УГРОЗЫ ДЛЯ БАНКОВСКИХ КЛИЕНТОВ. НЕЦЕЛЕВЫЕ АТАКИ

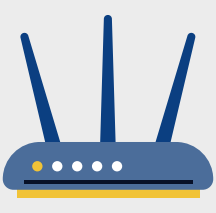
Часть 2

ROOT LEVEL RESOURCES

Основной угрозой для клиентов банков остаются
Веб-фишинг[1] и Социальная инженерия.

Активно продолжает развиваться **DNS hijacking**, что позволяет атакующим проводить фишинговые атаки еще более эффективно.

Коротко напомним, в чем заключается суть этого метода:



Получение доступа к роутеру одним из двух способов:

Вариант 1

Перебор паролей — провайдеры, которые предоставляют роутеры в аренду, мало заботятся об их безопасной настройке, пароли ставят по умолчанию, а интерфейсы управления доступны через интернет.

Вариант 2

Эксплуатация известной уязвимости — обновление домашних роутеров непростая задача. Цикл поддержки таких устройств очень короткий, обновления часто оказываются недоступны, но даже в случаях когда они есть, очень малый процент пользователей занимается обновлением.

Изменение настройки DNS-серверов, которые получают устройства, подключенные к Wi-Fi сети этого роутера.

Подмена IP-адреса — при запросе определенных доменных имен вредоносные DNS-серверы возвращают мошеннические IP-адреса. Таким образом, когда пользователь вводит в строке браузера название сайта (например, банка), то вместо IP-адреса банка ему возвращается IP-адрес мошенника.

Чтобы работать с собранными благодаря фишингу данными жертв, атакующие обычно используют один из этих методов:

Отправка данных по электронной почте (по-прежнему самый популярный метод)

Сохранение данных в локальный текстовый файл, который мошенник может забирать с удаленного сервера разными способами

Загрузка логов на удаленный FTP-сервер (встречается редко)

Мошенники, занимающиеся фишингом против клиентов банков, начали более активно использовать панели управления веб-инжектами для управления фишинговыми страницами. Это позволяет им проводить атаки в реальном времени, получать от жертв одноразовые пароли и выполнять дополнительные действия, необходимые для подтверждения финансовых операций. Одной из наиболее популярных панелей стала U-Admin.

Социальная инженерия

без использования вредоносных программ или фишинговых сайтов остается одной из самых массовых и популярных схем, которая выглядит так:

1. Злоумышленник звонит от имени банка и сообщает клиенту, что зафиксирована попытка взлома личного кабинета или вывода средств.
2. Службе безопасности банка якобы требуется помощь, чтобы решить техническую проблему для противодействия мошенничеству.
3. Жертву просят срочно установить программу для удаленного управления смартфоном, чтобы обезопасить пользователя.
4. Получив инструмент управления приложениями от имени пользователя, мошенник заходит в приложение мобильного банкинга и выводит средства со счета.

В результате такого общения жертва сама сообщает всю необходимую информацию либо по указанию мошенника устанавливает программы удаленного доступа на ПК, и атакующий может сам выполнять необходимые операции. Новая схема заключается в том, что жертву просят установить средства удаленного управления на мобильное устройство.

Трояны для банкоматов

ROOT LEVEL RESOURCES

Появление новых угроз

Неименованный троян из Африки

Программа позволяет управлять банкоматом через pinpad: при вводе правильного PIN-кода напрямую взаимодействовать с диспенсером, а при использовании банковской карты с определенным номером забрать из банкомата все наличные деньги. Для обхода белых списков атакующие используют файл cmd.dll — аналог системного инструмента cmd.exe, реализованный разработчиками ReactOS.

HelloWorld

Программа предлагается к продаже на андеграундном форуме в следующих вариантах:

- Работающий по принципу "Cutlet Maker" исполняемый файл с кейгеном или без него;
- Образ IMG для записи на флеш-накопитель;
- Образ на CD-диск;
- Образ на дискету;
- Образ ISO для загрузки через PXE (в процессе разработки).

Троян работает на всех моделях Wincor/Diebold Nixdorf после 2001 года, у которых есть MXFS/CSCW DLL-файлы, а его стоимость составляет 2000 долларов за EXE-файл или образ, 3000 — за все варианты и 10000 — за исходные коды.

