POSITIVE TECHNOLOGIES

Исследование защищенности приложений для трейдинга

Содержание

Введение 2
Существующие угрозы 3
Десктопные приложения 5
Мобильные приложения 7
Веб-приложения 11
Заключение 12

Введение

Возможность принять участие в операциях на финансовых рынках доступна любому желающему. Для того чтобы присоединиться к торгам, достаточно зайти на сайт брокерской компании или установить приложение на телефон. На сайте investing.com можно найти список из более чем 700 приложений для трейдинга — торговых терминалов, которые позволяют покупать и продавать акции, облигации, фьючерсы, валюту и другие активы.

При выборе торговой платформы трейдеры в первую очередь руководствуются имеющейся функциональностью, которая облегчает их задачи. Так, встроенные инструменты для анализа рынка и рекомендации экспертов помогают построить собственную торговую стратегию, а возможность автоматической торговли позволяет открывать и закрывать сделки без участия трейдера. Однако далеко 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 множество конфиденциальной информации: данные о текущих и планируемых сделках, история операций, информация о доступных средствах на балансе.

При работе с терминалом трейдер должен быть уверен, что его информация надежно защищена, что он получает достоверные сведения о состоянии рынка и при этом никто не может вмешаться в процесс торговли. Соответствуют ли приложения для трейдинга этим требованиям? Чтобы ответить на этот вопрос, эксперты Positive Technologies проанализировали торговые платформы шести вендоров, которые популярны не только среди частных трейдеров, но и используются в банках, инвестиционных фондах и иных организациях, деятельность которых связана с биржевой торговлей. В совокупности эти платформы составили 11 мобильных приложений (для Android и iOS), четыре веб-приложения, а также три десктопные версии. Исследования проводились в отношении клиентских частей приложений.

Сделанные выводы могут не отражать актуальное состояние защищенности информационных систем в других организациях. Анализ проведен с целью обратить внимание специалистов по ИБ в финансовой отрасли на наиболее актуальные проблемы и помочь им своевременно выявить и устранить уязвимости.

Существующие угрозы

Уязвимости были найдены в каждом исследованном приложении, при этом 72% приложений содержали хотя бы одну критически опасную уязвимость. Во всех случаях недостатки защиты позволяли атаковать пользователей.

Наибольшую опасность для участников торгов представляют следующие угрозы:

- выполнение операций от имени пользователя,
- кража учетных данных для авторизации в приложении,
- ввод пользователя в заблуждение (подмена отображаемых цен).

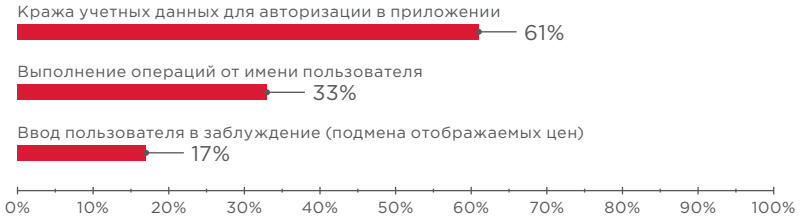

Рисунок 1. Наиболее опасные для трейдеров угрозы (доли уязвимых приложений)

В 33% приложений, которые входят в четыре из шести рассмотренных трейдинговых платформ, присутствуют уязвимости, позволяющие проводить финансовые операции от имени других пользователей. Такие атаки могут вызывать изменение цен на рынке в пользу злоумышленника.

Приведем пример. Предположим, что злоумышленник приобрел акции некой компании. Однако цена на них не растет или растет слишком медленно. В этом случае ему нужно искусственно повысить спрос: если бы другие инвесторы начали активно покупать эти акции, они бы поднялись в цене. Поскольку ждать такого момента можно долго, злоумышленник самостоятельно совершает сделки за других участников, после чего продает свои акции по выгодной цене. Точно так же злоумышленник может манипулировать курсами валют — если атака затронет крупных игроков или большое количество пользователей.

