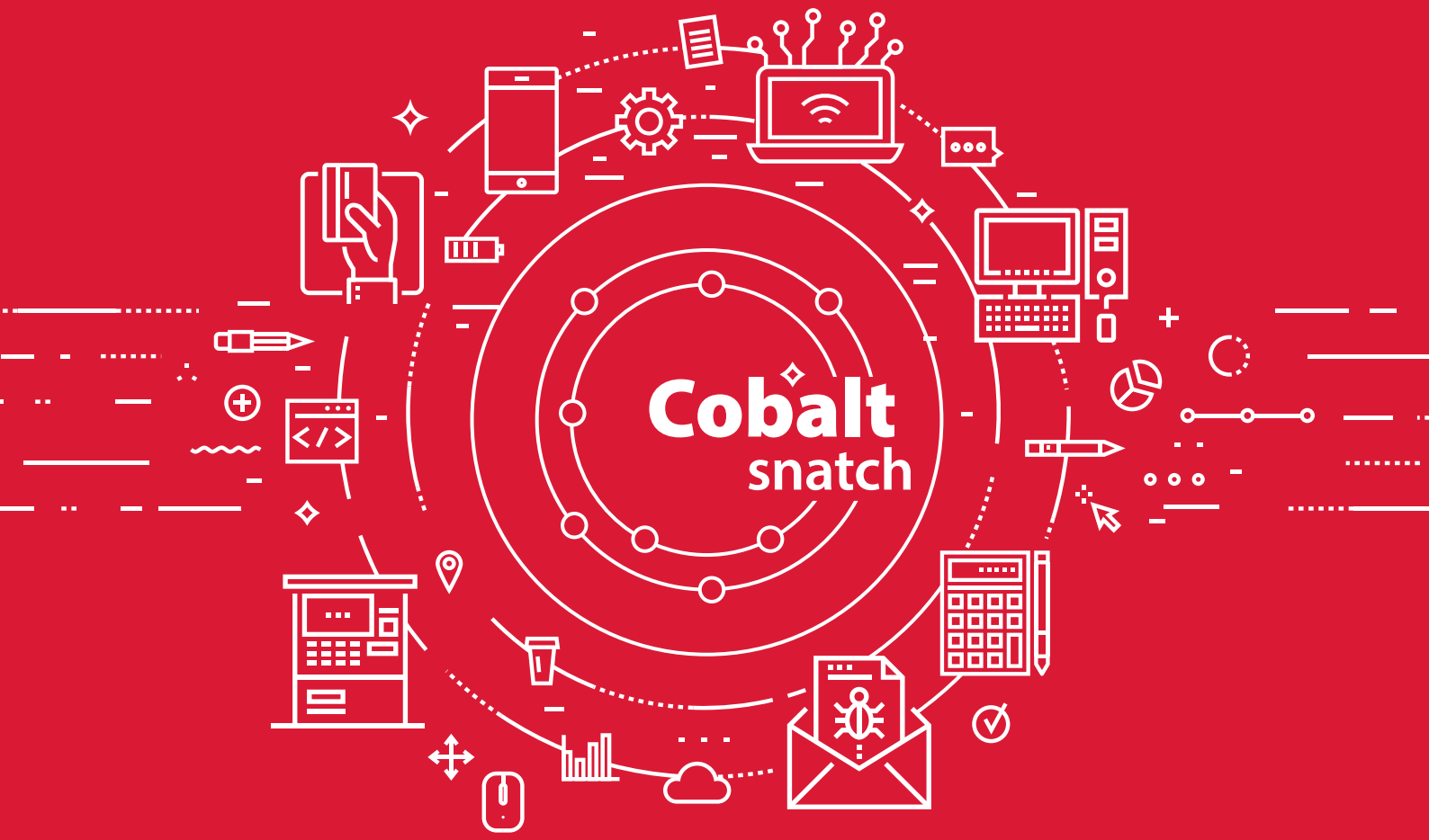
TLP: WHITE



Ноябрь

2016

POSITIVE TECHNOLOGIES

Содержание

Cobalt — новый тренд или старый знакомый?

