ОСНОВНЫЕ ТИПЫ АТАК В КРЕДИТНО-ФИНАНСОВОЙ СФЕРЕ В 2017 ГОДУ

БАНК РОССИИ
ФИНЦЕРТ

Настоящий материал подготовлен Центром мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ Банка России) Главного управления безопасности и защиты информации Банка России.

СОДЕРЖАНИЕ

1. ЦЕЛЕВЫЕ АТАКИ НА ОРГАНИЗАЦИИ КРЕДИТНО-ФИНАНСОВОЙ СФЕРЫ 2

2. АТАКИ НА КЛИЕНТОВ КРЕДИТНЫХ ОРГАНИЗАЦИЙ 6

3. АТАКИ НА УСТРОЙСТВА САМООБСЛУЖИВАНИЯ 9

4. МАССОВЫЕ АТАКИ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММ-ВЫМОГАТЕЛЕЙ (ШИФРОВАЛЬЩИКОВ) 11

1. Целевые атаки на организации кредитно-финансовой сферы

Начиная с 2016 г. наблюдается увеличение количества целевых атак на организации кредитно-финансовой сферы. Основной тренд последних лет – использование для компрометации информационных систем и сетей инструментов, предназначенных для проведения тестирования на проникновение. Прежде всего таких как Metasploit Framework и основанных на Metasploit – Cobalt Strike, Armitage, Empire. Данные наборы инструментов, разработанные с использованием техник, затрудняющих их обнаружение в системе, предоставляют простой в использовании механизм удаленного управления зараженными компьютерами, а также включают утилиты, предназначенные для сбора информации о сети организации и хищения данных (паролей, документов и прочего).

Атаки рассматриваемого типа не требуют особых технических знаний атакующих. Большинство используемых ими компонентов уже соответствующим образом подготовлены производителями программного обеспечения.

На протяжении 2017 г. в качестве такого инструмента использовался прежде всего набор программ Cobalt Strike, разработанный американской компанией Strategic Cyber, LLC. Общие потери российских кредитных организаций от атак с использованием Cobalt Strike в 2017 г. превысили 1 млрд рублей. В то же время, анализируя способы совершения различных атак, специалисты ФинЦЕРТ обоснованно предполагают наличие иных преступных групп, использующих похожие инструменты.

Большинство атак с использованием Cobalt Strike, наблюдавшихся в 2016–2017 гг., реализовали одну из двух схем: конечной целью были либо банкоматы (рис. 1), либо процессинг платежных карт (рис. 2). Кроме того, отмечены три успешные атаки на принадлежащие кредитным организациям компьютерные средства участков платежной системы Банка России (АРМ КБР) и одна успешная атака на средства системы международных переводов SWIFT. Еще в одном случае при атаке на информационную систему небанковской кредитной организации был использован нестандартный способ получения денежных средств, потребовавший своеобразного творческого подхода и написания дополнительных программ.

Типовая схема целевой атаки на кредитную организацию выглядит следующим образом:

1. Производится массовая рассылка электронных писем, содержащих вредоносные вложения, на адреса организаций кредитно-финансовой сферы.
2. В случае запуска вредоносного вложения из письма на компьютере получателя, проявившего неосторожность, происходит скрытное внедрение программ, чаще всего – загрузчика.

