Защита от криптомайнеров

Безмалый В.Ф.

Windows Insider MVP

Блокирование сценариев майнинга в браузере является важным шагом для обеспечения целостности и эффективности работы вашей системы

Как заблокировать скрипты Cryptomining в вашем веб-браузере

По мере того, как взлетела ценность криптовалют, таких как Биткойн и Монеро, появилась более зловещая тенденция. Киберпреступники увидели возможность использовать вычислительную мощность незащищенных компьютеров для майнинга криптовалюты.

Эти расчеты требуют большого количества ресурсов процессора и электроэнергии, поэтому хакеры используют сценарии майнинга в браузерах для незаконного использования компьютеров других людей (так называемый криптоджекинг), чтобы они могли бесплатно добывать криптовалюты.

Что такое криптоджекинг

Как и шифровальщики, криптомайнеры отнюдь не новое явление. Ведь примерно с 2011 года существует возможность использовать компьютерные ресурсы для майнинга биткойнов без помощи специализированного или мощного оборудования. Однако киберпреступники стали разрабатывать вредоносное ПО только после бума криптовалют в середине 2017 года.

Киберпреступники поняли, что если они заражают чужой компьютер вредоносным ПО, то могут заставить зараженный компьютер выполнять работу по майнингу, но злоумышленники получат прибыль. Ведь умножить прибыль на 1000 или 1000000 зараженных компьютеров, то очень легко понять, почему такой взлет получили вредоносные криптомайнеры.

Более того, злоумышленники решили, что могут резко увеличить прибыль, объединяя несколько типов вредоносных программ.

Фактически пользователь, перейдя по фишинговой ссылке или открывая вредоносное вложение, получает одновременно две инфекции: криптомайнинговое ПО и вымогатель. Естественно, что злоумышленник

выбирает какое ПО активировать, ведь одновременно они работать н могут. Выбор осуществляется на основе таких факторов, как аппаратная и программная конфигурация компьютера и того, какая атака окажется более прибыльной.

Как работает незаконный криптомайнинг

Для заражения компьютеров киберпреступники используют различные методы: от компрометации ПК и мобильных устройств отдельных пользователей до проникновения на популярные веб-сайты и распространения вредоносного ПО всем, кто их посещает.

Кроме того, чрезвычайно популярным методом заражения остается фишинг. В некоторых случаях используются компоненты-черви, что позволяет вредоносам атаковать по сети одну машину за другой.

Эксплойт EternalBlue, который использовался для распространения вымогателей WannaCry в глобальной эпидемии в 2017 году, до сих пор используется для распространения вредоносного криптомайнинга. Но в отличие от вымогателей, большинство жертв криптомайнинга не имеют ни малейшего представления о том, что у них крадут, кроме смутного ощущения, что их система работает не так эффективно, как раньше.

Поддельные обновления программного обеспечения — это еще один популярный метод проникновения, например, загрузка вредоносных программ, которая маскируется под законное обновление Adobe Flash Player. Другим распространенным методом является внедрение вредоносного сценария майнинга на легитимном веб-сайте или в блоке онлайн-рекламы, размещаемой на многих веб-сайтах. Когда жертва заходит на веб-сайт или ее браузер загружает онлайн-рекламу, начинается процесс криптомайнинга, который ворует ресурсы и прибыль без ведома пользователя.

Разработчики вредоносных программ Cryptomining извлекли уроки из своих ранних ошибок. Сегодня гораздо реже встречаются вредоносные программы, которые потребляют 100% мощности процессора жертвы, что приводит к заметному замедлению, которое, скорее всего, побудит пользователя заметить и предпринять корректирующие действия. В новых выпусках вредоносных программ для криптомайнинга предпринимаются более разумные меры для сокрытия их присутствия: загрузка ЦП жертвы примерно до 20 процентов, поиск времени простоя пользователя для выполнения самых ресурсоемких вычислений и т. Д. Таким образом, эти криптомайнеры могут украсть ресурсы у жертвы без обнаружения очень долгое время.

Хуже того, не нужно быть высококвалифицированным инженером-программистом, чтобы заняться незаконным майнингом. Как и в случае других наборов вредоносных программ, криптоджекинг как услугу можно приобрести всего за полдоллара США. Высокий уровень конфиденциальности и анонимности, свойственный некоторым криптовалютам, таким как Monero и Zcash, также значительно усложняет отслеживание и отлов злоумышленников.

Известные криптоджекеры

Smominru

Smominru, пожалуй, самый печально известный криптовалютный ботнет, состоящий из более 520 000 машин, которые к январю 2018 года заработали своим владельцам более 3 миллионов долларов в Monero, чему способствует умный, постоянно восстанавливающийся дизайн ботнета. Smominru был основан на EternalBlue, украденном эксплойте АНБ, который также использовался в глобальной эпидемии вымогателей WannaCry в 2017 году.

BadShell

Умные криптомайнеры, такие как BadShell, прячутся в легитимных процессах, таких как Windows PowerShell, через которые они выполняют скрытые вредоносные сценарии майнинга. Немногие традиционные антивирусные программы могут обнаружить угрозу, поскольку по умолчанию они доверяют исполняемым файлам с подписью Windows, таким как PowerShell.