Эволюция существующих ATM-троянов

Cutlet Maker

Один из самых популярных ATM-троянов, который можно найти с 2017 года в разных версиях и использовать бесплатно. Cutlet успешно используется в Европе, России и СНГ.

ATMii

ATMii был обнаружен в 2017 году, и его особенностью является выбор определенных операционных систем. Троян мог работать на Windows 7 и Windows Vista при том, что наиболее популярной операционной системой в банкоматах на тот момент была Windows XP.

Alice

Этот троян известен с ноября 2016. По сравнению с бесплатной Cutlet Maker, Alice менее удобен в использовании, и за прошедший период он не был замечен в активных атаках.

WinPot (Cutlet V2)

В 2018 году на андеграундном форуме появилось объявление о его продаже. В комплекте с трояном идут его исходные коды, а цена варьируется от 500 до 1000 долларов. Как и его предшественник, троян используется для атак на банкоматы европейских стран.

Ploutus

Эту вредоносную программу начали продавать еще в 2016 году и долгое время она использовалась в Мексике, а в 2018 году и в США. Несмотря на свой возраст, Ploutus по-прежнему актуален, и с 2019 года на хакерских форумах снова начали появляться объявления о его продаже.

Трояны для ПК

ROOT LEVEL RESOURCES

Тренд на снижение активности банковских троянов для компьютеров только усугубился, а новые техники хищений перестали разрабатываться. Единственной страной, где они развиваются, остается Бразилия. Трояны для ПК в основном используются локально и разрабатываются местными хакерами.

Новые трояны для ПК

BANKER.THBAIAI

Троян был обнаружен в 2019 году.
Коротко о его наборе инструментов:

1. Первый модуль заражает компьютер, загружает и выполняет PowerShell скрипты, которые записывают файлы .LNK в папку «автозагрузка» и вынуждают компьютер перезагружаться. После перезагрузки пользователю показывается поддельный экран входа в систему для перехвата логина и пароля.
2. Запускается второй троян, который пытается открыть Microsoft Outlook и получить все сохраненные в нем адреса электронной почты. Если Outlook отсутствует на компьютере, то этот шаг будет пропущен.
3. Дополнительно на систему устанавливается "RADMIN".
4. Последним устанавливается бестелесный банковский троян, который нацелен на данные клиентов бразильских банков Banco Bradesco, Banco do Brasil и Sicredi.

CamuBot

CamuBot начали использовать для атак в 2018 году, и нестандартным стал в первую очередь подход к его распространению. Вместо массовой дистрибуции, злоумышленники звонили жертве от имени банка и просили перейти на фишинговый сайт банка для загрузки «модуля безопасности». Загруженный на систему пользователя, CamuBot открывал туннель для компьютера жертвы и поддельный сайт банка, где пользователю предлагалось ввести логин и пароль от своего аккаунта.

Трояны для Android

ROOT LEVEL RESOURCES

Хищение денег с помощью банковских Android-троянов основано на одной из трех основных техник:

Денежные переводы по SMS

(ограничение - услуга перевода денег по SMS предоставляется малым количеством банков, а лимиты на перевод очень низкие)

Поддельное банковское мобильное приложение

(ограничение - распространение поддельных банковских мобильных приложений требует больших инвестиций и усилий для их рекламы и продвижения)

Сбор данных карт, логинов и паролей путем демонстрации поддельных окон

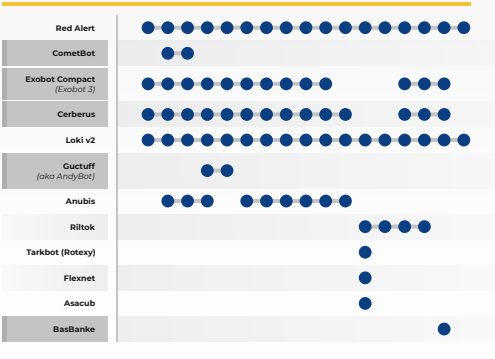
(самый эффективный способ)

Когда в обновленных версиях Android ужесточилась политика безопасности, и приложения потеряли возможность показывать произвольные окна, схема с демонстрацией окон перестала работать. Большинство разработчиков Android-троянов не смогли адаптироваться под обновления, и множество эффективных троянов под Android перестали работать. Некоторые проекты закрылись, разработчики ушли, развитие этих троянов заметно замедлилось, как и ущерб от их действий.

