УДК 336.717.1:004.738.5

ЧЁРНЫЙ МАЙНИНГ. КАК РАБОТАЮТ ВИРУСЫ-МАЙНЕРЫ. ЗАЩИТА КОМПЬЮТЕРОВ ОТ КРИПТОВИРУСОВ

Кандера Д.Р., Караневич К.А.
Научный руководитель: ст. преподаватель Ковалькова И.А.
Белорусский национальный технический университет

Сегодня криптовалюты становятся всё более популярными, однако их добыча требует не только мощных вычислительных ресурсов, надёжных серверов и специализированных программ для майнинга, но и значительного расхода электроэнергии. Если компьютер начинает работать медленно и счета за электроэнергию растут, то есть вероятность того, что владелец данного компьютера стал жертвой чёрного майнинга. Поэтому важно, чтобы пользователи имели понимание о процессе майнинга и особенностях чёрного майнинга, чтобы не стать жертвами мошенников, злоупотребляющих ресурсами компьютеров других людей.

Извлечение криптовалюты с использованием специализированного оборудования, известного как майнинг, представляет собой добычу цифровой валюты. Эта валюта измеряется в цифровых монетах и содержит зашифрованную информацию, которая обеспечивает защиту от мошенничества и подделки.

В настоящее время из-за острой конкуренции для успешной добычи криптовалюты требуется использование мощного оборудования, такого как майнинг-фермы, которые характеризуются высоким уровнем энергопотребления.

Учёные из Кембриджского университета определили, что годовое потребление энергии на майнинг составляет около 121,36 тераватт-часов (ТВтч), что превышает потребление энергии в Аргентине, Нидерландах и Объединённых Арабских Эмиратах. [1]

Исходя из вышесказанного, можно сделать вывод о том, что стоимость легального создания майнинг-фермы является большой, что приводит к появлению нелегальных, так называемых "чёрных ферм". Майнеры начали использовать чужие компьютеры для добычи криптовалюты, а также прибегают к другим нечестным методам, таким как неоплата электричества путём незаконного подключения к трансформаторам или контрабандного ввоза оборудования для собственных майнинг-ферм. Важной тенденцией стало установка ферм в заброшенных зданиях и использование самодельных устройств для подключения к сети.

Чёрный майнинг – это незаконный способ добычи криптовалюты, который включает использование компьютера или другого устройства без разрешения владельца.

Два основных способа нелегального майнинга с использованием чужих компьютеров – это майнинг в браузере и вирусы-майнеры.

1. Браузерный майнинг.

Этот метод добычи криптовалюты, известный как майнинг в браузере, осуществляется непосредственно внутри браузера с использованием языка сценариев. Важно отметить, что посещение подозрительных веб-сайтов может нанести вред компьютеру пользователя, также как и в случае с криптовалютами. Для активации браузерного майнинга на персональном компьютере (ПК) достаточно перейти по ссылке на ресурс, где прописан соответствующий код в скрипте, и во время пребывания пользователя на сайте его компьютер будет привлекаться для создания криптовалюты в рамках сети майнеров.

2. Вирусы-майнеры.

Первые упоминания о вирусе-майнере появились ещё в 2011 году, и с тех пор он продолжает атаковать компьютеры обычных пользователей. Вирус-майнер может заразить компьютер, если пользователь перейдёт по ссылке в письме или установит непроверенное программное обеспечение. Особенно уязвимыми являются компьютеры с высокой производительностью.

Вред, наносимый вирусами-майнерами, превосходит вред от браузерного майнинга, так как они более активно используют ресурсы персонального компьютера. Однако браузерный майнинг встречается гораздо чаще, так как он более прост в использовании.

Существует три наиболее распространённых типа вирусов-майнеров:

– web-майнер;

– простой;

– скрытый.

Web-майнер размещается на веб-странице или в установленном расширении браузера. Когда такой вирус присутствует на компьютере, работа в Интернете может замедляться. Согласно данным AdGuard, около 220 из 100 тысяч веб-сайтов используют веб-майнеры. Однако веб-майнеры легко обнаруживаются и удаляются, так как они не являются скрытыми вирусами-майнерами. [2]

Простые и скрытые вирусы-майнеры могут быть размещены на компьютере пользователя-жертвы. При наличии этих видов вирусов замедляется отклик компьютера, даже на простые действия пользователя. Несмотря на это, простой вирус может быть легко обнаружен и удалён без применения постороннего программного обеспечения.

