УДК 336-161.1; 004.056.53

С.Б. Вепрев[1]
В.А. Перов[2]

ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ КРИПТОВАЛЮТ

В статье рассмотрены вопросы обеспечения информационной безопасности при использовании криптовалюты. Анализируются возможные уязвимости при использовании с целью оборота криптовалюты анонимайзер Tor и способы незаконного создания ботнет-сетей с целью осуществления майнинга криптовалют.

Ключевые слова: *информационная безопасность, криптовалюта, блокчейн, биткойн, Ботнет, майнер-вирус, анонимайзер.*

S.B. Veprev
V.A. Perov

INFORMATION SECURITY ISSUES WHEN USING CRYPTOCURRENCY

In the article, the issues of ensuring information security when using cryptocurrency are considered. Possible vulnerabilities are analyzed when using the anonymizer Tor for the circulation of crypto currency and ways of illegal creation of botnet networks for the purpose of implementing cryptocurrency mining.

Keywords: *information security, cryptocurrency, blockchain, BitCoin, Botnet, minor virus, anonymizer.*

Развитие информационных технологий в XXI веке привело к созданию такого финансово-информационного феномена, как криптовалюта. Криптовалюта основывается на применении пиринговых платежных систем, использующих соответствующий протокол передачи данных, основанный на криптографических методах обработки транзакций. Бесспорным лидерством среди ряда криптовалют конечно же является *биткойн*. На сегодняшний день как в России, так и во всем мире отсутствует единое мнение о целесообразности его использования. Особое внимание уделяется вопросам обеспечения безопасности криптовалютных расчетов при совершении сделок. Отмечается, что «в настоящее время в мировом сообществе не наблюдается единства мнений о биткойне ни со стороны регуляторов, ни ведущих представителей экономической и юридической наук» [6, с. 26]. «В настоящее время вопросы о правовой природе и правовых рисках использования криптовалюты не только не решены, но и надлежащим образом не поставлены» [7, с. 194]. Отметим, что на сегодняшний день в Российской Федерации законодатель пока еще не дал четкого правового определения криптовалюты и ее правового статуса.

Использование криптовалюты как определенного экономического инструмента, влияющего на материальные интересы субъекта, его использующего, должно быть безопасным. В противном случае полностью теряется смысл практического использования криптовалюты. Учитывая, что криптовалюта использует сетевые информационные технологии, особое внимание должно уделяться вопросам обеспечения информационной безопасности. Это – обеспечение надежности парольной защиты криптокошелька, защита от вредоносных программ и т.п.

Необходимо отметить, что уже появился некий, если его так можно назвать, *майнер-вирус*, использующий зараженные Ботнет-сети, позволяющие сторонним лицам незаконно и удаленно управлять зараженными компьютерами в своих интересах.

Майнер-вирус является троянским вирусом, ориентированным на использование технологии

[1] Доктор технических наук, зав. кафедрой информационных технологий, Московская академия Следственного комитета РФ.

[2] Доцент кафедры предварительного расследования преступлений в сфере экономики института повышения квалификации, Московская академия Следственного комитета РФ.

блокчейн. Он проникает в операционную систему с открытием самим пользователем определенной программы из Интернета. Такая вредоносная программа включается в некоторый ресурс – это может быть неизвестное, но «интересное» письмо, предложение зарегистрироваться на каких-то ресурсах, угроза заблокировать счет и т.п.

Когда передается управление такому ресурсу, – он параллельно, незаметно для пользователя, загружает соответствующую вредоносную программу.

Основой технологии блокчейн является *майнинг* – процесс по поддержанию *пиринговой* сети и созданию новых блоков блокчейн с возможностью получить соответствующее вознаграждение в форме эмитированной валюты и комиссионных сборов.. Проникнув в ваш компьютер, такой вирус прописывается в разнообразные приложения и маскируется под них. Майнер-вирус ориентирован только на использование вычислительных ресурсов компьютера в целях майнинга, то есть налицо обогащение неизвестного вам лица за ваш счет. Особенность его «работы» проявляется в том, что скорость выполнения любых процедур вашего ПК значительно затормаживается. Но если вы активно не загружаете процессор, например работаете в MS WORD, просматриваете загруженный файл, редактируете графические объекты и т.п., то работу такого вируса вы даже не заметите. Если имеется целая сеть зараженных персональных компьютеров (Ботнет), то она может заменить целый пул, а это уже достаточно большой ресурс для майнинга определенного лица или группы лиц за чужой счет. Отметим, что майнер-вирус просто выполняет множество вычислений и поэтому, как таковой, является обычной программой. Вследствие этого антивирус далеко не всегда реагирует на такие действия, считая их вполне нормальными (по крайней мере, до определенного времени).

Еще одним характерным аспектом использования криптовалюты является обеспечение анонимности проведения транзакций. Достаточно часто криптовалюта используется в криминальных целях: продажа наркотиков, оружия, оказание криминальных услуг вплоть до заказного убийства. В этих целях используются *аномайзеры*, наибольшей популярностью среди которых пользуется Tor. Технология Tor представляет собой сеть маршрутизаторов, на которые перенаправляют полученный на них пакет в зашифрованном виде, причем в заранее непредсказуемом направлении. Передаваемая информация от одного маршрутизатора к другому каждый раз снова шифруется. Последний выходной узел снимает последний слой шифрования и отправляет сообщение адресату. Установленная цепочка остается доступной для двусторонней передачи данных в течение некоторого периода времени. Получатель запроса может отправить ответ по той же цепочке без ущерба для анонимности каждой из сторон. Примеры сайтов и общения в Tor показаны на рис. 1.