3. После скачивания загрузчика на компьютере устанавливается компонент Beacon – основной инструмент из набора Cobalt Strike. Атакующий получает возможность удаленного доступа к зараженному компьютеру.
4. Атакующий проводит исследование доступных с зараженного компьютера сегментов сети и пытается установить доступ к контроллеру домена сети с целью последующего получения паролей администраторов. Для получения пароля могут быть использованы возможности специальных инструментов (Mimikatz и другие).
5. После получения доступа к контроллеру домена и администраторских паролей атакующий проводит поиск в сети интересующих серверов и компьютеров. Прежде всего ищется компьютер или сервер, с которого есть доступ в подсеть, где находятся банкоматы или иные сегменты сети, например в сегмент процессинга платежных карт.
6. На банкоматах устанавливается программное обеспечение, взаимодействующее, предположительно, через программный интерфейс XFS и обеспечивающее выдачу денежных средств по команде, подаваемой удаленно. После получения контроля над банкоматами к процессу привлекаются соучастники, занимающиеся получением денежных средств. Их задача – обеспечить присутствие около банкоматов в условленное время для получения денег. После успешной выдачи денежных средств программное обеспечение с банкоматов, как правило, удаляется.
7. В случае получения доступа к процессингу платежных карт привлекаются соучастники, занимающиеся оформлением на подставных лиц платежных карт атакованной организации. Данные карты консолидируются в руках лиц, занимающихся получением денежных средств. Их задача – обеспечить снятие денежных средств в банкоматах непосредственно после того, как балансы и лимиты карт будут повышены в системе процессинга. В процессе получения денег соучастниками оператор может при необходимости продолжать поднимать лимиты по снятию или балансы карт.
8. В случае получения доступа к компьютерным средствам сегмента платежной системы Банка России (АРМ КБР) или системы переводов SWIFT производятся платежи на заранее подготовленные счета, с которых денежные средства далее переводятся и обналичиваются по стандартным для компьютерной преступности схемам.

