АТАКИ НА БАНКОМАТ НА ПРИМЕРЕ GREENDISPENSER: ОРГАНИЗАЦИЯ И ТЕХНОЛОГИИ

POSITIVE TECHNOLOGIES

Потери банков в некоторых странах в результате хакерских кампаний (2016)

Бангладеш	81 000 000 $
Россия	30 000 000 $
Япония	13 000 000 $
Украина	10 000 000 $
Тайвань	2 200 000 $
Вьетнам	1 100 000 $
Таиланд	350 000 $
Индия	194 000 $

ВВЕДЕНИЕ

На популярных банковских конференциях всегда особое внимание уделяется темам, связанным с обеспечением информационной безопасности, защитой банковской инфраструктуры, конфиденциальных данных и финансовых операций. В таких конференциях участвуют как представители банков, регуляторов, телеком-операторов, так и представители IT-компаний, занимающихся разработкой средств защиты.

С одной стороны, обмен опытом повышает общий уровень осведомленности, а совместное обсуждение проблем и инцидентов, с которыми столкнулись коллеги, позволяет вырабатывать общее направление в стратегии развития защиты на ближайшее будущее. С другой стороны, если вход на такие мероприятия свободен для всех желающих, то злоумышленники вполне могут посещать их для получения самых актуальных сведений о трендах развития информационной безопасности, средствах и мерах защиты, чтобы с учетом этих данных планировать будущие преступления.

«Гонка вооружений» тяжело дается банкам, что подтверждается как ростом нанесенного ущерба, так и тем, чтозлоумышленники придумывают новые способы краж, совершенствуют методы и инструменты, обходя введенные с запозданием меры защиты и удивляя изощренностью и масштабностью операций.

В данном отчете на основе материалов расследований инцидентов, которые проводила компания Positive Technologies, в нескольких банках Восточной Европы, анализируются технологии, организация и сложность проведения логической атаки на банкомат с применением вредоносного ПО на примере GreenDispenser.

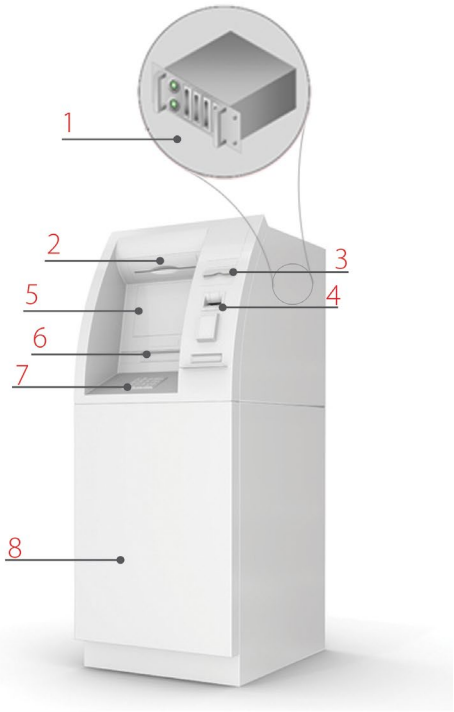
АТАКИ НА БАНКИ В 2016 ГОДУ

Вот основные методы, используемые грабителями для атаки на банки, не считая, конечно, вооруженного ограбления:

+ Атаки на инфраструктуру банка с целью получения доступа к системе денежных переводов[1]
+ Атаки на инфраструктуру банка с целью получения доступа к системе управления банкоматами[2,3]
+ Атаки на банкоматы, предполагающие непосредственное нахождение вблизи с банкоматом[4,5]
+ Атаки, основанные на доступе к системе ДБО на устройстве клиента банка[6,7,8]

Методы атак в этой сфере можно условно поделить на три группы:

+ Мошенничество[9]
+ Физические атаки[10,11]
+ Логические атаки[12]



1. Системный блок
2. Камера безопасности
3. Принтер чеков
4. Кардридер
5. Экран
6. Диспенсер
7. Pin-пад
8. Сейф