Coinhive

Первоначально предназначенный и все еще используемый в качестве законного инструмента монетизации веб-сайтов, код майнинга Coinhive в настоящее время является крупнейшей в мире угрозой крипто-взлома.

MassMiner

MassMiner — интересный пример, потому что он использует много эксплойтов для различных уязвимостей в одной полезной нагрузке. Использование неисправленных ошибок в Oracle WebLogic, Windows SMB и Apache Struts принесло криптовалюте Monero на сумму около 200 000 долларов для создателей MassMiner.

Prowli

Prowli — это крупная известная бот-сеть из более чем 40 000 зараженных веб-серверов, модемов и других устройств Интернета вещей (IoT), которые используются для майнинга криптовалюты и перенаправления пользователей на вредоносные сайты. Часть Prowli — это червь с перебором паролей, способствующий распространению майнера Monero. В некоторых случаях ботнет также устанавливает бэкдоры на зараженные системы.

WinstarNssMiner

В течение трех дней в мае 2018 года WinstarNssMiner заразил более полумиллиона систем. Когда этот криптоджер обнаруживает эффективное антивирусное программное обеспечение на своей целевой машине, он остается бездействующим, активируя себя только в системах со слабой защитой. Хуже того, если вы попытаетесь удалить WinstarNssMiner, это приведет к аварийному завершению работы зараженной системы.

Стоимость криптомайнинга

Во-первых, нам нужно понять природу криптовалюты. Эти цифровые валюты основаны на криптографии (также называемой алгоритмами хэширования), которая записывает финансовые транзакции. Доступно только определенное количество хэшей, которые помогают установить относительную ценность каждой единицы.

Создание новых единиц криптовалюты предполагает решение сложной математической задачи. Первый человек, который решит проблему, получит деньги за свои усилия в этой криптовалюте. Это означает, что законные криптомайнеры должны инвестировать в серверные фермы для обеспечения вычислительной мощности, огромного количества электроэнергии и систем охлаждения, которые помогают поддерживать эффективность майнинга при сокращении количества.

Распространение cryptomining

Скрипты майнинга в браузерах не являются вредоносными. Некоторые веб-сайты экспериментируют с ними в качестве возможного источника дохода, который заменит онлайн-рекламу. Например, одним из первых веб-сайтов, попробовавших такой подход, был Quartz . Идея распределить усилия по шифрованию на пользовательские компьютеры в обмен на доступ к веб-сайту казалась разумной, тем более что пользователь будет проинформирован и попросит согласиться на сделку.

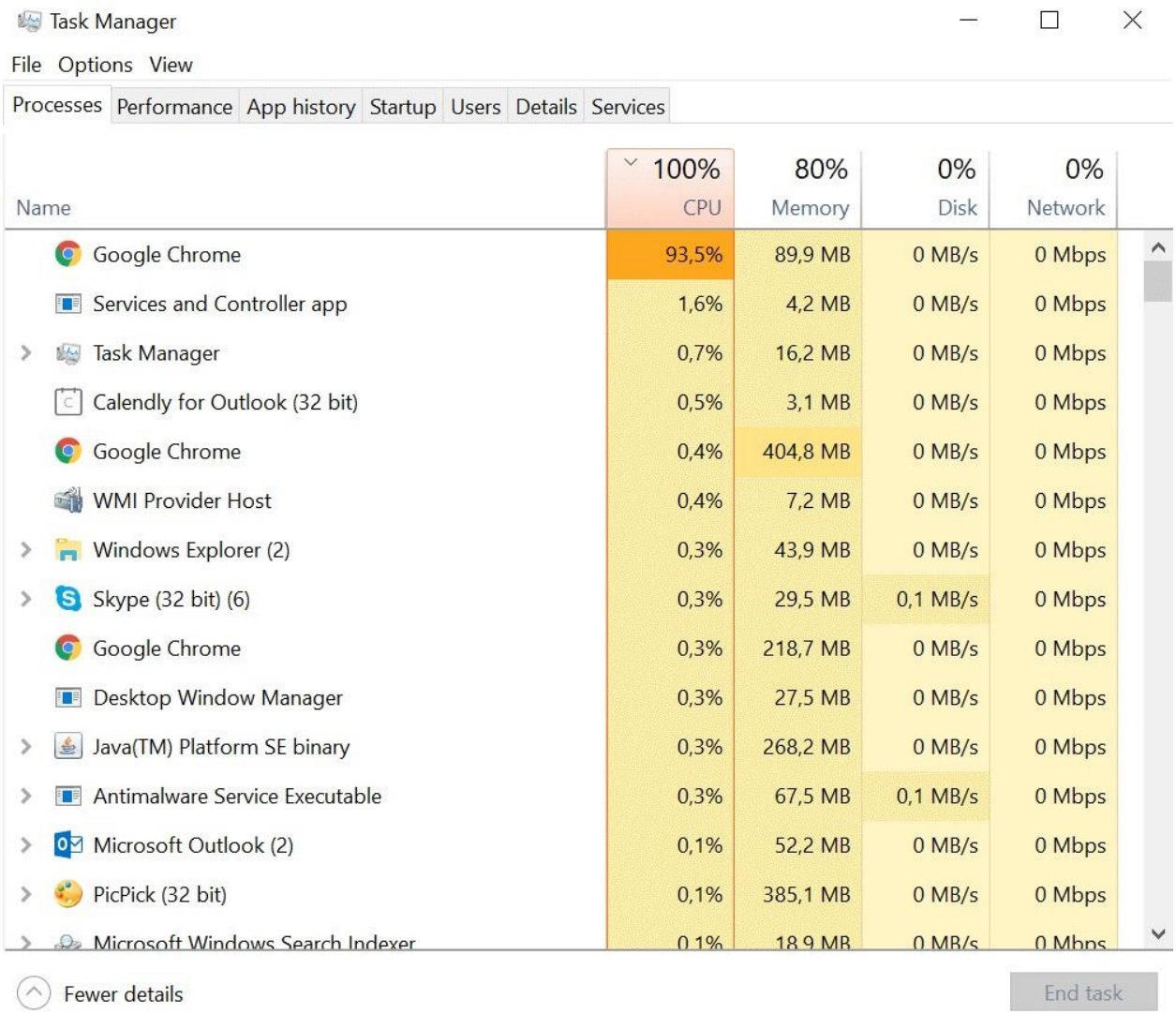
К сожалению, этот подход был использован преступниками. Вместо того чтобы инвестировать в инфраструктуру, необходимую для законного

