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

Килессо Г.Д.
Научный руководитель: ст. преподаватель Ковалькова И.А.
Белорусский национальный технический университет

Стоит задуматься о том, что владелец устройства может стать жертвой чёрного майнинга. Поэтому очень важно, чтобы пользователи знали о процессе майнинга и также об особенностях чёрного майнинга, чтобы не стать жертвами мошенников, которые используют ресурсы компьютеров других людей.

Чтобы добывать криптовалюту нужно использовать оборудование, которое может использовать технологию блокчейн. Это определенная последовательность блоков, в которых содержится информация. Из этих блоков в будущем и будет формироваться майнер.

Так называемая «валюта» измеряется в цифровых монетах и содержит зашифрованную информацию, которая защищает от мошенничества и подделки.

На сегодняшний день, чтобы добывать криптовалюту, требуется большое количество энергии. Также цена на электроэнергию влияет на выбор криптовалюта, которой осуществляется майнинг, при помощи специального оборудования. Так же нужно специализированное помещение с низкой температурой в нём. Это делается для охлаждения оборудования.

Учёные из Великобритании определили, что потребление энергии на майнинг-фермах составляет около 121,36 тераватт-часов за год

(ТВтч), что значительно превышает использование энергии в Аргентине, Нидерландах и Объединённых Арабских Эмиратах. [1]

Важно отметить, что появилась тенденция по установке ферм в заброшенных зданиях, сараях, заброшенных фермах. При этом также используются самодельные устройства для подключения к сети.

Чёрный майнинг – это нелегальный способ добычи криптовалюты, который включает использование видеокарт или другого устройства без разрешения владельца.

Существует два основных способа незаконной добычи цифровых монет с использованием чужих устройств – это майнинг в браузере и вирусы-майнеры.

1.Браузерный майнинг

Это метод добычи криптовалюты, известный как майнинг в браузере, осуществляется непосредственно внутри браузера с использованием языка программирования. Важно отметить, что посещение вредоносных веб-

сайтов может нанести вред вашему компьютеру, так же как и в случае с криптовалютами. Чтобы майнер смог работать вам нужно находиться на сайте, где присутствует вирус.

2.Вирусы-майнеры

Вирус-майнер может заразить компьютер, если пользователь перейдёт по ссылке или установит небезопасное программное обеспечение.

Самые распространенные типы вирусов-майнеров:

− web-майнер;

− простой;

− скрытый.

Web-майнер может располагаться в расширении браузера. Если он присутствует на компьютере, то производительность будет уменьшаться.

Скрытый майнер активно избегает обнаружения системой. Он блокирует работу антивирусов и отключается во время использования компьютера. [2]

Простой вирус-майнер – это вредоносная компьютерная программа, которая работает в автоматическом режиме и никак не уведомляет пользователей о добычи монет.

Рассмотрим программы, используемые злоумышленниками:

1. Miner Bitcoin

Обычно пользователь, который использует компьютер, наблюдает нагрузку системы на 20%, но, при наличии данного вируса, нагрузка на компьютер может возрасти до 80% или даже 100%.

2. EpicScale

Программа использует ресурсы компьютеров других пользователей для решения своих задач.

3. JS/CoinMiner

Данная программа является программным обеспечением. Она позволяет добывать криптовалюту с использованием ресурсов процессора браузеры компьютеров.

Чтобы избежать заражения вирусами-майнерами, рекомендуется соблюдать следующие меры:

1. Избегайте скачивания различных приложений.

2. Установите антивирусное программное обеспечение. Помните, что регулярное обновление антивируса до последней версии важно для эффективной защиты.

3. Проверяйте производительность вашего компьютера.

4. При необходимости обратитесь к специалисту.

Будьте бдительны и следите за безопасностью вашего компьютера!

Литература

1. Сколько мирового электричества тратят на майнинг. [Электронный ресурс] Режим доступа: https://devby.io/news/maining.amp, свободный.

2.Чёрный майнинг.[Электронный ресурс] Режим доступа: https://lifehacker.ru/chernyj-majning/, свободный.

УДК 338.2

ИСТОРИЯ КИБЕРУГРОЗ И КИБЕРБЕЗОПАСНОСТИ: ОСНОВНЫЕ ЭТАПЫ

Литвинюк К.В.
Научный руководитель: ст. преподаватель Ковалькова И.А.
Белорусский национальный технический университет

Кибербезопасность – это защита компьютерных систем от кражи или повреждения их оборудования, программного обеспечения или данных, а также от отказа или нарушения предоставляемых ими услуг. История киберугроз начинается с первых шагов информационных технологий, когда создаваемые вирусы были простыми и не представляли серьезной угрозы. Однако со временем, как и технологии, методы кибератак стали усложняться. Это способствовало постоянному развитию методов кибербезопасности, направленных на нейтрализацию угроз. Понимание этапов развития кибербезопасности помогает осознавать текущие вызовы и прогнозировать будущие угрозы.

Ранние годы развития киберугроз и кибербезопасности, охватывающие 1970-е и начало 1980-х годов, являются ключевым периодом в истории информационных технологий, отмеченным зарождением первых компьютерных вирусов и началом осознания необходимости защиты информационных систем. Этот этап характеризуется началом широкого использования компьютеров не только в академических и военных целях, но и в коммерческих организациях, а также появлением первых сетевых технологий, которые способствовали быстрому распространению вредоносного программного обеспечения.

Одним из первых вирусов, оказавших заметное влияние на развитие кибербезопасности, был Creeper, появившийся в 1971 году. Эта экспериментальная программа, созданная Реем Томлинсоном, могла самостоятельно перемещаться по сети ARPANET, выводя на экраны пользователей сообщение: "I'm the creeper, catch me if you can!" В ответ на эту угрозу был