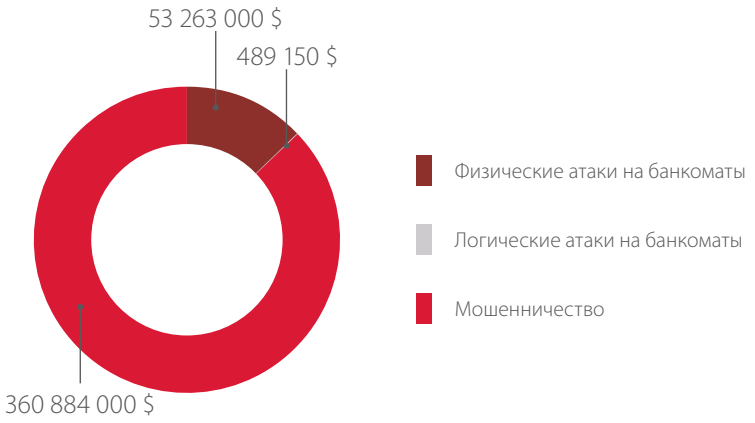
1 http://blog.group-ib.ru/lazarus
2 https://www.ptsecurity.com/upload/ptru/analytics/Cobalt-Snatch-rus.pdf
3 http://www.group-ib.ru/cobalt.html
4 https://www.gazeta.ru/social/2016/12/20/10440293.shtml
5 https://www.european-atm-security.eu/atm-explosive-attacks-surge-in-europe/
6 https://tools.ext.nokia.com/asset/201094
7 http://blog.group-ib.ru/cron
8 http://www.kaspersky.ru/about/news/virus/2017/finansovaya-kampaniya-twobee
9 http://www.securitylab.ru/news/476880.php
10 https://www.european-atm-security.eu/tag/atm-physical-attacks/
11 http://www.rbc.ru/finances/22/11/2016/5833f7289a79476da86aec0d
12 https://www.european-atm-security.eu/tag/atm-malware/

Самая известная схема мошенничества, связанная с банкоматами, — это кража данных банковских карт с помощью скиммера и создание на их основе дубликатов, с помощью которых злоумышленники затем снимают деньги со счетов клиентов банка. Скиммер — замаскированное под кардридер устройство, которое считывает данные с магнитной полосы или чипа[13] банковской карты в тот момент, когда пользователь вставляет карту в банкомат. Кроме того, существуют реализации скиммеров, которые могут считывать данные с EMV-чипа банковской карты дистанционно[14].

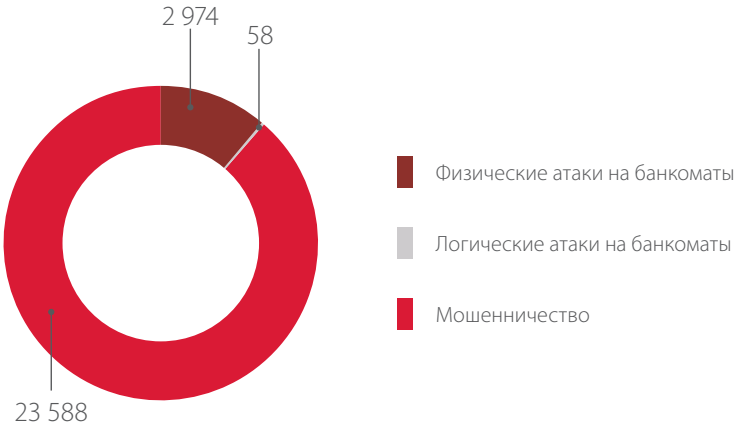
По данным European ATM Security Team[15], в 2016 году инциденты, связанные с мошенническими операциями, составили 89% от общего числа инцидентов, в которых атаки злоумышленников были направлены на банкоматы. При этом доля от ущерба, нанесенного в результате этих инцидентов, составила 87%.

Количество инцидентов, связанных с физическими атаками на банкоматы в Европе, в 2016 году выросло на 12% по сравнению с 2015 годом и составило 11% от общего числа инцидентов, связанных с банкоматами.

Следует отметить, что такое количество физических атак на банкоматы достигнуто в основном из-за роста инцидентов, связанных с подрывом банкоматов (на 47%). Этот метод также получил широкое распространение в России в 2016 году.



Общий ущерб от атак, связанных с банкоматами (Европа, 2016)



Количество инциндентов, связанных с банкоматами (Европа, 2016)

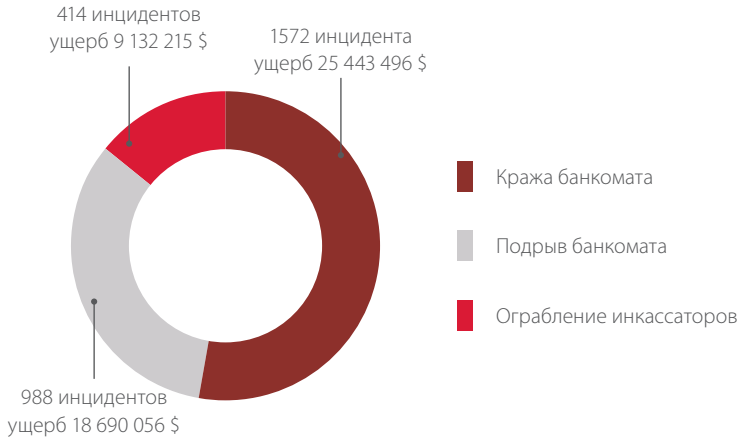
13 https://www.blackhat.com/us-16/briefings.html#hacking-next-gen-atms-from-capture-to-cashout
14 https://www.youtube.com/watch?v=6VaG1mwoukQ
15 https://www.european-atm-security.eu/atm-black-box-attacks-increase/