Изначально коды для подтверждения банковских операций банки отправляли через SMS, однако с распространением мобильных приложений SMS заменили PUSH-уведомления. Они дешевле для банка и к тому же безопаснее, поскольку все банковские трояны под Android уже умеют перехватывать SMS. Это стало еще одной причиной снижения активности этих троянов.

Обойти ограничения безопасности возможно с помощью Accessibility Service — службы специальных возможностей, призванной облегчить работу с устройствами людям с ограниченными возможностями. Получив разрешение на использование Accessibility Service, вредоносное приложение фактически получает возможность перекрывать окна других приложений, управлять устройством голосовыми командами, прослушивать, а не просматривать контент, управлять PUSH уведомлениями, тайно разблокировать устройство и выполнять произвольные действия, при этом держа экран отключенным.

Троян использует Accessibility Service для взаимодействия с элементами окон приложений и может выполнять следующие действия: сфокусироваться на объекте, кликнуть на объект, изменить содержимое текста объекта.



Новые трояны для ANDROID

Gustuff

Является продолжением развития трояна AndyBot и принадлежит тому же автору.

Однако самым важным отличием Gustuff от других Android-троянов является возможность осуществления автозалива следующим образом:

- Троян отправляет PUSH-уведомление пользователю с иконкой банковского приложения
- Пользователь нажимает на PUSH-уведомление
- Открывается банковское приложение
- Пользователь авторизуется в приложении
- По команде сервера Gustuff осуществляет автозалив

Стоимость аренды составляет 800 долларов в месяц, при этом автор заботится о собственной безопасности и при продаже сообщает, что бот не работает в России, СНГ и США.

Exobot Compact

Является третьей версией хорошо известного и зарекомендовавшего себя трояна Exobot. В мае 2018 года исходные коды Exobot второй версии были выложены в открытый доступ, и новая версия была полностью переписана и оптимизирована. Exobot Compact может работать на современных версиях Android вплоть до Android 9. Аналогично случаю с Gustuff автор запрещает работать в России, СНГ и США, но при этом поддельные страницы под американские банки у него есть. Стоимость аренды составляет 1500 долларов в месяц.

Cerberus

По возможностям он напоминает Gustuff и тоже умеет работать с PUSH-уведомлениями от банков. Однако в трояне Cerberus реализованы следующие методы самозащиты:

1. Выключение Google Play Protect и отключение по истечении времени, установленного в панели администратора;

2. Блокировка удаления бота, блокировка отключения прав администратора, блокировка отключения Accessibility Service;

3. Определение запуска в песочнице благодаря анализу акселерометра.

Стоимость аренды составляет 2000 долларов в месяц, и по аналогии с Gustuff автор Cerberus также запрещает использовать троян на территории России и СНГ.

CometBot

Этот троян сильно уступает по возможностям, однако тоже поддерживает работу на последних версиях Android. Предложение включает готовые веб-фейки только под немецкие и один испанский банк с возможностью простого расширения для поддержки банков других регионов. Аренда CometBot стоит 850 долларов в месяц.

BasBanke

Новый Android троян, нацеленный на пользователей Бразильских банков. Функциональные возможности BasBanke базовые, однако его владельцы сумели разместить его в Google Play, в результате чего он был загружен более 10 000 раз. Троян обладает функциями кейлогера, может делать запись с экрана и перехватывать SMS.

Однако, злоумышленник не сможет достичь своей цели, если атака будет вовремя выявлена и остановлена, а это возможно на любом ее этапе, если принимаются соответствующие меры защиты.

1 – Один из самых старых и простых видов мошенничества, который постепенно заменяет собой сложные атаки с использованием дорогостоящих троянов или инструментов для взлома.

2 – по-прежнему продолжает использовать веб-инжекты и применяет автозалив для автоматического хищения денег с банковских счетов.

3 – за последний год получил новый модуль для сбора паролей из установленных приложений, научился красть конфигурационные файлы с директорий SYSVOL на контроллере домена, начал использовать Mimikatz, проводить Fileless атаки и активно рассылать письма со скомпрометированных компьютеров. Новая версия трояна позволяет проводить целенаправленные атаки на крупные организации.

4 – Единственный активны троян в России, «родине» большинства банковских троянов, но его жертвами становятся в основном клиенты слабо защищенных банков.

5 – Владельцы бот-сети Buhtrap2 ранее использовали автозалив через российскую ERP систему 1С, однако такая схема позволяла детектировать зараженные устройства, поэтому хищения проводить не удавалось.