Рисунок 1
Атака, направленная на банкоматы

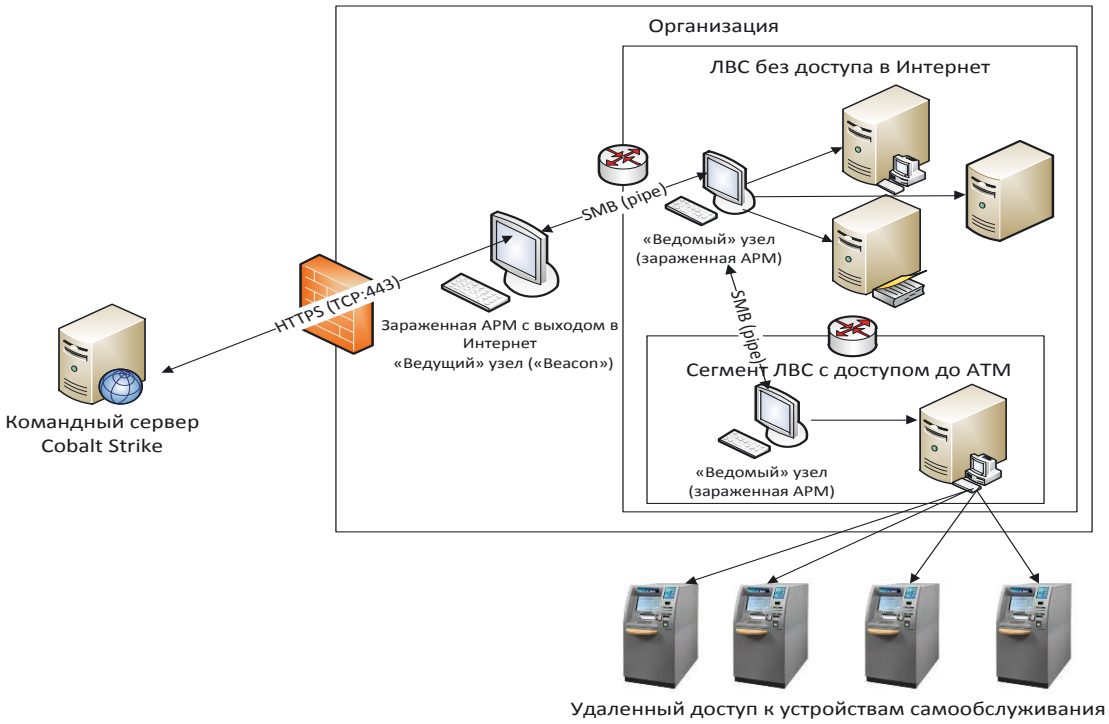
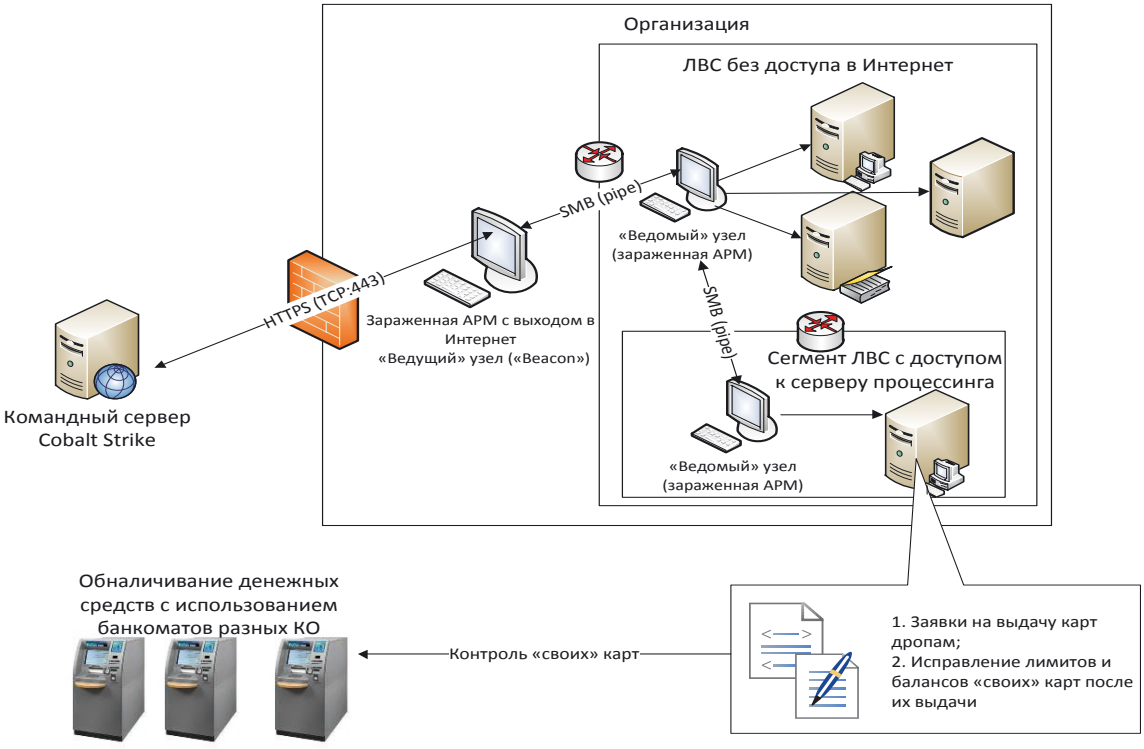


Рисунок 2
Атака, направленная на процессинг



Основными мерами противодействия атакам рассматриваемого типа являются:

1. Организационные меры, такие как повышение осведомленности сотрудников организации в области информационной безопасности, проведение тренировок сотрудников (например, рассылка тестовых «фишинговых» писем, анализ «успешных» проникновений, с обязательным подведением итогов тренировок).
2. Технические меры:
   2.1. Своевременное обновление антивирусных баз – большинство загрузчиков быстро выявляется и блокируется по сигнатурам.
   2.2. Установка на банкоматы программного обеспечения контроля целостности и предотвращения несанкционированного запуска сторонних программ (необходимо уточнять у вендора банкомата список совместимого программного обеспечения).
   2.3. Периодическая проверка на индикаторы компрометации, рассылаемые как ФинЦЕРТ, так и другими участниками рынка.
   2.4. Регулярное обновление сигнатур для систем IDS/IPS и подписок Threat Intelligence для своевременного детектирования подозрительного трафика.