С 2009 году троян Skimer[16] положил начало логическим атакам на банкоматы, связанным с применением вредоносного ПО. С тех пор специалистами исследовательских лабораторий было выявлено несколько семейств троянов: Skimer, Ploutus [17], NeoPocket [18], Padpin [19](Tyupkin [20]), Suceful [21], GreenDispenser [22], Ripper [23], Alice [24].

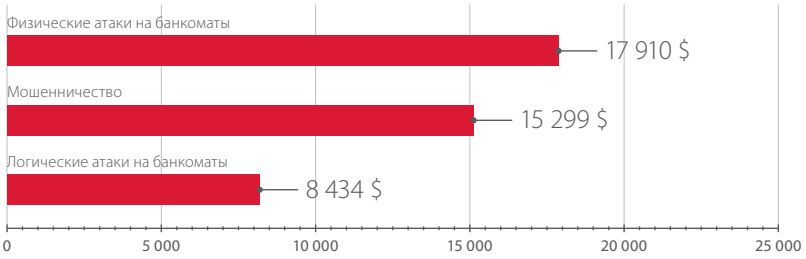
В 2016 году доля атак на банкоматы с применением вредоносного ПО в Европе в результате логических атак составила менее одного процента. Но несмотря на то, что количество логических атак на банкоматы несопоставимо по количеству с инцидентами, связанными с мошеннической деятельностью, подобные случаи всегда широко обсуждаются в СМИ и серьезно сказываются на репутации банка, защиту банкоматов которого удалось преодолеть преступникам.

В данном отчете приводятся результаты анализа ключевых особенностей трояна GreenDispenser, выявленных в ходе расследований в нескольких банках Восточной Европы, которые проводили эксперты Positive Technologies.

По нашей оценке, суммарный ущерб, нанесенный в ходе инцидентов с применением трояна GreenDispenser в 2015–2016 годах, составил порядка 180 тыс. долларов США. В сравнении с крупными хакерскими кампаниями этот ущерб выглядит несущественно, однако подобные методы начали применяться злоумышленниками относительно недавно, а на фоне планируемого внедрения банкоматов с повышенной защитой сейфа с денежными кассетами от взрывов логические атаки на банкоматы могут получить еще большее распространение. Данный тренд подтверждается ростом количества подобных инцидентов в Европе в 2016 году по сравнению с 2015 годом на 287%. В 2017 году эксперты Positive Technologies прогнозируют 30-процентный рост кибератак на банки в целом и на банкоматы в частности.



