Surf Anonymous Free – программа, которая защищает пользователя от небезопасных сайтов, предотвращает отслеживание и мониторинг сетевого трафика.

Tor Project – приложение, представляющее программный комплекс для обеспечения анонимного статуса при сёрфинге сайтов.

TryCatchMe – сервис, который поможет зайти на заблокированный администратором сайт и сохранить практически все конфиденциальные данные при себе.

Чёрный майнинг. Как работают вирусы-майнеры. Защита компьютеров от криптовирусов

Чепикова Д.А.
Научный руководитель: Ковалькова И.А.
Белорусский национальный технический университет

Сегодня понятие «майнинг» уже успело засветиться на страницах узкопрофильных экономических или IT-изданий. ***Майнинг*** (от англ. mining – добыча полезных ископаемых)– деятельность по созданию новых структур для обеспечения функционирования криптовалютных платформ[1].

Везде, где существуют правила, найдутся те, кто хочет их обойти или нарушить. Мир криптовалют не является исключением, потому чтосовременные майнеры уже разработали методы,которые позволят получать цифровую валюту посредством компьютеров, принадлежащих другим людям. Так появился *чёрный майнин*г – незаконная добыча криптовалюты.

Есть два вида чёрного майнинга, подразумевающие использование чужих ПК: майнинг через браузер и вирусный майнинг.

Майнинг через браузер.

Если пользователь последует по предложенной ему ссылке на каком-либо сайте, есть возможность, что его ПК войдет в сеть по добыче криптовалют. Допустим, существует веб-сайт, который решил майнить криптовалюту на ресурсах посетителей. Сайт начинает использовать мощности пользовательских видеокарт, в то время как они, ничего не подозревая, продолжают пользоваться сайтом. Хотя выработка при таком майнинге не особо большая, злоумышленники берут количеством посетителей. Первыми за таким «экспериментом» поймали торрент-трекер Piratebay. Заметили неладное сами пользователи сайта – при посещении торрента нагрузка на процессоры увеличивалась практически до ста процентов.

Вирусные майнеры.

отличие отклассических вирусов, которые просто крадут ипересылают информацию скомпьютера, вирусы-майнеры используют его технические мощности. Попасть в компьютер вредоносная программа может двумя способами: вместе с различными установочными файлами (когда вирусная программа маскируется под безопасные компоненты программы или различные активационные ключи), или же в результате атаки на сервер.При ежедневном использовании компьютер работает на 20-30% своей мощности, а при чёрном майнинге машина разгоняется до 80-100%[2]. Вирусы способны сильнее навредить ПК, нежели браузерный майнинг, однако браузерным атакам подвергается гораздо больше компьютеров.

Самыми распространёнными вирусами-майнерами на сегодняшний день являются:

1. **Троян «MinerBitcoin».**

то время, как рядовой пользователь использует лишь 20% возможностей своего ПК, то данный троян способен увеличить этот показатель до 80%, а в некоторых случаях и до целых 100%. «Miner Bitcoin» пользуется не только ресурсами, но и получает доступ к данным, касающихся владельца техники. Выявить наличие такого трояна можно, прислушившись к работе кулера видеокарты: если он издаёт сильный шум, значит вы столкнулись с «Miner Bitcoin». Обычно троянская программа сопровождает документы Word либо фотографии. Чаще всего его подхватывают пользователи «Skype».

2. **«EpicScale».**

данной утилитой сталкиваются владельцы ПК, которые часто применяют «uTorrent».

3. **«JS/CoinMiner».**

данном случае речь идёт о вредоносных утилитах, которые предусматривают генерирование цифровых валют посредствам браузеров. Зачастую такими скриптами оснащаются сайты для геймеров, а также ресурсы, которые имеют потоковые видео [3].