Информация о деятельности группы, именуемой Cobalt, появилась совсем недавно: в ноябре 2016 года был выпущен отчет[1] компании Group-IB. В нем деятельность Cobalt связывают в первую очередь с известной ранее кампанией Buhtrap[2]. Именно эта группа, предположительно, стоит за хищением более 1,8 млрд рублей со счетов российских банков в 2015—2016 гг. Предполагается также, что часть участников группы перешли в Cobalt, либо вовсе костяк Buhtrap переключил свое внимание на банкоматы.

В это же время, осенью 2016 года, Positive Technologies проводила расследование компьютерного инцидента в одном из банков Восточной Европы , где были зафиксированы фишинговые рассылки и факты компрометации множества ресурсов внутренней сетевой инфраструктуры, а также сети банкоматов. Все следы явно указывали на нацеленную атаку, а выявленные артефакты — на деятельность организованной преступной группы, которая, по данным Positive Technologies, в период с августа по октябрь успешно осуществила ряд аналогичных атак на различные банки в России и Восточной Европы, а в ближайшем будущем может активизироваться и на Западе. Анализ данных подтвердил причастность группы Cobalt.

Данный отчет отражает наиболее важные результаты проведенного расследования. В нем показан пример реальной APT-атаки, которая потенциально может произойти в любом из банков. Для ее реализации группа использовала общедоступное ПО, а недостатки и уязвимости, которые были эксплуатированы, являются одними из наиболее распространенных в корпоративных системах большинства организаций, в том числе финансового сектора (см. исследование Positive Technologies www.ptsecurity.com/upload/ptru/analytics/Corporate-Vulnerability-2015-rus.pdf).

По мнению Group-IB, Buhtrap — первая преступная группа, начавшая использовать сетевого червя для поражения всей инфраструктуры банка. В качестве основного вектора проникновения в корпоративную сеть группа использовала фишинговые рассылки от имени Банка России или его представителей, при этом в ряде атак было зафиксировано распространение вредоносного программного обеспечения (ВПО) через эксплойты, в частности с использованием инфраструктуры группы Metel[3].

Преступники нацелены на банки России и СНГ

Кто следующая цель?

В 2016 году наблюдается тенденция использования преступниками общедоступных утилит, ПО для легитимных тестов на проникновение и стандартных функций операционных систем. Показательным примером можно считать нашумевшие в 2016 году атаки группы Carbanak[4], жертвами которой также стали банки в России и Восточной Европе. Эта группа использовала аналогичные инструменты, а также Metasploit. Предположительно, она же стоит за недавним взломом производителя PoS-терминалов Oracle MICROS[5] и атаками на зарубежные банки, о которых недавно сообщила компания Symantec[6].

Главными ошибками в противодействии киберпреступникам можно назвать недооценку их возможностей и распространенное мнение, что все эти атаки происходят где-то далеко и к нам никакого отношения не имеют. Подобная позиция может обернуться существенными финансовыми потерями.

Несмотря на обилие информации об используемых методах, применяемых инструментах, индикаторах компрометации, преступники продолжают атаковать и искать новые пути получения прибыли. Целевые атаки на банки и другие финансовые организации по всему миру все чаще освещаются в новостях. Общие финансовые потери от деятельности преступных групп исчисляются сотнями миллионов долларов. В 2017 году стоит ожидать как увеличения числа самих атак, так и роста объемов финансовых потерь банков от их реализации, поскольку преступники явно вошли во вкус, а банки просто не готовы им противостоять.

[1] http://www.group-ib.com/cobalt.html
[2] http://www.group-ib.ru/brochures/gib-buhtrap-report.pdf
[3] http://www.group-ib.ru/brochures/Group-IB-Corkow-Report-EN.pdf
[4] http://www.group-ib.com/files/Anunak_APT_against_financial_institutions.pdf
[5] https://krebsonsecurity.com/2016/08/data-breach-at-oracles-micros-point-of-sale-division
[6] https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks