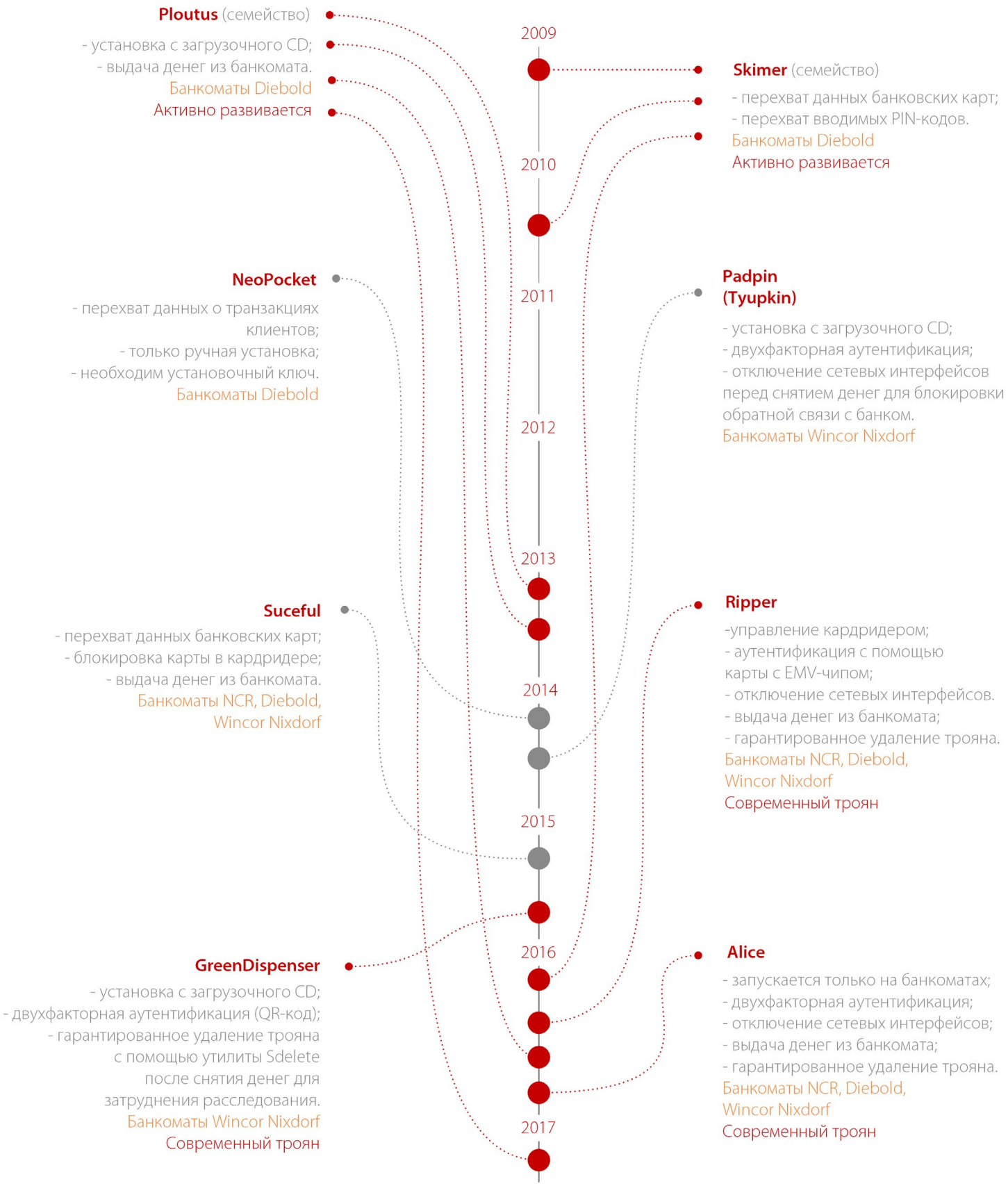
Общий ущерб от физических атак, связанных с банкоматами (Европа, 2016)



Средний ущерб от одной атаки на банкомат, (Европа, 2016)

16 https://vms.drweb.ru/virus/?i=426550
17 https://www.symantec.com/connect/blogs/criminals-hit-atm-jackpot
18 http://www.communicationstoday.co.in/images/reports/20170301-TrendLabs-2016-annual-security-roundup-report.pdf
19 https://www.symantec.com/security_response/writeup.jsp?docid=2014-051213-0525-99
20 https://securelist.com/blog/research/66988/tyupkin-manipulating-atm-machines-with-malware/
21 https://www.fireeye.com/blog/threat-research/2015/09/suceful_next_genera.html
22 https://www.proofpoint.com/us/threat-insight/post/Meet-GreenDispenser
23 https://www.fireeye.com/blog/threat-research/2016/08/ripper_atm_malwarea.html
24 http://blog.trendmicro.com/trendlabs-security-intelligence/alice-lightweight-compact-no-nonsense-atm-malware/