Хакерская атака может вызвать хаотичное изменение цен и спровоцировать панику на финансовом рынке. В 2015 году атака на Энергобанк привела к резким изменениям курса доллара к рублю на Московской бирже: в течение 15 минут от имени Энергобанка выставлялись поддельные заявки на покупку и продажу валюты. Банк оценил потери в 243,6 млн рублей. Атаки хакеров сказываются и на котировках криптовалют. В начале 2018 года злоумышленники вывели с биржи Coincheck криптовалюту NEM на сумму более 500 млн долларов США, что повлекло за собой общее падение курсов, а NEM при этом потеряла в стоимости 16%.

В 61% случаев злоумышленник может получить контроль над личным кабинетом пользователя. Недостатки защиты мобильных и десктопных версий платформ позволяют узнать чужие учетные данные и авторизоваться в приложении, если не используется двухфакторная аутентификация. При атаке на веб-приложение злоумышленник может перехватить сессию пользователя и получить доступ к его личному кабинету.

Уязвимостям, с помощью которых злоумышленник может подменить цены, отображаемые пользователю, подвержены 17% приложений. В результате трейдер будет принимать решения на основе подложных данных и совершать убыточные сделки.

Существуют два распространенных 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. Внутри компании сегмент сети, в котором осуществляется торговля, должен быть изолирован, но на практике это может оказаться не так, и у трейдеров будет доступ в интернет. Недостатки сегментации часто выявляются нашими экспертами при проведении тестов на проникновение во внутренней сети.

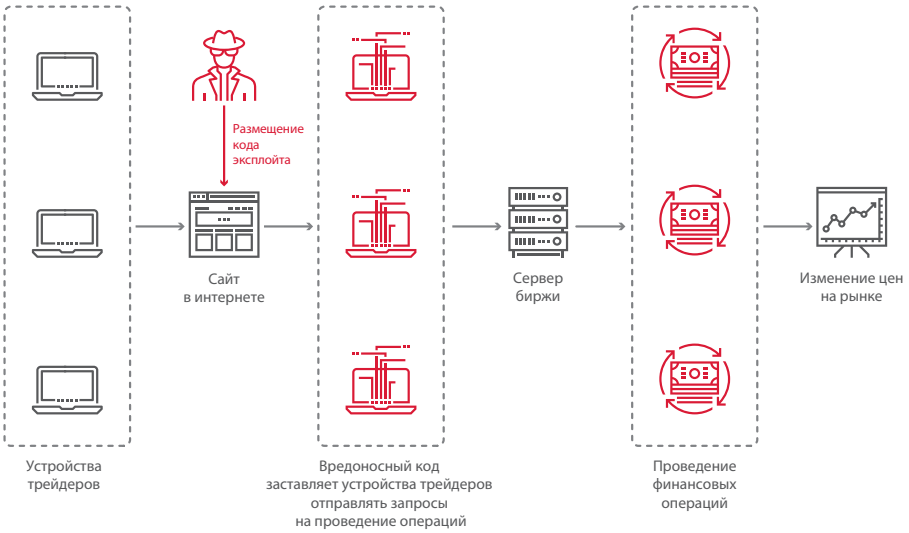

Рисунок 2. Сценарий массовой атаки на пользователей приложения

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, как это недавно случилось с пользователями электронного кошелька MyEtherWallet.

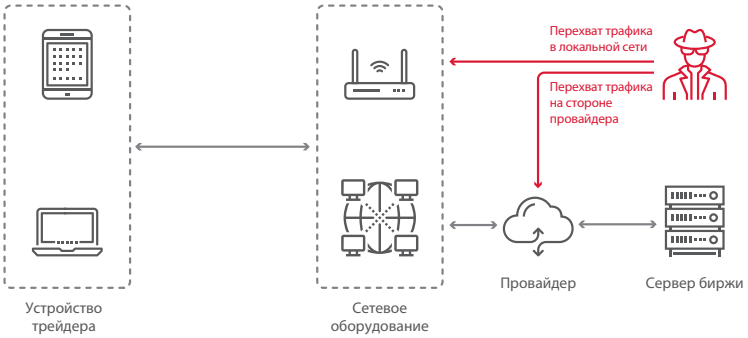

Рисунок 3. Сценарий атаки, включающей перехват сетевого трафика

Рассмотрим подробнее уязвимости, которые мы обнаружили в разных версиях торговых платформ.