Однако существует определенная опасность использования криптомонет и при помощи анонимайзеров. И в этом случае риск утечки персональных данных существенно возрастает. Это обнаружили исследователи (авторы исследования – Иван Пустогаров и Алекс Бирюков из исследовательской лаборатории CryptoLUX Люксембургского университета), которые определили, что с помощью определенных манипуляций возможно определить персональные данные биткойн-пользователя, работающего через

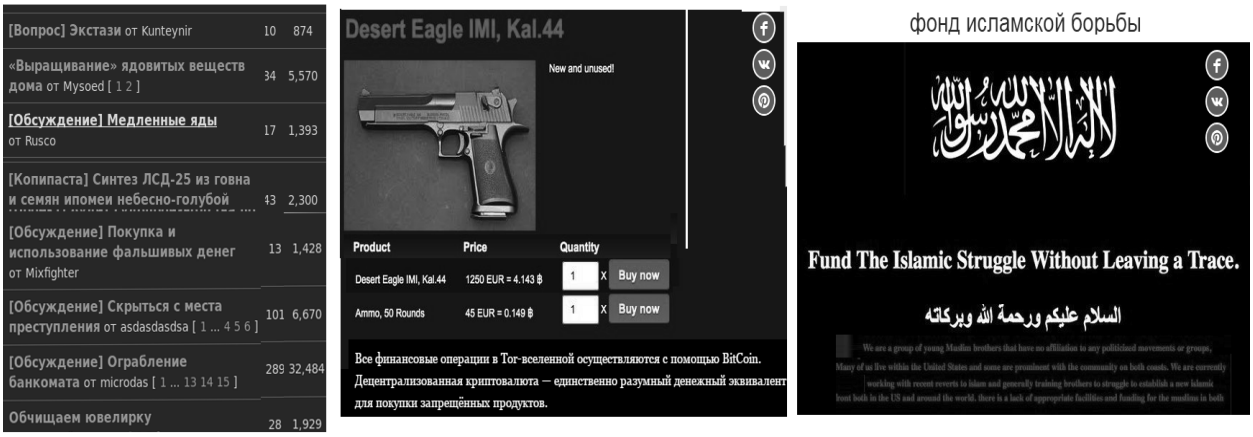

Рис.1. Примеры сайтов и общения в Tor

браузер Tor. Подключаясь к сети Tor, люди ожидают полной анонимности и вроде бы ее получают, однако ее несложно обойти. И. Пустогаров и А. Бирюков выявили возможность подобной манипуляции, сфокусировавшись на малоизвестном аспекте протокола биткойн: встроенной защите от DoS-атак (атака отказа в обслуживании). В целях самозащиты, биткойн-серверы присваивают баллы пользователям, генерирующим проблемные транзакции. В том случае, если количество баллов превышает 100, сервер блокирует пользователя на 24 часа. Авторы поясняют, что когда пользователь сети Tor подсоединяется к биткойну, его IP-адрес никак не фигурирует в сети. Вместо этого адреса биткойн-сеть видит только адреса выходного Tor-узла. Таким образом, злоумышленники могут заблокировать все выходные узлы «Тора», инициировав большое количество невалидных транзакций через Tor. Благодаря принципу работы защитной системы на серверах биткойна через какое-то время после начала спам-атаки все выходные узлы Tor попадут в черные списки. Когда жертва начнет использовать Tor для подключения к биткойну, ей ничего не остается, кроме как подсоединиться к тем биткойн-серверам, которые уже захвачены взломщиком, так как все остальные заблокированы. С этой секунды вся информация о биткойн-транзакциях жертвы проходит через руки злоумышленника. В результате атаки транзакции и блоки, запущенные истинным владельцем биткойн-адреса, тоже подвергаются рискам, поскольку взломщик может отложить их или вовсе отменить. Данный вид атак представляет серьёзную опасность для продавцов на теневом интернет-рынке, чей бизнес существует только при условии полной анонимности. Подобные предприниматели рискуют оказаться рассекреченными руками своих конкурентов.

Популярность криптовалют всё более возрастает. Технология блокчейн объявляется технологией будущего, технологией, обеспечивающей электронную экономическую деятельность, основанную на цифровых технологиях. Не уменьшая значимости данной технологии, все-таки следует заметить, что она еще не исследована в полном объеме.

Литература

1. Гражданский кодекс Российской Федерации (части первая–четвертая).
2. Налоговый кодекс Российской Федерации (части первая, вторая).
3. Федеральный закон от 02.12.1990 № 395-1-ФЗ «О банках и банковской деятельности».
4. Кузнецов В.А., Якубов А.В. О подходах в международном регулировании криптовалют (BITCOIN) в отдельных иностранных юрисдикциях // Деньги и кредит. – 2016. – № 3.
5. Информация Банка России от 27.01.2014 «Об использовании при совершении сделок виртуальных валют, в частности Биткойн».
6. Беломытцева О.С. О понятии криптовалюты биткоин в рамках мнений финансовых регуляторов и контексте частных электронных денег // Проблемы учета и финансов. – 2014. – № 2 (14).
7. Сидоренко Э.Л. Криптовалюта как новый юридический феномен // Общество и право. – 2016. – № 3 (57).
8. Поппер И. Цифровое золото. Невероятная история Биткойна, или как идеалисты и бизнесмены изобретают деньги заново. – М. : ООО «И.Д. Вильямс», 2016.
9. Материалы Международной научно-практической конференции (2 июня 2016 г.). Федеральное собрание Российской Федерации. Государственная Дума. – М. : Юрлитинформ, 2016.