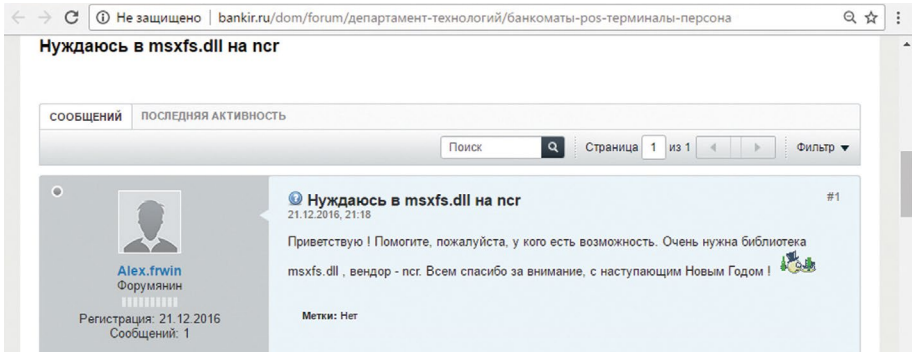
ХРОНОЛОГИЯ ПОЯВЛЕНИЯ ВПО ДЛЯ БАНКОМАТОВ



**Частота появления нового ВПО для банкоматов растет.
Готовы ли банки к надвигающейся угрозе?**

GREENDISPENSER. ОРГАНИЗАЦИЯ И ТЕХНОЛОГИИ АТАКИ

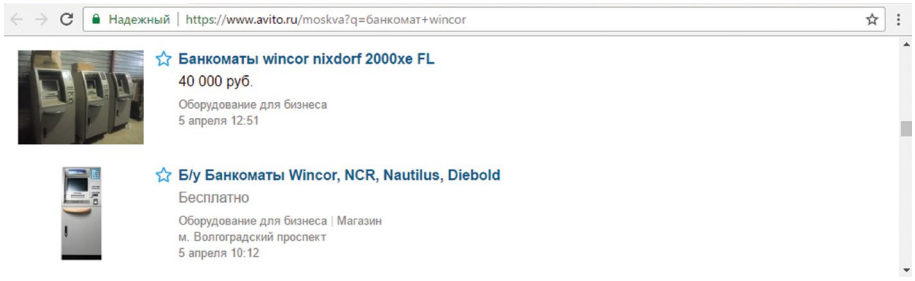
При разработке финансовых приложений на платформе Microsoft Windows используется специальный стандарт Extension for Financial Services (XFS) для совместимости программного обеспечения оборудования банкоматов с различными устройствами. GreenDispenser, как и аналоги Tyupkin и Padpin, использует XFS API из библиотеки msxfs.dll для работы с PIN-падом, диспенсером и другими устройствами банкомата.

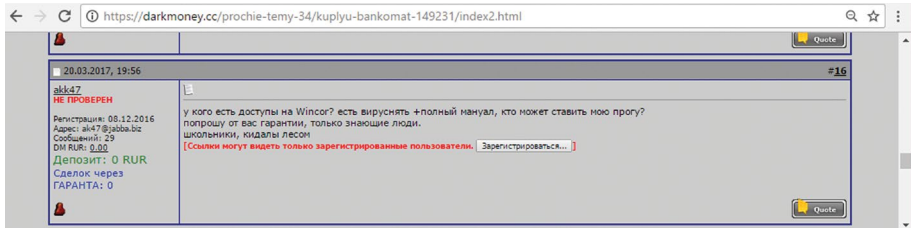


Поскольку XFS используется всеми крупными производителями банкоматов, то злоумышленники с помощью универсальных инструментов могут атаковать банкоматы вне зависимости от типа и производителя. Подтверждением этому являются обнаруженные во второй половине 2016 года трояны Ripper и Alice, задающие тренд на совместимость вредоносного ПО с банкоматами сразу нескольких производителей.

Библиотека msxfs.dll поставляется со специальной версией Microsoft Windows, поэтому для разработки и тестирования троянов преступник должен получить эту библиотеку в свое распоряжение. Для этого существуют различные варианты:

+ Купить старый (списанный) банкомат для изучения и тестирования
+ Подкупить сотрудника банка, который может не только скачать необходимую библиотеку, но и впоследствии установить троян на банкомат
+ Открыто попросить необходимые файлы на одном из интернет-форумов, посвященных банковской тематике





Впервые термин GreenDispenser возник после атак на банкоматы в Мексике в 2015 году. Далее кражи с его применением были зафиксированы в 2016 году в странах Восточной Европы. Вероятно, автор GreenDispenser продавал его преступникам, планирующим организовывать кражи без применения физического воздействия на банкомат и без удаленного взлома корпоративной инфраструктуры банка.

Автор GreenDispenser

Разрабатывает троян для продажи, обеспечивает локализацию и адаптацию трояна для применения в разных странах.

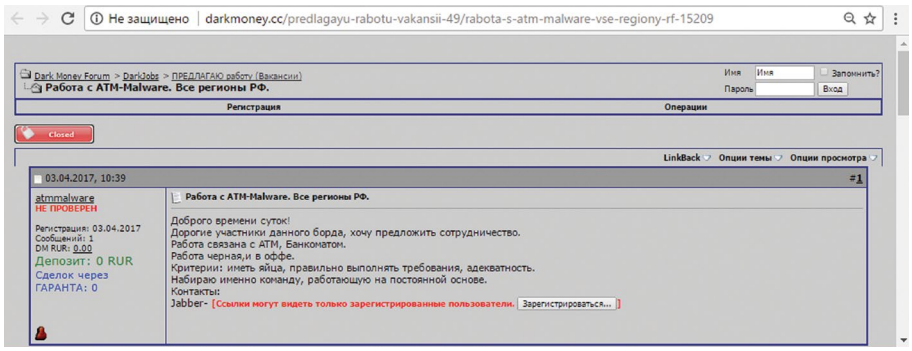
Для того чтобы троян был эффективен и зараженный банкомат не вызывал подозрений у прохожих и сотрудников банка при использовании в разных странах, автор должен был заниматься его локализацией по запросу злоумышленников. Таким образом можно утверждать, что разработка трояна автором велась с целью продажи. Из этого можно заключить, что разработчик GreenDispenser и организаторы краж вероятнее всего между собой не связаны.