Десктопные приложения

Эксплуатация выявленных уязвимостей предполагает, что злоумышленник находится в одной сети с атакуемым пользователем либо компьютер трейдера заражен вредоносным ПО. В 2017 году в рамках работ по тестированию на проникновение экспертам Positive Technologies удалось преодолеть внешний сетевой периметр 68% компаний. И хотя финансовые организации прикладывают значительно больше усилий для защиты своего периметра, проникнуть во внутреннюю сеть банков получилось в 22% случаев, а для атак с помощью социальной инженерии оказались уязвимы 75% банков.

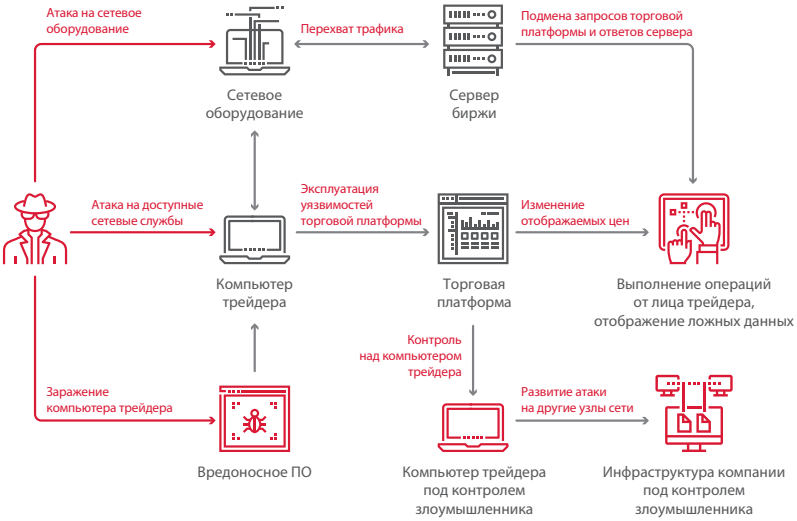

Рисунок 4. Сценарии атак на пользователей десктопных торговых платформ

Контроль над компьютером трейдера

В двух рассмотренных приложениях были обнаружены опасные уязвимости, позволяющие выполнить произвольные команды на компьютере пользователя. Таким образом злоумышленник мог бы получить доступ к важной информации пользователя, хранящейся на рабочей станции, и даже полностью взять под контроль управление его компьютером. Одно из этих приложений при запуске проверяет наличие обновлений. Запрос к серверу и ответ, содержащий файл с обновлениями, передаются в открытом виде, поэтому если подменить ответ сервера, вместо новой версии установится вредоносная программа.

Wireshark · Follow TCP Stream (tcp.stream eq 10) · update

```
GET /files/[redacted].zip HTTP/1.1
Host: support.[redacted]
Accept: text/html, */*
Accept-Encoding: identity
User-Agent: Mozilla/3.0 (compatible; Indy Library)
Authorization: [redacted]

HTTP/1.0 200 OK
Server: BaseHTTP/0.3 Python/2.7.6
Date: Thu, 23 Aug 2018 13:20:58 GMT
Content-type: application/zip, application/octet-stream
Content-Disposition: attachment; filename="[redacted].zip"
```

Рисунок 5. Передача запроса на обновление приложения в открытом виде

Подделка операций

По умолчанию одно из приложений передает данные в открытом виде, чем может воспользоваться злоумышленник, который находится в одной сети с атакуемым пользователем. Злоумышленник может перехватить и изменить трафик: подменить запрос от трейдера и тем самым выполнить от его имени нежелательную операцию.

Отображение ложных данных

Обнаруженные уязвимости могли использоваться для изменения цен, показываемых в терминале, что вынудило бы трейдера изменить решение о покупке или продаже определенных активов.

