Краткая сводка

Цифровая «прачечная» по отмыванию денег

Анализ виртуальных валют и их использования в киберпреступности

Радж Самани (Raj Samani), регион EMEA, McAfee
Франсуа Паже (François Paget), Мэтью Харт (Matthew Hart), McAfee® Labs

Недавние действия правоохранительных органов и судебные обвинения лишний раз подтверждают, что цифровые валюты являются основным средством отмывания денег преступниками. До закрытия служба виртуальной валюты Liberty Reserve была использована для отмывания 6 млрд долларов США. Это крупнейшая в истории операция по отмыванию денег.

Однако Liberty Reserve — это не единственная виртуальная валюта, используемая преступниками. Распространение таких служб только способствует развитию киберпреступности и других форм правонарушений в цифровой сфере. Кроме того, проблемы, связанные с такого рода валютами, выходят далеко за рамки их удобства для отмывания денежных средств — это и целенаправленные атаки на финансовые биржи, и специально разрабатываемые вредоносные программы, ориентированные на электронные кошельки.

Некоторые валюты, например, Bitcoin, позволяют создавать новые блоки для получения средств. Этот процесс называется «майнинг» (от англ. mining — добыча полезных ископаемых). Изначально пользователи использовали для майнинга свои компьютеры. Но в июне 2011 года появился генератор Bitcoin («майнер») на основе JavaScript, позволивший веб-сайтам с высокой посещаемостью задействовать в майнинге ресурсы компьютеров посетителей сайтов. Хотя некоторые сайты предупреждают посетителей о наличии таких скриптов, эти процессы вполне могут быть и полностью скрытыми, что, по сути, приравнивает их к вредоносным ботам. Один нечистоплотный сотрудник компании E-Sports Entertainment Association однажды установил такой майнер на 14 000 компьютеров с целью тайного накопления биткоинов.

Определение цифровых валют

Европейский центральный банк (ЕЦБ) обращает внимание на существенное отличие виртуальных валют от электронных денег. Электронные деньги — это эквивалент традиционной валюты, обращение которой контролируется; виртуальные валюты являются нерегулируемыми вымышленными валютами.

В отчете *Redefining Virtual Currency* (Новое определение виртуальной валюты), подготовленном компанией Yankee Group, объем рынка виртуальных валют по состоянию на 2012 год оценивается в 47,5 млрд долларов США; по прогнозам, к 2017 году эта сумма увеличится на 14 % и составит 55,4 млрд долларов США. В отчете высказано мнение, что такому заметному росту в значительной степени способствует распространение мобильных устройств, и это позволяет сделать вывод о том, что расширение рынка происходит далеко не за счет одного лишь криминалитета.

Виртуальные валюты привлекают клиентов рядом преимуществ, таких как надежность, мгновенность операций и анонимность. Даже когда возникли трудности с обеспечением конфиденциальности при работе с определенными валютами (особенно с Bitcoin), рынок тут же отреагировал, предоставив пользователям модули расширения для обеспечения еще большей анонимности. Реакция рынка — это важный показатель, так как независимо от действий правоохранительных органов, направленных против компаний, продвигающих виртуальные валюты, пользователи быстро находят новые платформы для отмывания своих денег. Простое закрытие наиболее популярной платформы не решит проблему.

Как видно на рисунках 1–4, многие незаконные службы принимают в качестве средства платежа только виртуальные валюты. Такая тенденция перехода только на виртуальные валюты, скорее всего, усилится, в частности, потому, что такие валюты имеют явные преимущества с точки зрения киберпреступников и предпринимателей.

Рис. 1. Виртуальные валюты иногда являются единственным средством расчетов при покупке и продаже таких товаров, как номера украденных кредитных карт, личные учетные данные для аутентификации при доступе к онлайн-счетам, например, в системах PayPal и eBay.