криптомайнинга, они рассматривают сценарии майнинга браузеров как способ избежать этих затрат. И будь то Coinhive, предлагающий инструменты майнинга Monero, которые вы вставляете на веб-сайт, или альтернативы Coinhive, такие как EObot и Awesome Miner, которые используют браузерные майнеры Bitcoin, у преступников есть инструменты, которые всегда под рукой.

Как определить, был ли ваш компьютер заражен

Учитывая нагрузку вашего процессора, если ваш компьютер неожиданно стать работать медленнее или батарея разряжается особенно быстро, вы могли быть взломаны. Как вы можете это доказать?

Откройте **диспетчер задач Windows** или **MacOS Activity Monitor** и нажмите **«Процессы».** Если вы видите, что ваш браузер потребляет слишком много ресурсов, вы можете закрыть его и перезапустить. К сожалению, это не говорит вам, на каком сайте запускался скрипт майнинга браузера.



К сожалению, сложно это заметить. В то время как старые сценарии максимально загружали процессор, новые сценарии криптомайнинга нагружают максимум до 20 процентов, что затрудняет их обнаружение.

Остановка криптомайнинга в браузерах

Несмотря на то, что идентифицировать подобные атаки стало намного сложнее, существуют шаги, которые вы можете предпринять, чтобы автоматически уменьшить вашу уязвимость к атакам через браузер.

Развертывание расширений браузера

Большинство популярных веб-браузеров сегодня включают в себя расширения, которые могут помочь остановить атаки криптомайнинга в сети. Они могут включать как решения, разработанные разработчиком браузера, так и расширения с открытым исходным кодом, которые могут быть добавлены. Например, решения No Coin и MinerBlocker отслеживают подозрительную активность и блокируют атаки, и оба имеют расширения, доступные для Chrome, Opera и Firefox.

Ad-Blocker Software

Учитывая взрыв вредоносного ПО криптомайнинга, многие блокировщики рекламы теперь включают в себя блокиратор Coinhive, который отфильтровывает запуск сценария в вашем браузере. Если у вас установлен блокировщик рекламы, вам нужно выбрать этот блокировщик скриптов.

Отключить JavaScript

Если вы хотите полностью блокировать определенные атаки, большинство браузеров разрешат отключить JavaScript — хотя многие легальные сайты по-прежнему используют JavaScript, поэтому отключение может вызвать проблемы.

Блокировать домены

Вы также можете заблокировать определенные домены, которые вы подозреваете в криптомайнинге. Просто откройте браузер, найдите раскрывающийся список «Настройка» и заблокируйте URL-адрес. Чтобы заблокировать Coinhive, вы можете скопировать / вставить *https://coin-hive.com/lib/coinhive.min.js* в текстовое поле.

Заключение

Блокирование сценариев майнинга в браузере является важным шагом для обеспечения целостности и эффективности работы вашей системы, и совсем не сложно предпринять шаги, необходимые для защиты вашего компьютера.

Однако стоит учесть, что сегодня существует много криптоджекеров, не основанных на браузерах. Вместо этого они представляют собой отдельные программы, которые напрямую заражают вашу систему.

Надеюсь, хоть антивирусное ПО у вас лицензионное? Безусловно, сегодня можно применять и бесплатное антивирусное ПО, широко представленное на рынке. Но хватит ли вам бесплатного антивируса? Не думаю. Хотя, безусловно, решать вам!