В ходе исследования нашим экспертам удалось подделать интервальный график типа «японские свечи», который отображает изменения котировок за определенные периоды. На основе этого графика трейдер делает выводы о том, как движется курс, и принимает решение о последующих операциях. Информация о ценах поступает от сервера брокера и записывается в локальную базу данных, а затем по этим значениям приложение отрисовывает графики. Если подменить содержимое базы, то на экране будет отображаться тот вид «свечей», который нужен злоумышленнику.

Рисунок 6. Исходный вид «японских свечей» в торговом терминале

Рисунок 7. Изменение «свечей» в торговом терминале

Кража учетных данных

Одно из приложений передает учетные данные без использования шифрования. Злоумышленник, имеющий возможность перехватывать трафик пользователя, может получить доступ к его личному кабинету.

Выявленные уязвимости

Уязвимости, которые были обнаружены в приложениях, заключаются в отсутствии шифрования передаваемых данных и возможности выполнения произвольных команд. Для защиты от некоторых типов атак, направленных на выполнение произвольного кода, используются технологии DEP (Data Execution Prevention) и ASLR (Address Space Layout Randomization). DEP используется для предотвращения выполнения кода из тех областей памяти, в которых должны храниться данные, а ASLR изменяет расположение структур данных в адресном пространстве случайным образом. Эти технологии затрудняют эксплуатацию уязвимостей, которые могут присутствовать в исходном коде. При компиляции двух приложений не были установлены флаги, указывающие на необходимость применения DEP или ASLR.

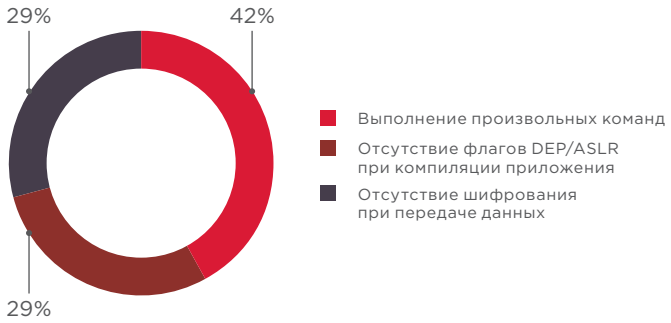

Рисунок 8. Уязвимости в десктопных приложениях

Мобильные приложения

В ходе исследования были проверены шесть приложений для Android и пять приложений для iOS. Пользователи этих приложений подвержены следующим угрозам:

- выполнение действий от имени пользователя;
- кража учетных данных;
- подмена информации о ценах;
- подбор PIN-кода приложения;
- проведение фишинговых атак.

Рисунок 9. Возможные атаки на пользователей приложений для Android (доли уязвимых приложений)

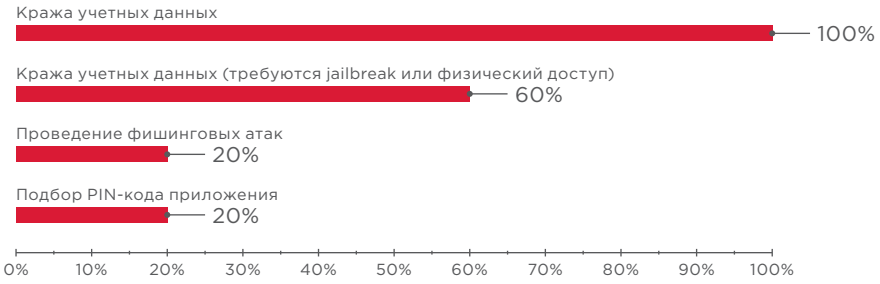

Рисунок 10. Возможные атаки на пользователей приложений для iOS (доли уязвимых приложений)

Эксплуатировать выявленные уязвимости можно при выполнении одного из условий:

- злоумышленник находится в одной сети с пользователем и имеет возможность перехватывать трафик;
- злоумышленник получил физический доступ к устройству;
- устройство пользователя заражено вредоносным ПО (особенно если при этом доступны права root или jailbreak).

