Міністерство освіти і науки України
Сумський державний університет
Наукове товариство студентів, аспірантів,
докторантів і молодих вчених СумДУ

ПЕРШИЙ КРОК У НАУКУ

Матеріали
IX студентської конференції
(Суми, 25 лютого 2018 року)

Суми
Сумський державний університет
2018

ПРОТИДІЯ ПРОГРАМНИМ СИСТЕМАМ БРАУЗЕРНОГО ТА МОБІЛЬНОГО КРИПТОВАЛЮТНОГО МАЙНІНГУ

Осадчий В.М, *студент*; ННІ БТ "УАБС" СумДУ, гр. ЕК-61а

Разом з популярністю криптовалют, з'явився новий вид кібершахрайства – прихований браузерний та мобільний майнінг, який може вразити користувачів комп'ютерів та смартфонів, тому захист від таких систем є актуальним завданням.

Метою дослідження є аналіз систем браузерного та мобільного майнінгу та розробка рекомендацій щодо протидії таким програмам.

В Україні приховане добування криптовалют за рахунок відвідувачів сайтів було виявлено на популярних ресурсах Football.ua, Korrespondent.net, iSport.ua. Браузерний майнінг активується під час відвідування веб-сторінки, в скрипті якої записаний шкідливий програмний код, що використовує ресурси комп'ютера для добування криптовалют. Наслідком цього є сповільнення роботи пристрою, підвищення його енергоспоживання, швидкий знос електронних компонентів. При мобільному майнінгу також підвищується ймовірність виведення смартфону з ладу. Головними ознаками прихованого майнингу під час відкриття веб-сторінки зі шкідливим скриптом є сповільнення роботи пристрою, значний шум системи охолодження та підвищений рівень навантаження процесору.

Для захисту комп'ютера від браузерного майнінгу пропонуємо: встановити спеціальні розширення для браузеру, які блокують роботу шкідливих скриптів (наприклад, NoCoin); відключити JavaScript у браузері та вмикати його лише на перевірених сайтах; слідкувати за рівнем навантаження процесора та закривати веб-сторінки, які викликають підвищення до рівня 80-100%; використовувати останню версію браузеру Opera, який містить вбудований захист від майнінгу; додати домени майнингу в файл hosts. Щоб вберегти смартфон від майнінгу потрібно в налаштуваннях пристрою заборонити встановлення додатків з не перевірених джерел та користуватися програмами тільки з PlayMarket або AppStore.

Запропоновані рекомендації дозволять ефективно протидіяти системам браузерного та мобільного криптовалютного майнінгу.

Керівник: Яценко В.В, *доцент*