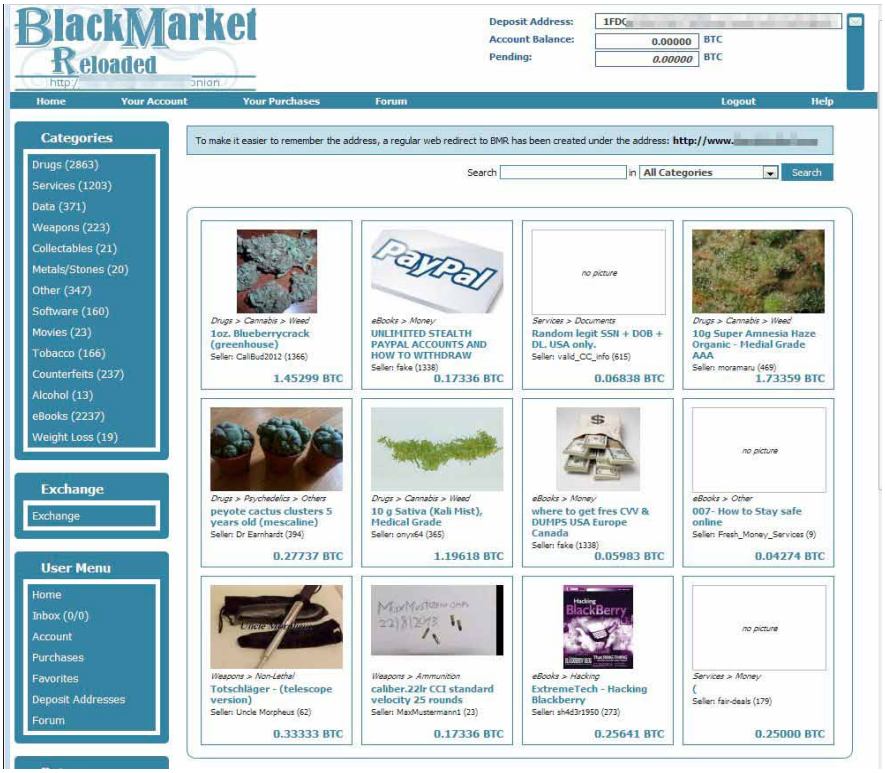

Рис. 2. Виртуальные валюты принимаются в качестве средства оплаты множества незаконных товаров на анонимных торговых площадках.

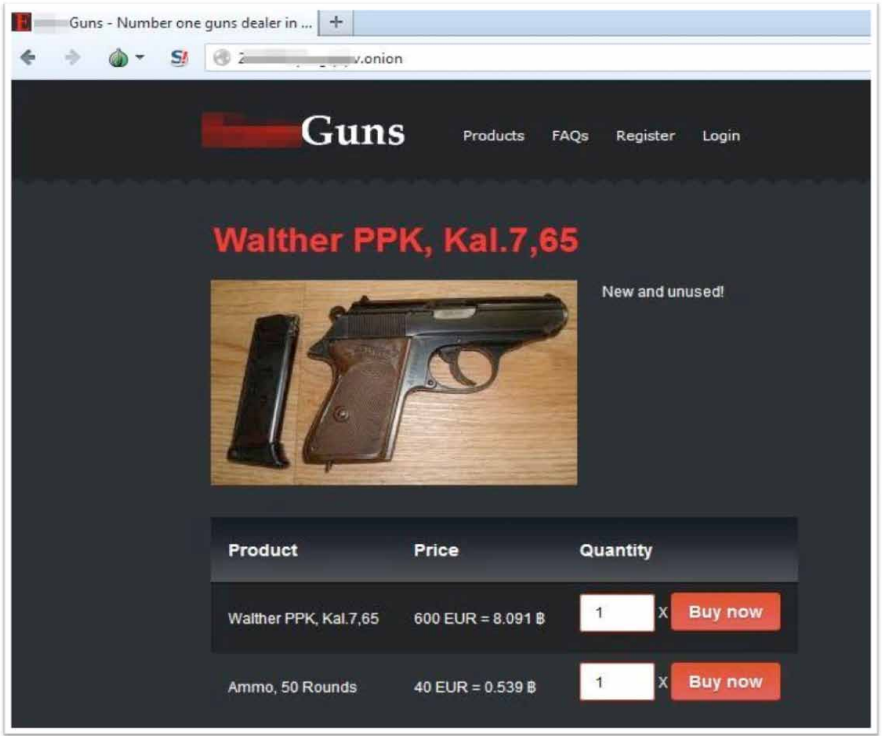

Рис. 3. Торговля контролируемыми товарами, такими как огнестрельное оружие, также переходит на виртуальные валюты, поскольку сама природа таких валют не только затрудняет контроль над оборотом оружия, но и не позволяет проследить связь между оружием и преступником в случае применения оружия.