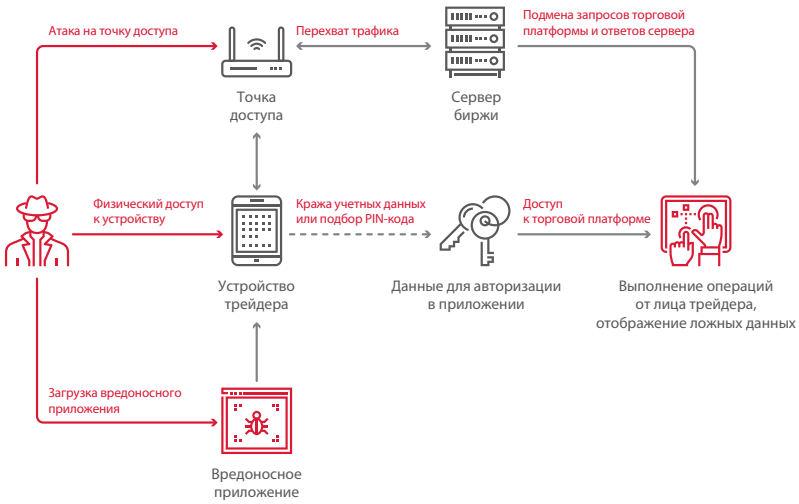

Рисунок 11. Сценарии атак на пользователей мобильных приложений

Покупка и продажа от имени пользователя

В двух приложениях для Android мы обнаружили уязвимости, которые позволяют выполнить любое действие от имени атакуемого пользователя или подменить информацию о текущих ценах. Злоумышленнику требуется находиться в одной сети с пользователем, чтобы прослушивать трафик и подменять запросы. Для этого нужно провести атаку «человек посередине», например подключить устройство пользователя к поддельной точке доступа Wi-Fi или поддельной базовой станции мобильного оператора.

Приложения устанавливали соединение с сервером по защищенному протоколу HTTPS. Это означает, что приложения должны проверять, действителен ли сертификат SSL, используемый сервером. Однако в нашем случае они игнорировали все ошибки, возникающие при проверке. Подменив сертификат, злоумышленник выдавал себя за сервер приложения и получал возможность перехватывать пользовательский трафик.

Кража учетных данных

Если злоумышленник узнает логин и пароль пользователя, то сможет получить доступ к его личному кабинету с другого устройства при условии, что в приложении не используется двухфакторная аутентификация.

Небезопасное хранение учетных данных было выявлено в трех приложениях для Android и трех приложениях для iOS, но для их получения требовался физический доступ к устройству или полные административные права (root-права или устройство с проведенным jailbreak). Тем не менее существуют и другие способы завладеть учетными данными.

Приложения для iOS не ограничивали возможность использования сторонних клавиатур. Такой подход небезопасен, поскольку сторонние расширения для клавиатуры могут оказаться кейлоггерами и похищать учетные данные пользователей. Кроме того, одно приложение для iOS передавало аутентификационные данные без шифрования.

Рисунок 12. Передача учетных данных в открытом виде

В приложении для Android была обнаружена уязвимость «Межсайтовое выполнение сценариев», которая позволяла узнать логин и пароль пользователя. В приложение встроен собственный браузер, в котором оно открывает ссылки на внутренние страницы, используя при этом логин и пароль пользователя. Проблема заключается в том, что приложение некорректно определяет, что ссылка является внутренней, тогда как на самом деле она ведет на внешний сайт. Злоумышленник может сформировать ссылку на собственный сайт таким образом, что приложение откроет ее в своем браузере, а затем похитить логин и пароль.

Подбор PIN-кода

Пользователь может потерять телефон или просто оставить его на виду у злоумышленника. Для защиты от несанкционированного доступа к приложению используется PIN-код, который злоумышленник может попытаться подобрать.

В двух приложениях разных разработчиков мы обнаружили возможность неограниченного перебора PIN-кода. Приложение для Android предоставляло три попытки ввода пароля; если код был трижды введен неправильно, приложение выходило из учетной записи пользователя. Приложение для iOS каждый раз при вводе неверного PIN-кода увеличивало задержку до следующей попытки. Однако в обоих случаях счетчик попыток сбрасывался при перезапуске приложения, поэтому перебирать код доступа можно было без ограничений.