В случае если заражение Cobalt Strike все же произошло (сработали индикаторы компрометации или есть признаки подготовки снятия денег), основной задачей является выявление и выведение из строя (закрытие доступа к сети Интернет) всех компонентов Beacon для пресечения коммуникаций с сервером управления.

Таким образом, основные меры сводятся к детектированию внешних сетевых соединений по известным адресам командных центров либо выявлению иных подозрительных сетевых соединений, обнаружению узлов, инициирующих указанные соединения, и очистке узлов от компонентов Cobalt Strike. Также необходимо определить «ведомые» Beacon-узлы, не имеющие прямого выхода в сеть Интернет, соединяющиеся с «ведущими» Beacon-узлами, имеющими такой выход. Узлы можно выявить, например, по аномальной активности SMB-трафика в локальной сети или отслеживанию факта создания новых системных служб.

Успех атаки в большинстве случаев обусловлен следующими факторами:

- Снижение бдительности сотрудников организаций, открывающих письма, пришедшие из недоверенных источников (в большинстве случаев).
- Повышение квалификации злоумышленников в части социальной инженерии и совершенствования способов доставки загрузчиков вредоносного программного обеспечения (ВПО).
- Появление в свободном доступе программного обеспечения, предназначенного для проведения тестирования на проникновение (как бесплатного, так и коммерческого программного обеспечения с легко преодолеваемой защитой «триального» периода использования).
- Недостаточная бдительность или оснащенность техническими средствами сотрудников служб ИТ и ИБ, в результате которой злоумышленники получают возможность длительное время совершать действия в скомпрометированной сети, избегая обнаружения.

2. Атаки на клиентов кредитных организаций

В 2016 г. и первой половине 2017 г. отмечено большое количество атак на юридических лиц – клиентов кредитных организаций, использующих бухгалтерские системы. Основная характерная особенность атак – автоматическая подмена платежных поручений на этапе их передачи из бухгалтерской системы в систему дистанционного банковского обслуживания. Несмотря на простую схему атак, суммарный ущерб от нее превысил 200 млн рублей. Атакам подверглись многие организации как в России, так и в странах СНГ.

Целью используемого в таких атаках вредоносного программного обеспечения, как правило, являлся файл экспорта-импорта, генерируемый бухгалтерской системой для передачи платежных поручений в систему ДБО, содержащий реквизиты получателя (получателей), суммы и иную необходимую для переводов информацию.

В общем виде атака выглядела следующим образом:

1. Клиент формировал в бухгалтерской программе платежные поручения и отправлял их на экспорт для системы ДБО. Бухгалтерская система формировала текстовый файл экспорта-импорта.
2. Вредоносная программа отслеживала появление (изменение) этого файла и производила подмену реквизитов получателя на заранее подготовленные злоумышленником. При этом название получателя оставалось неизменным, подменялись БИК кредитной организации, номер счета, ИНН получателя. Суммы переводов, как правило, не изменялись, хотя были отмечены и обратные примеры.
3. Клиент производил вход в систему ДБО и загружал подготовленные (и уже измененные) платежные поручения, которые, не глядя, благополучно направлял на обработку. В некоторых случаях от клиентов требовались подтверждения платежей по внеполосным каналам, и это делалось. В иных случаях подмена производилась после отправки корректных платежных поручений, но до их фактической передачи банку.

От момента заражения и до момента фактического хищения средств в среднем проходило от 7–10 дней до месяца. Заражение происходило, как правило, при посещении скомпрометированных специализированных бухгалтерских и финансовых сайтов в сети Интернет. На страницах таких сайтов в результате их взлома скрытно размещались какие-либо коды, вызывающие загрузку вредоносных программ (скрипты, обрабатывающиеся на стороне пользователя, поддельные рекламные баннеры и тому подобное). В других случаях распространение вредоносных программ данного типа происходило с использованием традиционных спам-рассылок по электронной почте.