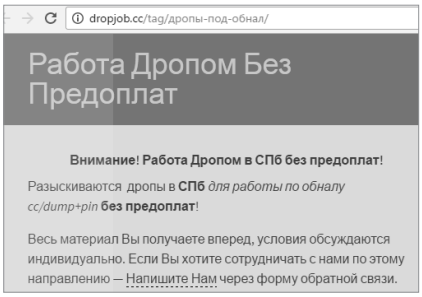
Взлом банкомата, или Почему он не нужен

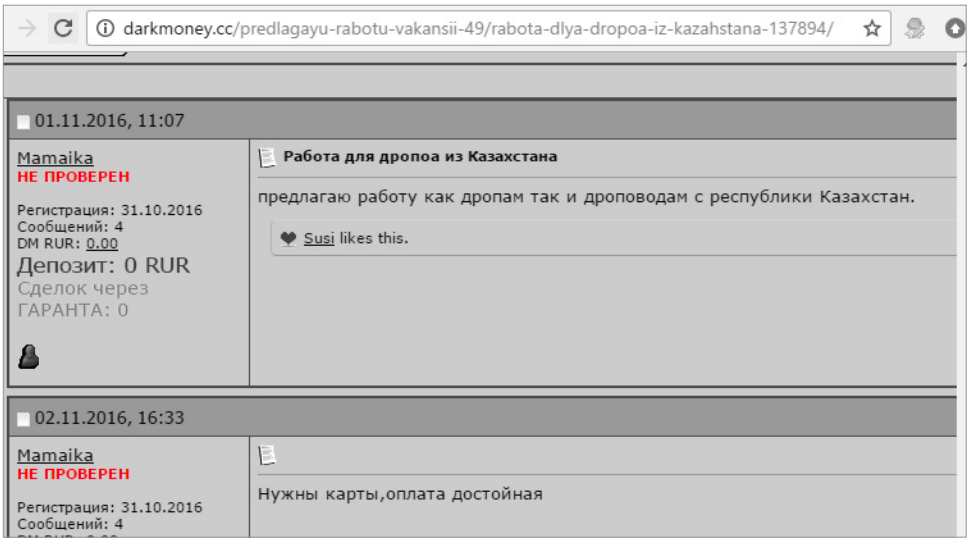
Эксперты Positive Technologies в начале октября 2016 года получили сообщение от одного из банков Восточной Европы о произошедшем инциденте ИБ, результатом которого стало хищение денег из банкоматов.

За одну ночь из 6 банкоматов банка были похищены денежные средства в размере, эквивалентном 2 213 056 российским рублям в местной валюте. Оперативное реагирование банка и органов внутренних дел позволило предотвратить более крупные потери. Теоретически, в случае более продолжительной атаки нарушители могли бы похитить более 10 млн в рублевом эквиваленте в течение нескольких дней, а размер хищений ограничивался бы лишь возможностями выдачи купюр в банкомате и количеством скомпрометированных устройств.

Чтобы получить наличные из банкоматов использовались подставные лица (дропы). Один из таких дропов, гражданин Молдавии, был задержан с поличным правоохранительными органами при выемке банкнот. Эти наемники привлекаются преступными группами для того, чтобы минимизировать риски раскрытия основного состава организаторов в случае, если дроп будет пойман. Наемники не знакомы с ядром группы и действуют исключительно под командой кураторов, отвечающих за сбор наличных и доставку денег организаторам атак.

Cobalt используют так называемые сервисы money mule для обналичивания денег. Подобные сервисы завлекают отчаявшихся людей легким заработком. В интернете можно найти множество таких сервисов. Вот, например, несколько скриншотов:





Расследование инцидента, проведенное командой экспертов Positive Technologies, показало, что получение денежных средств стало возможно благодаря компрометации локальной вычислительной сети и распространению вредоносного программного обеспечения на банкоматы со стороны внутренней инфраструктуры банка в течение августа-сентября 2016 года. На банкоматах использовалось специализированное ВПО, которое по команде злоумышленника выдавало денежные средства из банкомата дропу. При этом со стороны дропа никаких манипуляций в отношении банкомата не требовалось.

Cobalt Strike как инструмент атаки

В функции Cobalt Strike входят:

+ модуль для проведения фишинговых атак;
+ модуль для проведения атак через веб-приложения (drive-by);
+ модуль для закрепления на ресурсах и развития вектора атаки внутри сети Beacon;
+ скрытные методы коммуникации, включая туннелирование через DNS и Peer-To-Peer SMB.