Социальная инженерия и прочие угрозы

Другие угрозы, выявленные в мобильных приложениях, связаны с возможностью проведения атак методами социальной инженерии. Приложения позволяли отправлять поддельные уведомления или перенаправлять пользователей на фишинговые сайты.

В Android приложения могут обмениваться сообщениями, например отправлять друг другу оповещения о событиях. Если торговый терминал не ограничивает список приложений, от которых он получает оповещения, а на устройстве пользователя установлено вредоносное приложение, то оно может отправить терминалу

специальное сообщение, которое появится в панели уведомлений. В одном из приложений сообщения отображались и во внутреннем чате, что позволяло создать видимость настоящего диалога с пользователем. Распространенный сценарий социотехнической атаки — отправка письма от имени технической поддержки, в котором содержится ссылка на сайт злоумышленника, замаскированный под страницу авторизации для входа в личный кабинет. Таким угрозам подвержены 33% приложений для Android.

Половина приложений для Android и 20% приложений для iOS используют незащищенный протокол HTTP при переходе на внутренние ресурсы, например на страницы с новостями. Злоумышленник, который имеет возможность перехватывать трафик, может перенаправить пользователя на фишинговый сайт. Помимо рисков, связанных непосредственно с торговлей, пользователи подвержены и иным угрозам: злоумышленник может, к примеру, заразить их устройства вредоносным ПО.

Выявленные уязвимости

Приложения для обеих систем содержали в среднем по три уязвимости. Большинство уязвимостей связаны с небезопасным хранением данных, например хранением резервных копий и другой информации в публичных каталогах, а ключей для шифрования — в исходном коде приложения.

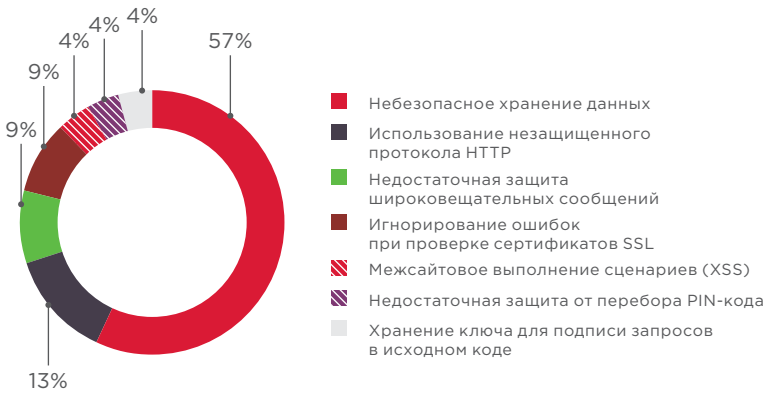

Рисунок 13. Уязвимости в мобильных приложениях для Android

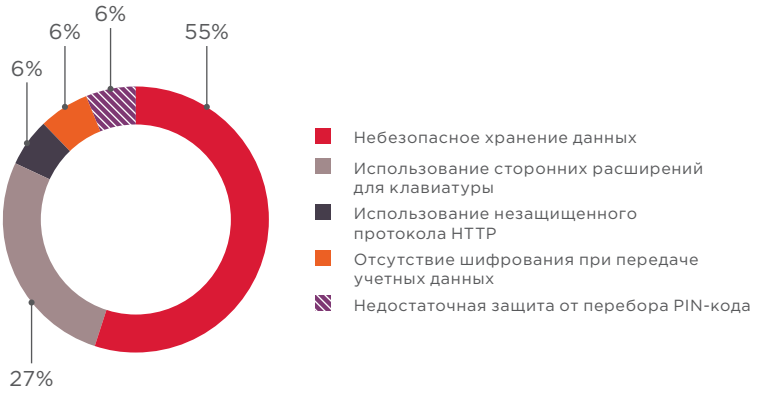

Рисунок 14. Уязвимости в мобильных приложениях для iOS

Веб-приложения

Если при атаке на торговый терминал для мобильного устройства или компьютера злоумышленнику нужны особые условия, в частности возможность перехватывать трафик или физический доступ к устройству, то для атак на клиентов веб-приложений этого не требуется. Атаки могут носить массовый характер и оказывать существенное влияние на изменение цен.

