**Литература**

1. Единый портал электронных услуг [Электронный ресурс]. – Режим доступа: https://portal.gov.by/. – Дата доступа: 10.03.2021.
2. Изменения электронного декларирования – правила ОАИС [Электронный ресурс]. – Режим доступа: https://epi-gge.com/novosti/izmeneniya-elektronnogo-deklarirovaniya-pravila-oais/. – Дата доступа: 25.03.2021.
3. ОАИС — альфа и омега в сфере оказания электронных сервисов государства [Электронный ресурс]. – Режим доступа: https://news.tut.by/press/627881.html. – Дата доступа: 19.03.2021.
4. Основы xml для начинающих. Язык XML практика и теория [Электронный ресурс]. – Режим доступа: https://akkordi-pesni.ru/osnovy-xml-dlya-nachinayushchih-yazyk-xml-praktika-i-teoriya-deklaracii-osnovnyh/. – Дата доступа: 03.04.2021.
5. Электронное декларирование теперь и через ОАИС [Электронный ресурс]. – Режим доступа: https://declarant.by/ru/news/electronic-declaration-now-and-through-nais/. – Дата доступа: 27.03.2021.

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

Платонова Е.С., Харитончик А.В.
Научный руководитель: ст. преподаватель Ковалькова И.А.
Белорусский национальный технический университет

Везде, где существуют правила, есть те, кто их не соблюдает и нарушает. Мир криптовалют не исключение. Некоторые майнеры не платят за электричество, подтягивая кабель к трансформатору, а кто-то контрабандой везёт видеокарты из Китая. Но чаще всего добытчики цифровой валюты используют чужие компьютеры. Обычно Litecoin, Feathercoin и Monero добываются в процессе чёрного майнинга. Для их добычи не требуется мощное оборудование, а монеты можно добывать с обычных домашних компьютеров. Хакеры используют два основных типа компьютерного майнинга:

1) Браузерный майнинг. Предупреждение о том, что посещение подозрительных веб-сайтов может нанести вред компьютеру, также действует и в случае с криптовалютами. Пользователю достаточно просто нажать на ссылку на ресурс, скрипт которого содержит необходимый код, и, как только он окажется на сайте, его компьютер станет частью сети

генерации криптовалюты. Однако в зону риска попадают не только малоизвестные сайты. Известный украинский медиахолдинг, пользователи которого стали невольными добытчиками Monero, оказался в эпицентре скандала. Аналогичное обвинение было предъявлено американскому телеканалу Showtime.

2) Вирусы-майнеры. Вирус-майнер впервые появился в 2011 году, но с тех пор продолжает заражать компьютеры обычных пользователей. Подцепить его можно, перейдя по ссылке из письма или установив подозрительную или ненадёжную программу. Все компьютеры с высокими техническими параметрами относятся к зоне риска. Вирусы причиняют компьютеру больше вреда, чем браузерный майнинг, потому что более активно используют мощности компьютера. Тем не менее, гораздо больше пользователей становятся жертвами атак браузера. [1]

Как понять, что компьютер заражён? Единственный явный признак атаки майнинга – замедление работы компьютера. Если это происходит на определённом сайте, то возможно, что злоумышленники проникли через браузер. Особенно важно наблюдать, нормально ли работает техника, на ресурсах, требующих длительного времяпрепровождения, например, на торрент-трекерах, сайтах с онлайн-играми и фильмами. Геймерские компьютеры особенно уязвимы для атак, поскольку они, как правило, имеют более мощные видеокарты и процессоры. Еще один вспомогательный признак атаки майнинга – увеличение энергопотребления. Довольно часто антивирусные программы распознают майнеры не как вирусы, а как потенциально опасные программы, снижающие производительность компьютера. По факту майнеры не наносят никакого другого вреда, кроме как использование ваших ресурсов.

Популярные вирусные программы для чёрного майнинга:

1) *Троян Miner Bitcoin*. Если среднестатистический человек в среднем нагружает свой компьютер на 20%, то Miner Bitcoin увеличивает эту цифру до 80, а то и 100%. Программа-шпион не только использует ресурсы, но и крадёт данные о владельце оборудования. Характерным внешним признаком наличия вируса является повышенный уровень шума кулера видеокарты. Пользователь может подхватить Miner Bitcoin, загрузив документы или изображения Word, в основном он распространяется через Skype.

2) *EpicScale* – это программа, которую заметили пользователи uTorrent, использующая возможности чужих компьютеров для решения своих задач. В ответ на обвинения представители компании отметили, что средства, полученные от майнинга, идут на благотворительность. Однако такая позиция по меньшей мере странна, учитывая незнание пользователей

торрент-трекера об использовании их техники. Важно знать, что при удалении EpicScale её исполнительные файлы остаются на компьютере.

3) *JS/CoinMiner* – это одна из разновидностей вредоносных программ, которая позволяет осуществлять добычу криптовалют через браузеры пользователей. В большинстве случаев скрипты внедряются в игровые сайты и потоковые видеоресурсы. Такие ресурсы загружают процессор, что позволяет оставлять майнинг незамеченным. [1]

Как не поймать вирус-майнер: меры предосторожности. Самое главное правило – не загружать нелицензионные продукты, не вводить ключи активации из непроверенных источников, а также не переходить по сомнительным ссылкам. Если пользователь является владельцем компьютера фирмы Apple, то он должен установить в настройках функцию скачивания программ исключительно из App Store. Если владельцы компьютеров замечают, что их компьютер тормозит, то следует запустить «Диспетчер задач» и проверить, есть ли программа, которая использует их процессор на 80–90%. Однако если её нет, то нельзя расслабляться, так как программы-майнеры потребляют меньше энергии и их труднее заметить. Следует установить утилиты, которые, помимо защиты от вирусов, сообщают обо всех изменениях в реестре. Лучше всего установить uMatrix и RequestPolicy Continued одновременно, а пользователям Google Chrome доступен ещё и блокировщик Antiminer. Также важно сканировать свой компьютер с помощью программ AdwCleaner или Malwarebytes, которые обнаруживают шпионские программы. [2]

**Литература**

1. Чёрный майнинг: как зарабатывают деньги через чужие компьютеры // Сайт Лайфхакер [Электронный ресурс] – Режим доступа: https://lifehacker.ru/chernyj-majning/. Дата доступа: 28.03.2021.

2. Чёрный майнинг: как защитить свой компьютер и не стать жертвой мошенников // Сайт Школа инвестирования и трейдинга [Электронный ресурс] – Режим доступа: https://investment-school.ru/black-mining/. Дата доступа: 28.03.2021.

## СТИРАЛЬНАЯ МАШИНА. ВИДЫ И УСТРОЙСТВО. РАБОТА И ОСОБЕННОСТИ

Полозняк А.В.
Научный руководитель: д.т.н., доцент Голубцова Е.С.
Белорусский национальный технический университет