Особенности Beacon:

+ разработан на языке PowerShell;
+ код исполняется только в оперативной памяти;
+ обладает широкими возможностями по удаленному управлению системами (загрузка и скачивание файлов, повышение привилегий, проксирование трафика, кейлоггер, сканер сети).

Антивирус обнаружил ВПО

Антивирусное ПО на серверах зафиксировало заражение. Оперативные действия службы информационной безопасности банка могли бы предотвратить инцидент. Однако сотрудники нередко отключают средства защиты на своих компьютерах, а журналы антивируса вовсе не проверяются.

Легко ли сменить тренд?

Атаки на клиентов банка сегодня отходят на второй план, уступая дорогу не менее эффективным, как оказалось, методам — атакам на сами банки, а точнее на их сетевую инфраструктуру. Злоумышленники осознали, что далеко не все финансовые организации достаточно инвестируют в свою безопасность, а некоторые инвестируют лишь для галочки, с целью соответствия требуемым стандартам. Более того, атаки на клиентов подразумевают ограничения в сумме хищений, ведь нарушители не смогут похитить больше, чем есть на счетах клиентов. В то же время получение контроля над ключевыми серверами и системами управления банкоматами позволяет нарушителям сорвать действительно серьезный куш.

Целевая атака с использованием методов социальной инженерии и фишинговых рассылок с ВПО стала настоящим трендом последних лет. Как правило, организации (будь то банк, промышленная корпорация, IT- и любая другая компания) уделяют особое внимание реализации непрерывных бизнес-процессов, а для защиты от атак закупают и внедряют различные дорогостоящие решения. Однако это с переменным успехом позволяет закрыть лишь часть брешей на периметре, а наиболее слабым звеном в организации защиты, как всегда, остается человек.

Атакующие группы постоянно модернизируют свои техники и выявляют все новые и новые уязвимости. Как принято считать, злоумышленник всегда опережает защищающуюся сторону как минимум на шаг, тем самым определяя направление развития индустрии безопасности.

При этом, как показывает опыт Positive Technologies, атакующие все чаще применяют вполне обычные и всем известные инструменты, к примеру ПО для проведения легитимных тестов на проникновение или встроенную функциональность ОС. Cobalt — очередное тому подтверждение.

Рассматриваемый в данном отчете пример атаки подтверждает этот тренд. Здесь преступники применили коммерческое ПО Cobalt Strike[7] для проведения тестов на проникновение, и в частности многофункциональный троян Beacon, входящий в его состав. Агент Beacon является основной полезной нагрузкой и представляет из себя ВПО класса RAT (Remote Access Trojan).

Для удаленного управления также применялось всем известное легитимное ПО Ammyy Admin, которое любой желающий может скачать с сайта производителя.

Также были использованы другие распространенные инструменты, к примеру:

+ Mimikatz
+ PsExec
+ SoftPerfect Network Scanner
+ TeamViewer

Для перемещения внутри инфраструктуры активно использовалась атака типа pass the hash, которая позволяет аутентифицироваться в ОС используя хеш-сумму пароля: знать сам пароль не требуется.

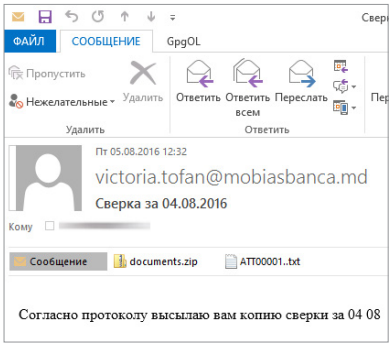
Неудивительно, что злоумышленники перешли на использование легального ПО, ведь современные утилиты для администрирования сетевой инфраструктуры и серверов обеспечивают столь широкую функциональность, что нет необходимости придумывать какие-то новые хитроумные инструменты (а выявить их использование при этом сложнее). Уровень же защищенности корпоративной инфраструктуры банков оставляет желать лучшего, этим рано или поздно должны были воспользоваться киберпреступники.