Организатор кражи

Взаимодействует с автором трояна по вопросам покупки, локализации и настройки GreenDispenser, организует поиск других участников операции; контролирует и координирует участников в ходе операции.

С другой стороны, преступнику, купившему троян, для организации краж необходимо было решить две задачи:

+ Как установить троян на банкомат?
+ Как забрать после этого деньги из банкомата?



В ходе расследований инцидентов, связанных с заражением банкоматов трояном GreenDispenser в нескольких банках Восточной Европы, которые проводили эксперты Positive Technologies, было подтверждено, что злоумышленники получали доступ в сервисную зону банкомата для установки вредоносного ПО.

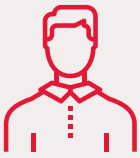
Установщик ВПО

Проникает в сервисную зону банкомата и устанавливает на него троян GreenDispenser.

Провести установку трояна на банкомат может человек, имеющий доступ к его сервисной зоне, например сотрудник банка, обслуживающий банкоматы, или человек, обладающий специальными инструментами и имеющий опыт вскрытия замков. Поэтому организатору нужно решить этот вопрос и провести инструктаж для этого человека по установке GreenDispenser на банкомат.

После того как необходимые банкоматы будут заражены, злоумышленники приступают к части плана, в которой им необходимо снять с банкомата деньги при помощи установленного на него трояна.

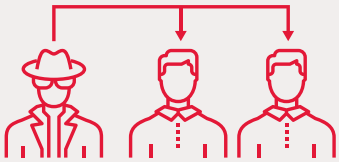
Несмотря на возможную техническую сложность взлома корпоративной сети, скорость проведения и масштабность операции, функциональность и скрытность используемого вредоносного обеспечения, для злоумышленника именно этап получения наличных денег сопряжен с максимальным риском быть разоблаченным.



Дроп

Передает QR-код, сгенерированный трояном, дроповоду; после ввода PIN2 снимает деньги с банкомата, отчитывается перед дроповодом.

Поэтому киберпреступники прибегают к помощи специальных людей — «дропов», типичные задачи которых заключаются в получении денег на свое имя, снятие денег с карты в банкомате или, как в случае с зараженными банкоматами, получение денег по команде из интерфейса управления трояном. В качестве оплаты дроп оставляет себе долю от обналиченных денег.



Дроповод

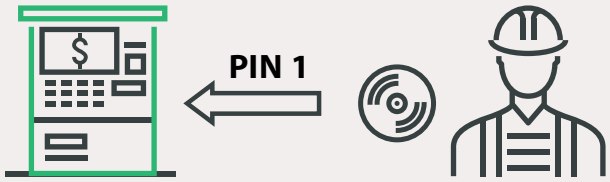
Вербует дропов и объясняет им порядок действий при краже обеспечивает передачу QR-кодов и кодов PIN2 между организатором и дропами в ходе опрации

Чем больше масштаб операции, тем больше злоумышленнику требуется дропов. Здесь на помощь приходят дроповоды — своеобразные бригадиры. Они занимаются вербовкой дропов, инструктажем и координацией их деятельности, а также обеспечивают коммуникацию между ними и организаторами операций. Так, при краже денег из банкомата с помощью GreenDispenser через дроповода организатор кражи мог передавать подтверждающий код дропу, находящемуся у банкомата.

GREENDISPENSER. СЦЕНАРИЙ КРАЖИ

Поскольку функционал GreenDispenser рассчитан только на выдачу наличных из денежных кассет, но не на кражу данных банковских карт, злоумышленники предусмотрели возможность того, что обычные держатели карт могут попытаться снять деньги с уже зараженного банкомата до прихода дропа и тем самым уменьшить количество денег, доступных для кражи. Для этого, после установки трояна в операционную систему, на экране банкомата отображается локализованная для страны размещения версия сообщения о том, что банкомат временно не работает. Для обычного прохожего банкомат будет выглядеть неработоспособным, и ему никогда не придет в голову подойти и снять с него наличные. Несмотря на предупреждающее сообщение, банкомат находится в рабочем состоянии, но GreenDispenser через XFS уже получил контроль над PIN-падом и ожидает ввода установленного авторами трояна статического PIN-кода.

