоит ожидать, что преступники будут вкладывать значительные средства в закупку неопубликованных эксплойтов для уязвимостей нулевого дня на теневом рынке.

Общее повышение уровня защищенности финансовых организаций может привести к тому, что часть злоумышленников попробует свои силы на других целях: клиентах банков, платежных устройствах и банкоматах. Проблемы, выявляемые при анализе защищенности банкоматов, платежных терминалов и финансовых приложений, говорят об острой необходимости совершенствования систем защиты.

Мы рекомендуем финансовым организациям активно участвовать в обмене информацией о кибератаках и индикаторах компрометации. Центры мониторинга и реагирования на инциденты (например, ФинЦЕРТ Банка России) помогают значительно снизить успешность кибератак на кредитно-финансовую сферу. Кроме того, необходимо быть готовым оперативно выявлять следы атак в своей инфраструктуре. Крайне важно постоянно отслеживать аномальную активность в сети своей компании, чтобы обнаруживать и исследовать новые неизвестные атаки, делиться такой информацией с другими финансовыми организациями.

Обнаружить атаку хорошо подготовленной кибергруппировки в момент проникновения в локальную сеть сегодня невозможно, крайне сложно сделать это и на этапе закрепления и распространения в инфраструктуре. Зачастую ситуация усугубляется неготовностью самой инфраструктуры атакованной организации к выявлению атак. Надеяться на защиту отдельных серверов и рабочих станций с помощью типовых решений бесполезно. Сегодня важно понимать, насколько эффективны те системы, которые внедрены в компании для обеспечения безопасности ключевых активов. Преступники уже давно научились обходить антивирусы, «песочницы», системы обнаружения вторжений. Компаниям необходимо реализовать комплексный подход, позволяющий сузить круг возможностей нарушителя и обеспечить максимальное понимание происходящих в инфраструктуре событий безопасности в контексте системных журналов, трафика и объектов, циркулирующих в сети. Только в этих условиях возможно построение процесса Threat Hunting, позволяющего успешно выявлять действия группировок уже внутри инфраструктуры.

Глубокий анализ трафика, ретроспективный анализ событий ИБ, профилирование действий пользователей и возможность исследования оперативной памяти, процессов и других форензик-артефактов позволяют значительно сократить время присутствия злоумышленников в инфраструктуре и предотвратить достижение поставленных ими целей. И конечно, средства защиты будут неэффективны без поддержки высококвалифицированных специалистов в области расследования инцидентов.

О Positive Technologies

Positive Technologies — один из мировых лидеров в сфере комплексной защиты крупных информационных систем от современных киберугроз, уже более 16 лет аккумулирует экспертные знания по кибербезопасности. Компания имеет представительства в России и за рубежом (в Великобритании и Чехии). Экспертная команда включает в себя и специалистов в области защиты прикладных банковских систем, АБС, ДБО, банкоматов, платежных терминалов, онлайн- и мобильных платежных систем. Ежегодно компания выполняет десятки проектов по анализу защищенности сетей банкоматов и POS-терминалов, систем ДБО (от анализа сетевой инфраструктуры и информационных потоков до выявления уязвимостей нулевого дня в аппаратном обеспечении банкоматов); выявляет более 150 уязвимостей в системах ДБО; проводит десятки расследований взломов инфраструктуры организаций, в том числе в кредитно-финансовом секторе (выявление и ликвидация последствий деятельности группировок Cobalt, Silence, RTM). Компания – активный участник информационного обмена в финансовой отрасли. С 2016 г. (с момента подписания соглашения об информационном обмене) сотрудничает с ФинЦЕРТ: за 2018 г. экспертный центр безопасности Positive Technologies ([PT Expert Security Center](#)) направил в ФинЦЕРТ несколько десятков уникальных уведомлений об актуальных угрозах. Также с 2018 г. запущен дополнительный канал коммуникации с банковским сообществом, который позволяет уведомлять комьюнити об угрозах с минимальной задержкой от момента их выявления.

Результаты исследований используются при разработке продуктов компании: систем [MaxPatrol 8](#), [PT Application Firewall](#), [PT Application Inspector](#), [MaxPatrol SIEM](#), [PT MultiScanner](#) и других. Эти решения позволяют обеспечить безопасность веб-приложений, оценить уровень защищенности сетей, блокировать атаки в режиме реального времени, контролировать выполнение нормативных требований и соответствие государственным и корпоративным стандартам.

Positive Technologies является организатором ежегодного международного форума по практической кибербезопасности [Positive Hack Days](#), а также развивает портал [SecurityLab.ru](#).

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.