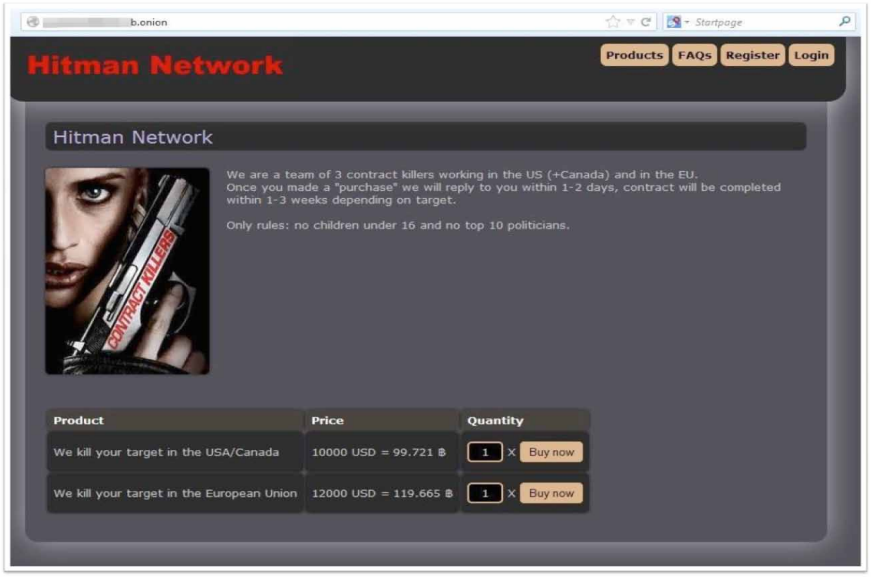

Рис. 4. Клиенты могут анонимно пользоваться услугами таких веб-сайтов, как Hitman Network — служба, предлагающая услуги киллеров с единственным заявленным ограничением: «Цель не должна быть младше 16 лет и не должна принадлежать к высшим политическим кругам».

Одним из самых больших преимуществ цифровых и электронных денег является простота их использования. Чтобы начать пользоваться той или иной системой, иногда необходимо пройти регистрацию на бирже. Однако в некоторых случаях достаточно просто купить виртуальные деньги за наличные.

Bitcoin в настоящее время является ведущей виртуальной валютой не только по популярности, но и по цене. 28 февраля 1 биткоин приравнивался к 33 долларам США. К 10 апреля курс подскочил до 266 длолларов США, а затем стабилизировался к июлю на уровне 100 долларов США. По состоянию на 4 сентября курс биткоина составлял 144 доллара США.

Во избежание централизации управления система Bitcoin строится на архитектуре одноранговой сети с алгоритмами шифрования. Правоохранительные органы утверждают, что это также затрудняет идентификацию подозрительных пользователей и получение записей об операциях.

Однако такая децентрализованная структура тоже не может не быть уязвимой. Например, сеть Bitcoin много раз страдала от атак типа «отказ в обслуживании» (DoS), которые заставили группу разработчиков исправить ядро. Кибератаки, направленные на виртуальные валюты, не ограничиваются сетью Bitcoin; достается и биржам.

В июне 2011 года был взломан сайт Mt.Gox — главная биржа сети Bitcoin. Серия мошеннических операций повергла экономику Bitcoin в хаос на целую неделю, обрушив курс биткоина с 17,5 доларов США практически до нуля.

Разработка майнера Bitcoin на основе JavaScript позволила создавать майнеры-боты. Хотя не все майнеры вредоносны, используемые ими противозаконные методы распространения являются причиной всплесков активности вредоносных программ и ботов. Эти всплески, как правило, соответствуют колебаниям курса Bitcoin.

Проведенный McAfee Labs анализ бот-сети Bitcoin выявил и другие бот-сети, взаимодействующие со службами-майнерами Bitcoin. Этими ботами управлял центральный сервер, который устанавливался и регистрировался в онлайн-службе майнера с использованием учетных данных, предоставленных атакующим, в результате чего биткоины зачислялись уже на счет атакующего. В июне 2011 года у пользователя Bitcoin под псевдонимом Allivain было похищено полмиллиона долларов США.

Расследование выявило потенциальные уязвимости в системе хранения личных данных в Bitcoins. Новые исследования, проведенные учеными из Университета Калифорнии, Сан-Диего, и Университета Джорджа Мейсона, позволили более подробно раскрыть проблемы сохранения анонимности, обусловленные применением сервиса Block Chain открытого реестра Bitcoin, в котором хранятся сведения обо всех операциях и который, по заявлению создателей, гарантирует прозрачность всех транзакций.

Выводы

Попытки закрыть службы виртуальных валют всегда приводили к тому, что преступники просто переводили свой бизнес на другие платформы, примером чего может служить история с Liberty Reserve. Несмотря на такие благоприятные условия для преступников, правоохранительные органы в сотрудничестве со своими коллегами из других стран и с частным сектором предпринимают все возможное для выявления и ареста лиц, эксплуатирующих такие платформы.

Виртуальные валюты не исчезнут. Несмотря на очевидные проблемы, связанные с атаками типа «отказ в обслуживании», использованием таких бирж для отмывания денег и содействием преступности, существуют и широкие возможности для законного использования систем. Игнорирование этих рыночных возможностей может лишить легальных инвесторов значительной доли прибыли, однако, пренебрежение потенциальными рисками может стоить дороже.

Полный текст отчета находится по этой ссылке: www.mcafee.com/ru/resources/white-papers/wp-digital-laundry.pdf.

McAfee
An Intel Company

ООО «МакАфи Рус»
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
БЦ «Башни на набережной», Башня «А»,
15 этаж
Телефон: +7 (495) 653-85-13
www.McAfee.ru

60589exs_digital-laundry_1013_fnl_ETMG