Фаза 1. Инфицирование банкомата



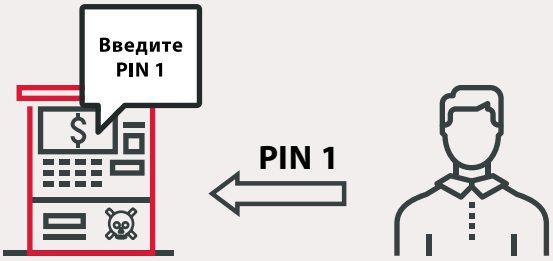
1.1 Получение доступа в сервисную зону и установка трояна

1.2 Визуальное подтверждение компрометации банкомата

После ввода первого корректного PIN-кода дропу необходимо подтвердить, что его дальнейшее управление трояном санкционировано организатором кражи. Для этого на экране банкомата появляется QR-код и предложение ввести второй PIN-код.

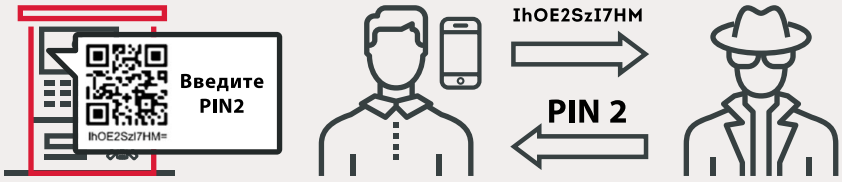
IhOE2SzI7HM=

Чтобы обеспечить уникальность второго PIN-кода, вредоносное ПО генерирует случайное значение, которого шифруется с помощью Microsoft CryptoAPI, а затем кодируется в Base64. Закодированный в Base64 результат отображается на экране в виде строки и QR-кода на тот случай, если дроп не имеет смартфона или считать QR-код камерой смартфона не представляется возможным. Кроме того, существует вероятность, что у злоумышленников могло быть специальное программное обеспечение для смартфона, позволяющее восстановить второй PIN-код, находясь непосредственно рядом с банкоматом.

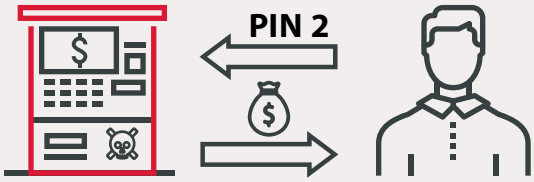


2.1 Первый этап аутентификации злоумышленника: вводит заранее полученный PIN1

Фаза 2.
Ограбление банкомата



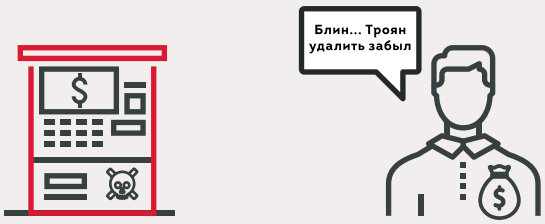
2.2 Второй этап аутентификации злоумышленника: сканирует QR-код с экрана банкомата, сообщает его дроповоду, получает PIN2



2.3 Снятие денег с банкомата: вводит PIN2, через интерфейс управления посылает команду диспенсеру на выдачу купюр

После прохождения аутентификации дроп переходит в интерфейс управления трояном, в котором становится доступна функция выдачи наличных из банкомата. Успешно сняв деньги, он следует инструкции оператора (координатора) и в том же интерфейсе выбирает пункт, отвечающий за удаление GreenDispenser из системы. Механизм удаления предусматривает добавление в планировщик Windows задания на создание и запуск пакетного файла del.bat, в котором будут записаны команды на удаление файла трояна с помощью утилиты SDelete из пакета Windows Sysinternals, переименованной в del.exe. Сегодня SDelete активно используется злоумышленниками как «анти-форензик», после применения которого восстановить удаленные файлы не представляется возможным, — что значительно усложняет криминалистическое исследование скомпрометированной системы и затрудняет проведение расследования.

```
:start
tasklist /FI “IMAGENAME eq <malware.exe>” 2>NUL | find /I /N “<malware.exe>”>NUL
if “%ERRORLEVEL%”==”0” goto start
“<path>\del.exe” / accepteula –p 3 –q “<path>\<malware.exe>”
del ”<path>\del.exe”
del ”<path>\<malware.exe>”
shutdown –t 0 –r –f
del “%~f0”
```