В 2017 г. для атак рассматриваемого типа, по данным ФинЦЕРТ, чаще всего использовались вредоносные программы TwoBee, Fibbit (она же Ranbyus) и их клоны.

Существует несколько модификаций TwoBee, основное отличие которых – прописывание реквизитов получателей непосредственно в файлах ВПО или же их получение от командного сервера в процессе развития основной фазы атаки. Ранние версии получали реквизиты с командного сервера, поздние содержали счета непосредственно в исполняемых файлах. Также примечательно, что TwoBee использовала некоторые компоненты вредоносной программы Buhtrap, при помощи которой производились атаки на АРМ КБР в 2015–2016 годах.

TwoBee состоит из трех основных модулей (табл. 1).

Таблица 1
Функциональные модули TwoBee

Модуль (функционал)	Назначение
Удаленное управление	Проверка окружения, загрузка остальных компонентов ВПО, предоставление возможности скрытного удаленного управления зараженным компьютером
Взаимодействие	Взаимодействует с командным сервером и получает данные о дроп-счете (ранние версии, в поздних версиях реквизиты содержатся в указанном модуле), обеспечивает подмену реквизитов в файле экспорта-импорта
Уничтожение следов	Отвечает за сокрытие следов активности ВПО

Риски при атаках программой TwoBee и аналогами лежат на клиенте кредитной организации, но у самой кредитной организации возможно возникновение репутационных рисков, вызванных распространением негативных отзывов пострадавших о том, что денежные средства были успешно выведены, несоответствие реквизитов и счетов проигнорировано и так далее. В некоторых случаях отмечались даже информационные кампании против кредитных организаций.

Меры противодействия подобным атакам со стороны кредитной организации:

1. Настройка правила антифрода, учитывающего типовые платежи клиента. Предупреждение клиента в случаях, если совершаемые платежи вызывают срабатывание правил антифрода.

2. Оповещение всех клиентов о данном способе хищений, с указанием мер противодействия со стороны клиента.

Меры противодействия со стороны клиента:

- Использовать антивирусное программное обеспечение; поддерживать его базы в актуальном состоянии, не реже одного раза в неделю проводить полное сканирование системы.
- Выполнять все рекомендации по работе с вложениями, пришедшими из подозрительных источников, не открывать вложения – исполняемые файлы и не включать макросы в документах Microsoft Office, если нет уверенности в надежности отправителя.
- Постоянная визуальная проверка в системе ДБО всех реквизитов платежных поручений, подготовленных в бухгалтерской системе. Отказ в подтверждении вызывающих сомнение платежей до выяснения всех обстоятельств.

- Также может быть рекомендовано изменение наименования файлов выгрузки платежных поручений штатными средствами бухгалтерской системы. Большинство известных вредоносных программ рассматриваемого типа проверяют наличие требуемого файла по названию.

Следует отметить, что некоторые производители бухгалтерских систем, зная о серии атак, разработали специальные технологии (в частности, производитель наиболее распространенной в России системы 1С разработал технологию DirectBank), обеспечивающие прямой обмен данными между бухгалтерскими системами и системами ДБО, минуя промежуточные файлы импорта-экспорта. Это позволяет минимизировать риски подмены информации вредоносными программами, попадающими на компьютер клиента.

Также в последних версиях бухгалтерских программ применяется способ препятствования несанкционированному изменению файла экспорта-импорта. Впрочем, вредоносные программы также были обновлены для обхода защиты, что повышает значимость указанных выше мер.

3. Атаки на устройства самообслуживания

На протяжении всего 2017 г. отмечался повышенный интерес преступников к атакам на банкоматы с использованием физического подключения к внутренним устройствам банкомата и удаленного управления диспенсером. Такие атаки совершались группами, систематически «кочующими» по определенным регионам Российской Федерации.