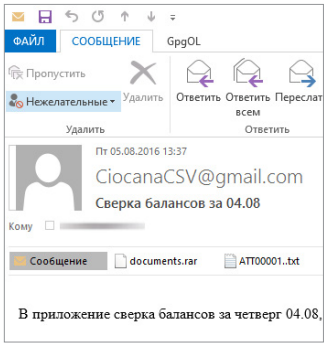
[7] https://cobaltstrike.com/

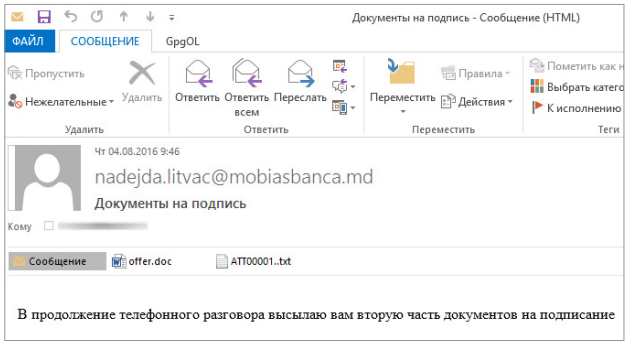
Хронология, или Как взломать банк за день

Начало атаки пришлось на первую неделю августа. Исходный вектор заражения инфраструктуры основывался на запуске файла documents.exe, RAR-архив с которым был получен по электронной почте одним из сотрудников. В день получения фишингового письма могла быть скомпрометирована вся инфраструктура банка, если бы он не пришелся на дату, когда этот сотрудник уходил в отпуск. Нарушителям пришлось ждать более двух недель, пока рабочая станция не была включена вновь. Все действия по развитию атаки и повышению привилегий в ОС злоумышленникам пришлось повторять заново.

На протяжении месяца на различные адреса банка велась целенаправленная рассылка электронных писем с вредоносным ПО от лица сотрудников различных банков. Анализ писем показал, что адреса отправителя были поддельные. Но сами по себе такие адреса действительно существуют, и большинство из них можно найти на официальных сайтах банков либо на портале curs.md/ru/lista_banci (агрегатор информации о молдавских банках).







Сама рассылка велась через почтовый сервер mail.peacedatamap.com, а в качестве обратного адреса указывались адреса на сервисе временной почты temp-mail.ru. В электронных письмах, полученных сотрудниками банка, использовались обратные адреса sesati@lackmail.ru и foyup@lackmail.ru.

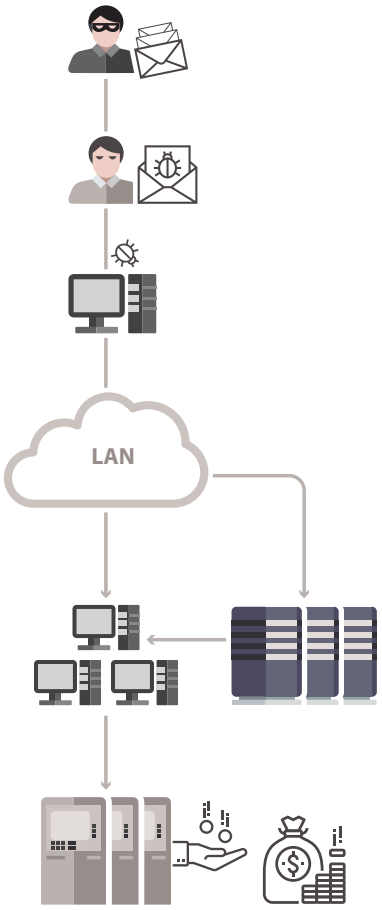
Необходимо отметить, что антивирусное ПО выявляло как исходные вредоносные вложения, так и активность злоумышленников после компрометации — задолго до того, как произошла кража средств. В числе прочего выявлялась подозрительная активность легитимного ПО Ammyy Admin. В некоторых случаях заражение было предотвращено антивирусом. Исходное заражение произошло из-за того, что антивирус на рабочей станции сотрудника, запустившего ВПО из фишингового письма, был отключен или использовал устаревшие антивирусные базы.