обоих случаях программа-майнер нагружает пользовательский ПК и его видеокарту по максимуму. Есть ещё одна незначительная особенность вирусов-майнеров – обслуживающий или дополнительный сервис вируса. Сервис обеспечивает закрепление в системе компьютера основной пиратской программы, её автозапуск при включении компьютера, а также следит за безопасностью. Такой дополнительный сервис зачастую отвечает за то, чтобы программа мониторинга активности компьютера не обнаружила пирата-майнера, поэтому вовремя приостанавливает его работу. В частности, приостановка работы вируса может произойти

именно в момент запуска утилиты, например, для проверки загрузки видеокарты. Кроме того, этот же сервис проверяет наличие майнера на жёстком диске, не давая его удалить и восстанавливая его после удаления. [4]

Как правило, о том, что ПК подвергся атаке со стороны чёрных майнеров, свидетельствует его замедленная работа.Когда компьютер начинает «тормозить» при посещении конкретного ресурса, то, скорее всего, чёрные майнеры воспользовались вашим браузером. Следует уделять внимание тому, как функционирует техника на тех сайтах, которые предусматривают длительное времяпрепровождение: торент-трекеров, онлайн-игр и сайтов с фильмами. Так же чёрный майнинг неизбежно ведёт к увеличению потребления электроэнергии.

Как обезопасить себя от браузерного майнинга?На сегодняшний день есть ряд эффективных мер, которые помогут оградить ПК от вирусных атак через браузер. Среди них можно выделить:

Редактирование файла, который носит название «hosts», если известны адреса сайтов-злоумышленников;

Установка утилиты «Anti-WebMiner» и браузерного расширения «NoCoin»;

Отключение JavaScript в браузере и применение «NoScript»;

Добавление антимайнинговой защиты в «AdBlock», а также «uBlock».

Такжесуществует ряд правил пользования ПК, которые обезопасят от деятельности чёрных майнеров:

Никогда не загружайте на компьютер нелицензионные программы, приложения. Также избегайте ввода активационных ключей из сомнительных источников и никогда не применяйте непроверенные ссылки;

Если вы являетесь владельцем ПК, который изготовила компания «Apple», следует установить в настройках опцию, которая подразумевает скачивание только программных продуктов из «App Store»;

Если вы предпочитает ОС «Windows», требуется создать учётную запись и загружать компьютер только через неё;

В том случае, если ПК стал сильно «тормозить», воспользуйтесь «Диспетчером задач» (возможно, вам удастся обнаружить те самые утилиты, которые отнимают 80-90% мощностей процессора), обратитесь в сервис [3].

Литература

Википедия. Свободная энциклопедия. Майнинг. – [Электронный ресурс]. – Дата доступа – 26.02.2020

Чёрный майнинг: как зарабатывают деньги через чужие компьютеры.– [Электронный ресурс]. – Дата доступа – 26.02.2020

Чёрный майнинг: как защитить свой компьютер и не стать жертвой мошенников. – [Электронный ресурс]. – Дата доступа – 27.02.2020

Чёрный майнинг: с миру по монетке. – [Электронный ресурс]. – Дата доступа – 27.02.2020

Технологии, применяемые в Дата-центрах. Услуги, предоставляемые Дата-центрами на современном этапе

Шило Е.С.
Научный руководитель: Ковалькова И.А.
Белорусский национальный технический университет

Дата-центр, или *центр обработки данных* (*ЦОД*)– это специализированное здание для размещения серверного и сетевого оборудования и подключения абонентов к каналам сети Интернет.

Дата-центр является высокотехнологичной охраняемой площадкой, где размещаются сервера различных компаний. Проще говоря, дата-центр – это своеобразный «дом серверов».

Для хранения и обработки большого количества информации используются специализированные технические решения, мощные серверы, дисковые хранилища. Создавать и обслуживать такие технические системы самостоятельно достаточно сложно и дорого: содержание серверов требует специальных технических условий, отдельных помещений и квалифицированного персонала.

Одним из основных назначений дата-центров как раз и является создание подходящих условий для размещения таких технических решений. Дата-центрыспециализируются на размещении специализированных компьютерных устройств, предназначенных для хранения, обработки информации, а также на предоставлении клиентам каналов связи для доступа в Интернет или передачи данных.

Дата-центры обычно расположены в пределах или в непосредственной близости от узла связи или точки присутствия какого-либо одного или нескольких операторов связи. Качество и пропускная способность каналов влияют на уровень предоставляемых услуг, поскольку основным критерием оценки качества работы любого дата-центра является время доступности сервера.