В значительной степени распространение таких атак связано с продвижением модели «атака как сервис» на криминальных форумах. Организаторы преступной схемы продают технические устройства для подключения к банкоматам (как правило, переходники для устаревших моделей) (рис. 3) и предоставляют «поддержку» в течение определенного периода времени. Под «поддержкой» подразумевается готовность организатора к удаленному управлению банкоматом, подключенным через переходник к портативному компьютеру исполнителя.

Исполнитель самостоятельно или по указанию организатора выбирает подходящий банкомат, открывает его (или проделывает в корпусе отверстие), подключает к свободному системному разъему через переходник компьютер, на котором запущены программа для «проброса» портов и программа удаленного администрирования. Также к ноутбуку подключается модем для доступа к Интернету. В некоторых случаях отключаются второстепенные устройства либо повреждается шлейф SDC для подключения к нему компьютера исполнителя. Организатор удаленно взаимодействует с устройствами банкомата, запуская, как правило, модифицированную сервисную программу. Направляется команда на выдачу имеющихся купюр. Исполнитель получает денежные средства, находящиеся в банкомате, а организатор, заранее или впоследствии, – фиксированную оплату за использование сервиса и, вероятно, определенный процент от успешно похищенной суммы.

Рисунок 3
Переходник USB – SDC

Из прочих атак на устройства самообслуживания, зафиксированных в 2017 г., необходимо упомянуть вредоносное программное обеспечение CutletMaker, предназначенное для опустошения всех доступных в диспенсере кассет.

Образец CutletMaker впервые был исследован ФинЦЕРТ в конце апреля 2017 года. Изученный образец был обнаружен на жестком диске банкомата одного из крупнейших производителей. Впоследствии такое же ВПО было найдено на банкомате другого крупного производителя.

Предотвращение заражения данным ВПО достигается за счет применения кредитными организациями – владельцами банкоматов общих мер по безопасности, таких как создание белых списков приложений, запрет подключения дополнительных устройств к USB-портам, установка средств физической защиты. Обычно ВПО подобного типа неработоспособно при переводе диспенсера банкомата в защищенный режим работы, обеспечивающий шифрование передаваемых данных между диспенсером и другими компонентами банкомата, и на текущий момент хорошо детектируется антивирусными программами.

Возможно, именно из-за невысокой эффективности устаревшая версия ВПО CutletMaker была «выброшена» на рынок, в том числе на общедоступные сайты. По мнению ФинЦЕРТ, продажа такого ВПО на ресурсах, не относящихся к теневым, может означать его практически полную неработоспособность и попытку заработать на начинающих преступниках.

Также в феврале 2017 г. был зафиксирован единичный случай реализации атаки типа Transaction Reversal Fraud. Цель атаки связана с получением наличных денежных средств с одновременным воздействием на работу банкомата и процессингового центра, в результате чего отсутствует корректное завершение операции по выдаче наличных средств и баланс по карте не меняется (манипулирование карточным счетом). Кроме того, в 2017 г. на территории России были зафиксированы первые случаи установки в POS-терминалы так называемых «шиммеров» – устройств, предназначенных для получения информации с EMV-карт. Более подробно об этих и иных атаках на устройства самообслуживания можно прочитать в ежегодном отчете ФинЦЕРТ за 2017 год.