При анализе ВПО были получены следующие вердикты антивирусов:

ESET	SYMANTEC	KASPERSKY
Win32/Rozena	Trojan.Odinaff	RemoteAdmin.Win32.Ammyy
	Trojan.Odinaff!g1	Hacktool.Win32.Cobalt
	Trojan.Odinaff!gm	HEUR:Trojan.Win32.Generic
	Backdoor.Batel	
	Remacc.Ammyy	
	Backdoor.Gussdoor	

Темы писем фишинговых рассылок

«Документы на подпись»
«Сверка за 04.08»
«Сверка балансов за 04.08»
«Протокол вчерашнего заседания»
«Требования к сотрудникам Информационная безопасность»



1 **Почтовые рассылки с ВПО**

Проникновение в ЛВС

Открытие письма из недоверенного источника и запуск приложенного файла

2 **Заражение рабочей станции**

Закрепление на рабочей станции

Избыточные привилегии пользователя

3 **Исследование сети и развитие атаки**

Сканирование локальной сети

В сети не обеспечена эффективная сегментация

4 **Подготовка к краже**

Компрометация ключевых ресурсов

Выявление компьютеров сотрудников, ответственных за работу банкоматов

5 **Заражение банкоматов**

Кража денег из банкоматов

Дропы забирают купюры без каких-либо манипуляций с банкоматом

Банки были предупреждены

По фактам аналогичных атак в 2016 году ФинЦЕРТ выпускал ряд бюллетеней (ATM-OTH-ML-JACKPOTTING-20160921-01, ATM-OTH-ML-JACKPOTTING-20161014-02 и BK-20160906-001), которые обращали внимание финансовых организаций на существующую опасность стать очередной целью злоумышленников и давали достаточно сведений для реализации превентивных мер защиты (к примеру, поиска перечисленных индикаторов компрометации в сетевой инфраструктуре банка).

Расследование показало, что запуск файла из фишинговых писем в разное время осуществили несколько сотрудников, что говорит о низком уровне осведомленности работников банка в вопросах информационной безопасности.

Для усложнения выявления активности используемого ПО злоумышленники применяли различные тактики:

+ использование легитимного ПО и встроенных в ОС функций;
+ исполнение кода ВПО только в оперативной памяти;
+ использование протокола HTTPS для управления;
+ использование легитимного сервиса sendspace.com для обмена файлами с целью загрузки исходного ВПО;
+ удаление файлов, в том числе с использованием утилиты SDelete, для гарантированного уничтожения данных;
+ работа преимущественно в ночное время.

После закрепления в инфраструктуре Cobalt действовала без спешки, возобновив активность лишь в последних числах августа. Именно на это время пришлись основные действия по распространению атаки внутри сети. Были скомпрометированы рабочие станции ключевых сотрудников, критически важные серверы, в том числе терминальный сервер и контроллер домена. Кроме того, злоумышленники получили пароли практически всех пользователей компании, включая учетные записи администраторов, что позволило беспрепятственно перемещаться внутри сети.

Преступники тоже ошибаются

Ошибка в ВПО не позволила злоумышленникам похитить деньги из банкоматов NCR, несмотря на многократные попытки устранения проблемы во время атаки

Адреса серверов C2:

23.249.164.26
149.56.115.70
142.91.104.135
173.254.204.67
23.152.0.210
185.82.202.232

Для поиска и загрузки различных утилит (например, Mimikatz), злоумышленники использовали легитимные ресурсы, в частности распространенные поисковые системы, прямо со скомпрометированных узлов. Выбирались сайты из результатов поиска (к примеру, сайт github.com), откуда ПО загружалось на рабочие станции и серверы. Для загрузки же файлов ВПО применялся общедоступный ресурс для обмена файлами sendspace.com. Злоумышленники сделали ставку на легитимные сервисы с целью сокрытия своих действий.

Важно отметить, что для использования Mimikatz с целью получения учетных данных пользователей ОС необходимо обладать привилегиями локального администратора. Ключевыми факторами, которые способствовали быстрому развитию вектора атаки на другие ресурсы ЛВС, стали отсутствие сегментации сети и избыточные привилегии учетной записи (атакованный пользователь являлся локальным администратором на всех рабочих станциях в локальной сети). Это позволило злоумышленникам легко развивать атаку, ведь им не пришлось использовать дополнительные эксплойты для повышения привилегий, а также искать пути проникновения в сегмент управления.