Скрытый вирус-майнер активно избегает обнаружения мониторинговыми системами, блокирует работу некоторых антивирусов и автоматически отключается во время активного использования компьютера, что затрудняет его обнаружение в системе. Также удаление данного вируса усложняется тем, что он создаёт множество копий, не позволяя удалить его обычными методами.

Для гарантии собственной безопасности, пользователю стоит ознакомиться с инструментами, которые наиболее часто применяются злоумышленниками-майнерами, такими как распространённые вирусные программы, используемые для чёрного майнинга. Рассмотрим подобные программы.

1. Троян Miner Bitcoin.

Обычный пользователь, использующий компьютер, может наблюдать нагрузку в размере 20%, однако, при наличии данного трояна, нагрузка на компьютер может возрасти до 80% или даже 100%. Эта программа также осуществляет кражу личных данных пользователя, что может иметь серьёзные последствия. Одним из характерных признаков этого трояна является повышенный уровень шума от компьютера. Miner Bitcoin может попасть на компьютер пользователя при скачивании документов или картинок, часто это происходит через Skype.

2. EpicScale.

Эта программа связана с использованием мощностей компьютеров других пользователей для решения своих задач. Её замечают на компьютерах пользователей определённых торрент-трекеров. В ответ на заявления компании о том, что собранные средства от майнинга направляются на благотворительные цели, пользователи выражают недоверие.

3. JS/CoinMiner.

Эта программа представляет собой вид программного обеспечения, позволяющий осуществлять майнинг криптовалюты с использованием ресурсов процессора через браузеры компьютеров пользователей. Она чаще всего встраивается в веб-сайты и платформы, связанные с играми и потоковыми видео, где она загружает процессор компьютера, обеспечивая незаметное протекание майнинга.

Для того чтобы избежать заражения вирусами-майнерами, следует соблюдать следующие рекомендации:

Рекомендуется не скачивать и не использовать нелицензионное программное обеспечение, а также избегать ввода ключей активации из непроверенных источников и переходов по подозрительным ссылкам.

Важно помнить, что установка антивирусного программного обеспечения может быть полезной мерой, однако необходимо регулярно обновлять его до последней версии.

Если вы заметили, что производительность вашего компьютера снизилась, то стоит проверить, используют ли какие-либо программы 80-90% ресурсов процессора, запустив "Диспетчер задач". Однако, даже если обнаружено, что такие программы не используются, необходимо оставаться бдительным, так как вредоносные программы-майнеры могут использовать меньшее количество мощности, что делает их более сложными для обнаружения.

Если антивирусное программное обеспечение, установленное на компьютере, не обнаруживает потенциально опасных программ, можно попробовать переустановить операционную систему, установить другое антивирусное программное обеспечение или обратиться к знакомому программисту, который поможет найти и удалить вредоносные файлы. [3]

Литература

1. Сколько мирового электричества тратят на майнинг. [Электронный ресурс] Режим доступа: https://devby.io/news/maining.amp, свободный.

2. Cryptocurrency mining affects over 500 million people. And they have no idea it is happening [Электронный ресурс]: AdGuard Blog.. — Режим доступа: https://adguard.com/en/blog/crypto-mining-fever/, свободный.

3. Чёрный майнинг. [Электронный ресурс] Режим доступа: https://lifehacker.ru/chernyj-majning/, свободный.

УДК 159.9

ЗАВИСИМОСТЬ ОТ КОМПЬЮТЕРНОЙ ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ

Капустина Д.С.
Научный руководитель: ст. преподаватель Галай Т.А
Белорусский национальный технический университет

40 лет назад об электронных СМИ можно было только мечтать. На смену громоздким вычислительным машинам стали приходить удобные компьютеры. Глобальная интеграция и увеличивающийся темп жизни требовали увеличения возможностей компьютера. Проверенная истина: одна голова хорошо, но две лучше, легла в основу объединить два компьютера, таким образом увеличить возможность каждого вдвое. Появилась гениальная идея – связать между собой сети, не объединяя отдельные компьютеры. Так появился Интернет – бесчисленное количество сетей. Название Всемирной