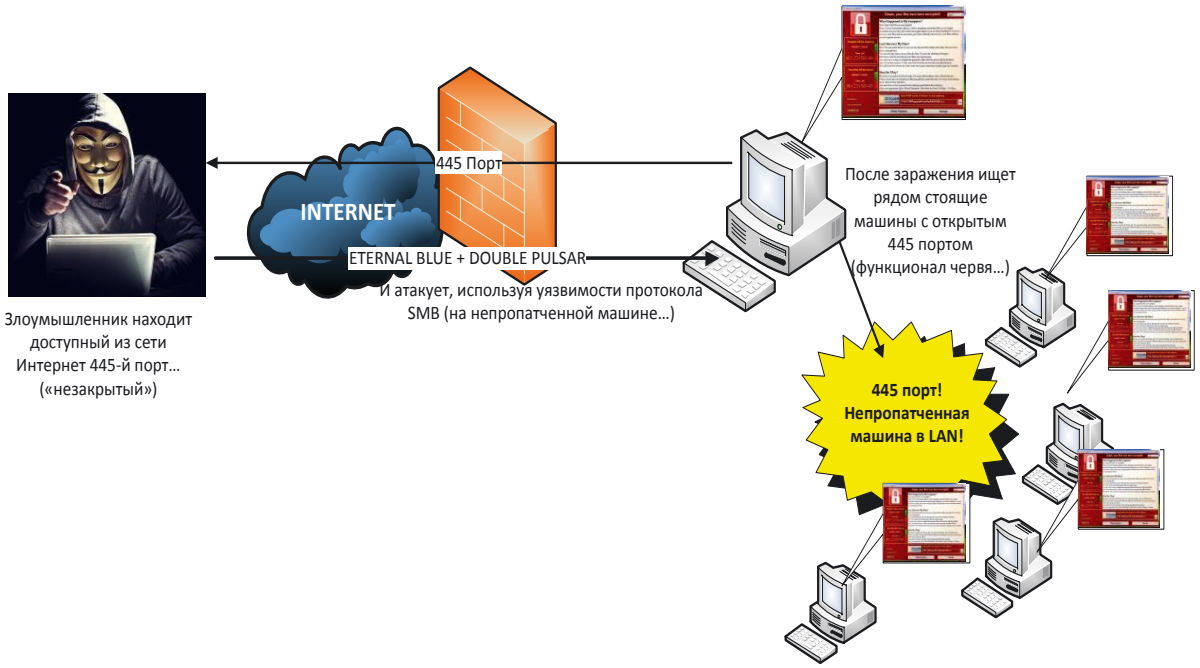
4. Массовые атаки с использованием программ-вымогателей (шифровальщиков)

В 2017 г. произошли две крупные эпидемии вирусов-шифровальщиков – WannaCry и NotPetya. Несмотря на то, что в мире в целом зафиксирован достаточно большой ущерб от них, для организаций кредитно-финансовой сферы России ущерб оказался незначительным. В ФинЦЕРТ поступили сведения о заражении WannaCry только семи устройств, принадлежащих кредитно-финансовым организациям, причем без ущерба. А от вируса NotPetya пострадала только одна кредитно-финансовая организация и опять же без ущерба.

Эти шифровальщики отличались от ранее встречавшихся наличием функций самораспространения с использованием уязвимости протокола SMB (CVE-2017-0147).

Условная схема заражения WannaCry приведена на рисунке 4. Следует отметить, что взаимодействие с командным сервером осуществляется через сеть TOR.

Рисунок 4
Схема заражения WannaCry



Основной мерой противодействия была установка патча от производителя, закрывающего данную уязвимость (бюллетень Microsoft MS17-010).

Шифровальщик NotPetya также позаимствовал некоторые особенности WannaCry, в частности использование возможности распространения по SMB. Однако он имел и новые функции, в основном за счет

использования переработанного инструмента Mimikatz. Исходный код NotPetya в значительной части совпадает с кодом шифровальщика Petya образца 2016 года.

Успех распространения NotPetya во многом определился следующими факторами:

- Отсутствие патча, закрывающего уязвимость CVE-2017-0147.
- Распространение ВПО с серверов украинской компании – разработчика программы M.E.Doc вместе с легальными обновлениями, что вызвало массовое заражение организаций Украины.
- Через VPN шифровальщик, предположительно, проник в организации других стран, которые имели свое представительство на Украине.

Необходимо отметить, что данные примеры наглядно показывают необходимость своевременного обновления критических компонентов операционных систем. Так, патч, устранявший указанную уязвимость, был доступен еще в марте, а атака произошла 12 мая. Вызывает удивление отношение специалистов, ответственных за настройку оборудования и контроль настроек, не обновлявших своевременно информационные системы в своей зоне ответственности.