Другой пик активности выявлен уже в начале сентября, когда нарушители активно атаковали ресурсы ЛВС с целью выявления рабочих станций сотрудников, ответственных за работу банкоматов и использование платежных карт. По сути эти атаки заключались в удаленном подключении к рабочим станциям, запуске Mimikatz для сбора учетных данных, исследовании файловой системы и установленного ПО, дальнейшем переходе на другие рабочие станции. После компрометации искомых узлов атакующие собрали необходимую информацию и подготовились непосредственно к краже денег.

Анализ журналов системы защиты подтвердил перемещения в сети со скомпрометированных компьютеров, в том числе подтвердились факты подключений к банкоматам с помощью RAdmin. В инфраструктуре атакованного банка это ПО активно используется администраторами для удаленного управления, среди прочего, и банкоматами. Поэтому подобная активность не вызвала подозрений.

Cobalt действовали практически не таясь, полагаясь на то, что их деятельность не будет замечена. Но они не стали торопиться и обналичивать деньги сразу. Определенное время они изучали банковские процессы и ждали момента, когда в банкоматах окажется максимально возможная сумма.

Только лишь в первых числах октября злоумышленники загрузили ВПО на банкоматы и осуществили кражу денежных средств. Действовали они ночью, чтобы не привлекать внимание. Оператор отправлял команду на банкоматы, а дропы в условленный момент подходили к устройству и просто забирали все деньги.

Примечательно, что из-за ошибки в ВПО, нарушителям не удалось похитить средства из банкоматов, поставляемых компанией NCR: действия ВПО приводили к ошибкам в самом ПО банкомата. Во время атаки были зафиксированы тщетные попытки злоумышленников разобраться в проблеме: в течение двух часов они перезагружали ВПО и банкоматы, но исправить ситуацию им так и не удалось. Эта случайность помогла банку избежать более крупных потерь.

По итогам расследования инцидента эксперты Positive Technologies собрали множество хостовых и сетевых индикаторов компрометации, которые были направлены в ФинЦЕРТ [8] Банка России с целью распространения данной информации среди финансовых организаций и предотвращения подобных атак в будущем.

[8] https://www.cbr.ru/credit/Gubzi_docs/main.asp?Prtid=fincert

В каждой шутке есть доля шутки

В процессе расследования эксперты Positive Technologies обнаружили артефакт: адрес электронной почты, который использовался для загрузки ПО Ammyy Admin, содержал нецензурные выражения в отношении «Лаборатории Касперского».

```
2016-09-**T17:22:35.489000+06:00,Page Visited,WEBHIST,Firefox History,http://www.
ammyy.com/AA_v3.exe?em=huy%40kasperskyc.com (AA_v3.exe) [count: 0] Host: www.ammyy.
com visited from: http://www.ammyy.com/ru/ (www.ammyy.com) (URL not typed directly)
Transition: DOWNLOAD,sqlite/firefox_history
```

Другими словами, Cobalt были готовы к противостоянию с исследователями «Лаборатории Касперского», ожидая, что именно они будут привлекаться к расследованию инцидента. Но преступники не могли предположить, что их деятельность раскроет команда Positive Technologies.

ВПО, взгляд изнутри

Эксперты Positive Technologies провели анализ обнаруженных образцов ВПО. Вот краткое описание основных его модулей:

winapma.exe	Stager-загрузчик агента Beacon. Загружает с 173.254.204.67:443/eHHr, указывая user-agent "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0; Avant Browser)"
atm.exe	Stager-загрузчик агента Beacon. Загружает с 142.91.104.135:443/svVv, указывая user-agent "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1)"
crss.exe	Загрузка библиотеки crss.dll Запускает функцию run_shell из библиотеки crss.dll
crss.dll	Stager-загрузчик агента Beacon Загружает с 173.254.204.67:443/eHHr, указывая user-agent "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0; Avant Browser)"
artifact.exe	Stager-загрузчик агента Beacon Загружает с 173.254.204.67:443, указывая user-agent "'Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; NP08; MAAU; NP08)"
documents.exe	Stager-загрузчик агента Beacon Загружает с 23.152.0.210:443/GizS, указывая user-agent "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)"
tkg.exe	Stager-загрузчик агента Beacon Загружает с 185.82.202.232:443/xRdM, указывая user-agent "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1)"
prikaz_08.08.2016.exe	Stager-загрузчик агента Beacon Загружает с 23.152.0.210:443/GizS, указывая user-agent "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)"

