УДК 004.056.5

ЧЕРНЫЙ МАЙНИНГ. КАК РАБОТАЮТ ВИРУСЫ-МАЙНЕРЫ. ЗАШИТА КОМПЬЮТЕРОВ ОТ ВИРУСОВ.

Полешук О.А.
Научный руководитель: ст. преподаватель Ковалькова И.А.
Белорусский национальный технический университет

Сейчас популярность криптовалюты возрастает, и для её добычи помимо мощных компьютеров также требуется повышенный расход электроэнергии. Поэтому для того, чтобы не стать жертвой чёрных майнеров, необходимо иметь представление о чёрном майнинге и майнинге в целом.

Майнинг (от англ. mining – добыча полезных ископаемых) – это добыча *криптовалюты* с использованием мощностей специального оборудования. В свою очередь, **криптовалюта** – это разновидность цифровых денег, в основе которой лежит технология криптографии, то есть шифрования данных. Она не имеет физического облика, а существует только в электронном виде.

Для того чтобы осуществлять майнинг криптовалюты, нужно располагать мощным ПК, специальной программой и надёжным сервером. Тем не менее, из года в год майнинг усложняется, а конкуренция возрастает.В настоящий момент для одной транзакции требуется большое количество электроэнергии. Согласно подсчётам экспертов, примерно через 2,5 года расход электричества на генерирование криптовалюты будет эквивалентен годовому показателю энергетического потребления такой небольшой страны, как Дания.

Рост курса криптовалют и расходов на их добычу автоматически влечёт за собой распространение нечестных способов майнинга – от покупки контрабандного оборудования для майнинг-ферм до подключения к электросети в обход счётчиков. Таким образом, **чёрный майнинг** – это добыча криптовалют незаконным способом. Как правило, чёрные майнеры пользуются ПК, которые принадлежат другим людям.

Впервые официальные сообщения о явлении чёрного майнинга начали появляться в 2011 году, а в 2013 году уже произошло массовое заражение ПК в различных странах, посредством «Skype». Причём вирусные программы, так называемые трояны, не только майнили, но и получали доступ к *криптокошелькам*. Самый известный случай – попытка разработчиков «µTorrent» дополнительно заработать на пользователях, внедрив в софт скрытый майнер «EpicScale».

Обычно чёрный майнинг предусматривает добычу таких криптовалют, как *Litecoin, Feathercoin*, а также *Monero*, так как для их получения не надо располагать техникой, которая имеет большие мощности.

На данный момент можно выделить *два типа майнинга* на чужом оборудовании, которым пользуются злоумышленники:

1. Браузерный майнинг.Для данного вида чёрного майнинга достаточно перейти по ссылке на ресурс, в скрипте которого прописан нужный код, и, пока пользователь будет находиться на сайте, его компьютер станет частью сети по генерированию криптовалюты.

2. Вирусы-майнеры.Подцепить их можно, перейдя по ссылке из письма или установив сомнительную программу. Вирусы более вредоносны компьютерам, чем браузерный майнинг, потому что более активно используют мощности компьютера. Тем не менее жертвами браузерных атак становится гораздо больше пользователей.

Однако зная средства, используемые злоумышленниками, можно эффективно противостоять их атакам. Для этого следует рассмотреть следующие виды *вирусов-майнеров*:

- **MinerBitcoin.**Данная программа относится к троянам, она нагружает компьютер на полную мощность и помимо этого ворует личную информацию пользователя. Распространяется через «Skype» или документы Word.
- **EpicScale.**Программа устанавливается вместе с «uTorrent». Представители разработчика заявили, что EpicScale была якобы частью их партнёрской программы.
- **JS/CoinMiner.**Программа-скрипт, позволяющая делать майнинг через браузер, загружая процессор пользовательского компьютера. Распространяется через игровые сайты или потоковое видео.

Принцип работы чёрного майнинга заключается в следующем: втайне от пользователя, например, при открытии любого файла, ему устанавливается программа-клиент, которая подключается к одному из майнинг-пулов и начинает добывать криптовалюту. «Пул» («mining pool») –сервер, распределяющий задачу расчёта подписи блока между всеми подключёнными участниками. Вклад каждого из них оценивается с помощью так называемых «шар» («share»), которые являются потенциальными кандидатами на получение драгоценной подписи. Как только одна из «шар» попадает в цель, пул объявляет о готовности блока и распределяет так называемые монеты.Выплаты производятся на указанные в аккаунте пользователя реквизиты, и он имеет право подключать к своей учётной записи любое количество ПК, и никто не требует с него доказательств, что они принадлежат именно ему или их владельцы

одобрили это действие.Поэтомупулы – идеальный вариантдля создания собственной майнинг-сети.

Чёрный майнинг также часто называют *скрытым майнингом*, так как свою работу майнер может осуществлять в скрытом режиме. Основные возможности, благодаря которым майнер может это делать, заключаются в следующем:

- майнер внедряется в связке с торрентами или в виде простых файлов, таких как картинки или Word-файлы, приложенные к сообщениям;
- установка производится в тихом режиме;
- процесс маскируется под одну из служб Windows или не отображается вовсе;
- во время повышенной нагрузки на машину – майнер отключается, чтобы не вызывать заметное торможение.

Однако для того, чтобы устранить попытку использования вашего компьютера для майнинга, нужно понять, что ПК всё-таки заражён. Первый признак – это снижение скорости работы ПК и увеличение потребления энергии. К сожалению, торможение компьютера – единственный признак, с помощью которого можно определить, что он заражён вирусом-майнером.

На сегодняшний день есть *ряд так называемых «профилактических» мер*, которые помогут оградить ПК от вирусных атак через браузер:

- редактирование файла, который носит название «hosts»;
- установка утилиты «Anti-WebMiner», а также браузерного расширения «NoCoin»;
- отключение JavaScript в браузере и применение «NoScript»;
- добавление антимайнинговогой защиты в «AdBlock», а также «uBlock».

И всё-таки остаётся главный вопрос – как не стать жертвой чёрного майнинга? Для этого стоит придерживаться ряда правил:

1. Не загружать на компьютер нелицензионные программы, приложения, избегать ввода активационных ключей из сомнительных источников и не применять непроверенные ссылки.
2. Для владельцев ПК, который изготовила компания «Apple», необходимо установить в настройках опцию, которая подразумевает скачивание только программных продуктов из «AppStore».
3. Необходимо регулярно обновлять антивирусник, так как его установка – это только полумера.
4. Если на ПКустановлена ОС «Windows», требуется создать учётную запись и загружать компьютер только через неё.

5. В том случае, если ПК стал сильно тормозить, надо воспользоваться «Диспетчером задач». С его помощью можно увидеть программы, которые запущены на ПК.

Таким образом, исходя из всего выше перечисленного, можно сделать вывод, что чёрный майнинг и майнинг в целом очень сложная, но вместе с тем очень интересная тема, разбираясь в который можно обезопасить себя от внешнего вмешательства в компьютер пользователя, сохранить свои данные в сохранности, а также не допустить утечку, используемой компьютером энергии.