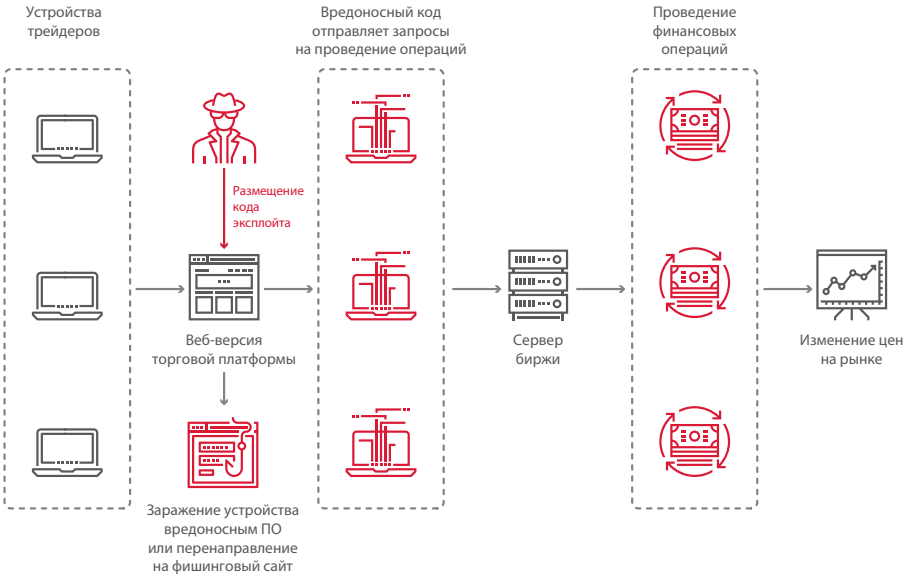

Рисунок 15. Сценарии атак на пользователей веб-приложений

Подделка операций пользователя

Во всех приложениях были выявлены уязвимости «Межсайтовое выполнение сценариев». Эта уязвимость используется для внедрения на страницу вредоносного кода, чтобы попытаться выполнить действие в приложении, к примеру перенаправить пользователя на сайт злоумышленника, похитить данные для авторизации на сайте или заразить компьютер вредоносной программой. В трех приложениях «Межсайтовое выполнение сценариев» позволяло злоумышленнику осуществить несанкционированные операции по покупке и продаже от имени пользователя. Одно приложение использует для авторизации дополнительный токен, который передается в каждом запросе и действует в течение короткого времени. Злоумышленник может похитить этот токен и выполнять любые действия от лица пользователя.

Выявленные уязвимости

Помимо уязвимостей в коде веб-приложений были также обнаружены уязвимости конфигурации. Во всех приложениях отсутствовали HTTP-заголовки, обеспечивающие дополнительную защиту от некоторых видов атак. Например, заголовок X-Frame-Options направлен на защиту от атак типа Clickjacking, а заголовок Content-Security-Policy препятствует выполнению атак с внедрением контента, в том числе «Межсайтового выполнения сценариев». Заголовок Strict-Transport-Security позволяет сразу устанавливать безопасное соединение по протоколу HTTPS — даже в случае перехода по ссылкам с явным указанием протокола HTTP.

Для защиты одной торговой платформы использовался межсетевой экран уровня приложений (web application firewall). Однако существующие правила корреляции оказались недостаточно эффективными и не позволили предотвратить атаки на приложение в ходе исследования. Необходимо внимательно относиться к выбору средств защиты и их конфигурации, а также проводить тестирование для проверки их эффективности.

