Опубликовано на Швейцария: новости на русском языке (https://nashagazeta.ch)

Как защититься от скрытого майнинга? | Comment se protéger du cryptojacking?

Auteur: Заррина Салимова, Берн , 15.02.2019.

Фото: Christopher Gower, Unsplash

Хакеры могут использовать компьютеры других пользователей для создания криптовалюты. Этот вид киберугроз называется криптоджекингом и значительно замедляет производительность компьютера жертвы.

|

Des hackers peuvent utiliser votre ordinateur pour créer de la cryptomonnaie. Cette forme

de menace cybernétique, le cryptojacking, met en péril la performance de l’ordinateur.

Comment se protéger du cryptojacking?

В конце января пользователи Youtube во многих странах стали жертвами компьютерных пиратов, сообщает Le Temps. В рекламу, которая отображается при воспроизведении некоторых видео-роликов, был встроен специальный скрипт, который начинал использовать, без согласия пользователей, мощности их компьютеров для создания криптовалюты. Этот метод известен как криптоджекинг (англ.: cryptojacking) или скрытый майнинг.

Криптовалюта, в отличие от евро, рублей или франков, не печатается эмиссионным центром, а создается в результате сложных компьютерных операций. Для майнинга цифровых денег создаются целые криптофермы – промышленные помещения с оборудованием, генерирующим криптовалюту. Криптоферма потребляет электричество, нуждается в охране, а также системах охлаждения, вентиляции и пожаротушения. Хакеры не хотят за все это платить и предпочитают с помощью вредоносных программ воровать электричество и вычислительные мощности у других. Причем им теперь даже не нужно взламывать компьютер пользователя и устанавливать на него вредоносное программное обеспечение. Программу-майнер можно интегрировать прямо в веб-страницу: она будет запускаться и воровать вычислительные мощности вашего ПК, как только вы зайдете на зараженный сайт.

Примером браузерного майнинга может служить Coinhive – появившаяся в сентябре 2017 года программа для создания криптовалюты монеро (эспер. monero – монета). Она может устанавливаться как самими владельцами сайта для его монетизации, так и пиратами, которые используют эту программу для анонимного майнинга, встраивая ее в приложения или на веб-страницы. Хакеров интересуют, прежде всего, популярные сайты с большим количеством пользователей. Coinhive, например, была установлена на американском сайте Politifact.com, который проводит проверку достоверности высказываний политиков и, по оценке аналитического сервиса Similar Web, имеет около 6 млн посещений в месяц. Администраторы сайта заверили, что вредоносный код был интегрирован третьей стороной, и пообещали принять необходимые меры для защиты сайта. Кроме того, майнер могут внедряться через публичные Wi-Fi-точки: любители бесплатного интернета могут и не знать, что за подключение придется заплатить мощностями собственного компьютера или смартфона.

Главным признаком того, что ваш компьютер используется для скрытого майнинга, может быть резкое падение его производительности. В браузере Chrome, например, можно проверить, какая из вкладок потребляет больше всего ресурсов. Если на нее приходится более 60% всей мощности, то ее лучше закрыть. Эксперты по компьютерной безопасности советуют установить браузерные расширения, блокирующие вредоносные скрипты, например, NoScript, No Coin, Antiminer, minerBlock или Mining Blocker.

Если программа-майнер попала на ваш компьютер, то избавиться от нее помогут антивирусы. Стоит отметить, что в диспетчере задач программы-майнеры могут «мимикрировать» под обычные процессы. Некоторые антивирусы, например, Kaspersky, могут не блокировать и не удалять майнеры по умолчанию, но включать их в категорию Riskware, т.е. «ПО, которое само по себе легально, но при этом может быть использовано в зловредных целях».

И не забывайте о простейших правилах безопасности в сети: регулярно обновляйте антивирусное ПО, не кликайте на подозрительные рекламные ссылки и не переходите по ссылкам, присланным от незнакомого отправителя.

Статьи по теме
[В Швейцарии появилось практическое руководство по использованию криптовалют]
[В Швейцарии появится своя криптовалюта?]
[В Швейцарии действует новый вирус-вымогатель]
[Швейцарцы также пострадали от хакеров Anonymous]
[Швейцария под прицелом хакеров]

Source URL:
https://nashagazeta.ch/news/la-vie-en-suisse/kak-zashchititsya-ot-skrytogo-mayninga