3.1 Дроп уходит, забыв удалить троян через интерфейс управления

Фаза 3.
Заметание следов

3.2 GreenDispenser запускает сценарий, гарантированно удаляющий его файлы из системы, и перезагружает систему

3.3 Прибывшие сотрудники службы безопасности обнаружат опустошенный нормально работающий банкомат

В любом сценарии необходимо предусматривать ситуации, когда что-то идет не по плану. Что может пойти не так при краже денег из банкомата? Учитывая, что заражением банкоматов занимаются одни люди, а снятием наличных — другие, может оказаться так, что после компрометации системы у злоумышленников в команде не будет достаточного количества дропов, или дроп не сможет найти подходящего времени, чтобы снять деньги. Так или иначе, поскольку банкомат не может длительное время стоять в состоянии out of service и не привлекать внимания, то GreenDispenser через неделю самостоятельно удаляет себя из системы. Если дроп уже подошел к банкомату и начал проходить процесс аутентификации, но его отвлекли, то он может запустить принудительное удаление трояна из системы как до ввода второго PIN-кода, так и после.

ПРОГНОЗЫ И ВЫВОДЫ

Результаты проведенного исследования, а также данные о тенденциях в разработке вредоносного ПО и росте количества инцидентов с его использованием, позволяют сделать выводы об актуальности логических атак на банкоматы. Все это в совокупности с зафиксированным в конце 2016 года ростом интереса участников специализированных сообществ к стандартам и системным библиотекам, которые используются в ПО банкоматов, может свидетельствовать о готовящейся или текущей разработке нового вредоносного ПО, которое будет использоваться как в атаках с непосредственным доступом к банкоматам, так и в целевых атаках на инфраструктуру банков с удаленным управлением банкоматами.

Схожее устройство банкоматов позволяет злоумышленникам использовать одно и то же вредоносное ПО в различных кампаниях по всему миру. Так, GreenDispenser, который использовали при атаках на банкоматы в Мексике, через некоторое время был обнаружен в странах Восточной Европы. Если в какой-то одной стране на сеть банкоматов была произведена атака со снятием наличных, это не значит, что такого не может случиться в любой другой. Более того, злоумышленникам удобнее переключаться на другие страны, так как пока в одном месте расследуют преступление и уже, возможно, разрабатывают способ противостояния данному способу атаки, их инструмент беспрепятственно отрабатывает в другом регионе, еще не готовом отразить такие атаки.

Наряду с повышением защиты сетевой инфраструктуры банка от внешних и внутренних нарушителей, рекомендуется уделить внимание непосредственно физической защите сервисной зоны банкоматов. Несмотря на то, что деньги хранятся в сейфе, который надежно защищает их от физического доступа, выдачей управляет специальный компьютер, установленный в сервисной зоне банкомата, доступ в которую получить значительно проще, например, воспользовавшись специальной отмычкой или ключом от другого банкомата. Злоумышленнику достаточно подключить к системному блоку микрокомпьютер со специальным ПО или загрузочный диск, чтобы опустошить банкомат за считанные минуты[25]. Поэтому важно не только следить за состоянием физической защиты банкоматов и осуществлять контроль над зонами, в которых банкоматы располагаются, но и проверять список лиц, имеющих доступ в сервисную зону банкоматов. Очевидно, что все коммуникационное оборудование должно располагаться внутри банкомата.

Отдельное внимание необходимо уделить защите компьютера, управляющего всем оборудованием банкомата. Во-первых, рекомендуется ввести запрет на подключение внешних устройств (клавиатура, мышь и т.п.) и загрузку со сторонних носителей информации (флеш-накопитель, компакт-диск и т. п.), которые может принести с собой злоумышленник, чтобы получить контроль над управлением банкоматом. При этом необходимо установить стойкий пароль для доступа в BIOS, чтобы нарушитель не смог внести изменения в конфигурацию загрузки системы банкомата. Во-вторых, следует установить и корректно настроить систему защиты, контролирующую целостность программного обеспечения, которая на основе белого списка ограничивает пул запускаемого ПО и контролирует его целостность. В-третьих, необходимо на регулярной основе организовать проведение анализа защищенности банкоматов, что позволит иметь актуальные сведения о состоянии безопасности банкоматов и свести вероятность взлома к минимуму.

Таким образом, реализация приведенных мер безопасности позволит повысить уровень защищенности и предотвратить подобные атаки в будущем.

25 http://www.banki.ru/news/daytheme/?id=8018520

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована ФСТЭК России и в системе добровольной сертификации «Газпромсерт». 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.

POSITIVE TECHNOLOGIES

pt@ptsecurity.com ptsecurity.ru facebook.com/PositiveTechnologies facebook.com/PHDays