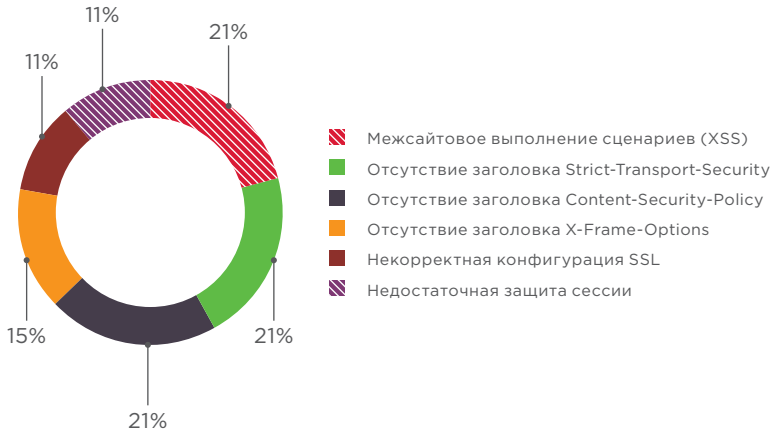

Рисунок 16. Уязвимости в веб-приложениях

Заключение

Результаты исследования показывают, что популярные торговые терминалы не защищены от злоумышленников. Кибератаки могут сказаться 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.

При выборе торговой платформы трейдерам следует обращать внимание не только на ее функциональность, но и на безопасность работы с ней. В противном случае трейдер рискует обнаружить, что от его имени совершают сделки посторонние лица, а реальная ситуация на финансовом рынке совсем не соответствует тому, что он видит на экране. Необходимо использовать только актуальные версии приложений и вовремя устанавливать обновления, выпускаемые вендором.

Частным трейдерам, которые используют торговые платформы на своих личных устройствах, требуется в первую очередь обеспечить защиту этих устройств — применять антивирусные средства и не загружать приложения из ненадежных источников. Не рекомендуется устанавливать мобильные версии приложений на устройства с правами root или проведенным jailbreak. Для предотвращения несанкционированного доступа к личному кабинету нужно использовать двухфакторную аутентификацию, если эта функция поддерживается приложением. При работе с торговым терминалом не следует подключаться к незащищенным сетям, таким как публичные точки доступа Wi-Fi, поскольку данные, передаваемые по ним, могут быть перехвачены злоумышленником. Кроме того, важно учитывать вероятность атаки методами социальной инженерии: не переходить по ссылкам на подозрительные ресурсы, с осторожностью относиться к сайтам с некорректными сертификатами, внимательно вводить учетные данные для доступа в личный кабинет на веб-ресурсах, а также проверять все вложения, полученные по электронной почте.

В корпоративных системах следует выделять отдельный сегмент сети, в котором расположены торговые терминалы, и обеспечивать защиту этого сегмента. При этом эффективная защита возможна только в том случае, если поддерживается высокий уровень защищенности инфраструктуры в целом и злоумышленник, тем или иным способом проникший в пользовательский сегмент сети, не сможет развить атаку и получить доступ к критически важным ресурсам. Для этого нужно следовать базовым рекомендациям по обеспечению приемлемого уровня защищенности корпоративных информационных систем, и в частности обучать сотрудников правилам информационной безопасности. Рекомендуется применять эффективные антивирусные средства для защиты конечных устройств и использовать технические

решения, направленные на своевременное обнаружение подозрительной активности в сети (SIEM-системы). Важно регулярно проводить внешнее и внутреннее тестирование на проникновение, чтобы выявлять потенциальные векторы атак и оценивать эффективность принятых мер защиты.

Для того чтобы обеспечить безопасность личных данных и сохранность денег своих клиентов, разработчикам необходимо более основательно подходить к вопросам информационной безопасности. Рекомендуется регулярно проводить тестирование защищенности приложений. Наибольшую эффективность при этом показывает тестирование методом белого ящика, то есть анализ исходного кода. Внедрение цикла безопасной разработки (secure software development lifecycle, SSDL) позволяет избежать многих ошибок еще на этапе проектирования приложения, а анализ кода в процессе его написания помогает существенно ускорить выявление и устранение возникающих уязвимостей. Для защиты веб-версий торговых платформ рекомендуется дополнительно использовать превентивные меры защиты, такие как межсетевой экран уровня приложений (web application firewall, WAF), который обнаруживает и предотвращает известные атаки на веб-приложения, а также выявляет эксплуатацию уязвимостей нулевого дня.

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.

Trading_Applications_A4.RUS.0003.04.SEP.14.2018