offer.doc	RTF-документ с эксплойтом, выполняющий stager-загрузчик агента Beacon Эксплуатирует уязвимость в Word CVE-2015-1641, внутри содержит другой экплойт для Adobe Flash CVE-2016-4117. В результате исполнения эксплойтов загружает с 23.152.0.210:443/GizS агент Beacon, указывая user-agent "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)"
jusched.exe	Stager-загрузчик агента Beacon. Загружает с 149.56.115.70:443/dDBr, указывая user-agent "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0; Trident/5.0; BOIE9;ENUS)"
CC323EA62B71E6 216A9ED830323B 18C8FAA03CB8.out	Восстановленный из карантина файл. SMB Beacon Ожидает получения команд через именованный канал \\.\pipe\status_8443
netscan.exe	SoftPerfect Network Scanner

Портрет типичного Cobalt

Письма, с помощью которых велась рассылка, были написаны на русском языке. Это означает, что, по меньшей мере, один из злоумышленников является русскоязычным. Группа хорошо разбирается в банковской специфике и обладает значительными ресурсами для поддержки своей деятельности.

Существуют и другой фактор, подтверждающий, что в группу Cobalt входят русскоговорящие злоумышленники: это ряд аналогичных инцидентов на территории России и Восточной Европы. Такого рода атаки невозможно совершить без знания внутренних процессов банка, что требует понимания русского языка.

Особенности атакующей группы	+ Использование сервисов **money mule** для обналичивания средств + Обеспеченность ресурсами для поддержания своей деятельности + Особый фокус на банках России и Восточной Европы
Особенности технического обеспечения	+ Использование ПО, предназначенного для проведения легитимных тестов на проникновение, например **Cobalt Strike** + Использование легитимного ПО для удаленного администрирования Ammyy Admin + Использование бесплатного и общедоступного ПО для сканирования сети SoftPerfect Network scanner + Использование **Mimikatz** + Использование встроенных функций ОС для перемещения внутри сети — **PowerShell**, **PsExec**, Runas
Методы хищения средств	+ **Обналичивание через банкоматы.** Используется специализированное или вредоносное ПО для манипуляции диспенсером

Подводя итог

Пример проведенного Positive Technologies расследования реальной атаки преступной группы Cobalt свидетельствует о том, что рассказываемые в публичных источниках истории про миллиардные убытки банков от действий хакеров вовсе не надуманы: это происходит здесь и сейчас. Банкам необходимо всерьез задуматься о превентивных мерах защиты, чтобы не стать очередной мишенью.

В рамках описанного в этом отчете инцидента ущерб оказался относительно небольшим (порядка 2,2 млн российских рублей), хотя далеко не для каждого банка из Восточной Европы эта сумма покажется невесомой. Избежать более серьезных потерь удалось лишь за счет оперативного реагирования как самого банка, подключившего к расследованию экспертов, так и сотрудников органов внутренних дел, сумевших задержать одного из дропов с поличным.

Инцидент показал, что хоть нарушители и старались скрыть свои действия (сделав ставку на использование легитимного ПО), антивирус выявил вредоносную активность на узлах. Таким образом, хищение денег можно было и вовсе предотвратить, если бы мониторинг существующих средств защиты был организован в банке на должном уровне.

Целевые атаки стали трендом последних лет. Причем целью атакующих являются не клиенты, а сами финансовые организации. Важно понимать, что злоумышленники все чаще используют не 0-day, а самые распространенные уязвимости, подтверждая тем самым, что APT-атаки не так сложны, как кажется на первый взгляд. Банкам необходимо обратить особое внимание на безопасность собственной инфраструктуры — и сделать это не только на бумаге. Кто знает, возможно, следующая атака придется на ваш банк?

О компании

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

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