УДК 004.056.2,004.5,336.744,339.72

Вікторія Олександрівна КОВТУН,
курсантка 2 курсу факультету № 4
Харківського національного університету внутрішніх справ

Петро Сергійович КЛІМУШИН,
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

ПРИХОВАНИЙ МАЙНІНГ КРИПТОВАЛЮТИ Й ОБМЕЖЕННЯ БРАУЗЕРНОГО КРИПТОДЖЕКІНГУ

Зазвичай, ціллю кіберзлочинців є ресурси жертви, під якими мається на увазі не тільки конфіденційна інформація, а й потужності машин, що є носієм цієї інформації. Особливо гострою проблема крадіжки потужності робочих машин стала з появою криптовалют. Сьогодні жертвами криптоджекінгу стали мільйони звичайних користувачів і кожна п'ята бізнес-компанія в світі.

Проте не лише класичний криптоджекінг несе велику загрозу. Зараз популярності набуває ще один вид прихованого майнінгу – криптоджекінг на веб сторінках. Прихованих майнерів уже виявляли на YouTube, в тисячах інтернет-магазинах і в додатках для Android. Скрипти, що видобувають криптовалюту, ховаються під рекламою та за допомогою диспетчера тегів Google інтегровані в код безлічі сайтів, а популярні CMS і зовсім захлеснула хвиля атак, метою яких є саме встановлення майнінгових скриптів [1, с. 2].

Криптоджекінг набрав катастрофічних наслідків у наш час. На сьогодні кіберзлочинці дуже швидко знайшли можливість добувати криптовалюти, не витрачаючи при цьому майже ніяких ресурсів. Тому актуальність дослідження полягає в тому, щоб знизити випадки прихованого майнінгу.

Метою дослідження є висвітлення методів для виявлення прихованого браузерного майнингу.

Криптоджекінг – це несанкціоноване використання обчислювальних потужностей (комп'ютерів) інших людей для видобутку криптовалюти.

Браузерний криптоджекінг у свій час став проблемою, яку неможливо було ігнорувати. Тож усі браузери при наступному обновленні вжили заходи для обмеження майнингу на вебсторінках. Найбільш жорстку політику щодо прихованого браузерного майнінгу ввела Opera. Цей браузер повністю блокує будь-яку активність, що стосується криптоджекінгу, тому справедливо вважається найбільш захищеним від цього виду атак.

Природньо, що за обмеження браузерного криптоджекінгу відповідають браузерні розширення. Існує три підходи для виявлення прихованого браузерного майнингу.

Перший метод полягає у моніторингу так званого чорного списку. Якщо адреса сайту збігається з адресою з чорного списку, вважається, що сайт користується прихованим браузерним майнінгом. За підрахунками експертів цей метод дозволяє виявити криптоджекінг у 58% випадків.

Другий підхід передбачає пошук у коді підозрілих бібліотек. Якщо входження відбулось, вважається, що сайт заражений криптоджекінгом. За підрахунками, цей метод дозволяє виявити близько 23% прихованого майнінгу. Проте на відміну від першого методу він дозволяє виявляти нові сторінки, заражені криптоджекінгом. Доведено, що використання обох цих методів у зв'язці дає результат у 67%. Реалізація цих методів полягає, головним чином, у javascript-функції indexOf [2, с. 5].

Третій спосіб полягає у тому, що розширення слідкує за наявністю підозрілої поведінки машини. Підозрілим, наприклад, вважається випадок, коли різко збільшується навантаження на процесор. Цей метод є ефективнішим аніж перші два, проте займає набагато більше часу. Тому використовується, зазвичай, тільки у великих антивірусних продуктах або виключно для пошуку нових сторінок, заражених криптоджекінгом.

Взагалі розширення Google Chrome, що використовуються для обмеження криптоджекінгу поділяються на два види. Перший – це великі антивіруси, в яких функція боротьби із прихованим майнінгом є лише однією з опцій. До таких відносяться такі додатки, як Avast та McAfee. Інші – навпаки вузькоспеціалізовані, і обмеження криптоджекінгу для них є основною функцією. До таких відносяться noCoin, MINEBlock, Coin-Hive, AntiMiner. На жаль, деякі з них не обновлювались на протязі 2-3 років.

Таким чином, у результаті досліджень проаналізовано ефективність методів виявлення прихованого браузерного криптоджекінгу та визначено застосування кожного з них. Метод чорного списку та метод, який виконує пошук шкідливих бібліотек у коді програми застосовується беспосередньо для виявлення прихованого браузерного криптоджекінгу. Тертій метод, що відслідковує підозрілу поведінку, зазвичай, використовується для пошуку нових вебсторінок, що заражені бібліотекою для прихованого майнінгу криптовалюти.

Проаналізувавши вже існуючі рішення, було виявлено деякі проблеми. По-перше, усі програмні засоби одразу блокують сайт із браузерним криптоджекінгом, не враховуючи те, що деякі вебсторінки дають можливість на вибір: або погодитися на узгоджений криптоджекінг, або ж продивлюватися рекламні пропозиції. По-друге, на сьогоднішній день не було знайдено сервісів, які б давали можливість виявляти прихований криптоджекінг у розширеннях браузера.

Звідси випливає, що актуальним завдання подальших досліджень є розробка розширення браузера, яке можливо використовувати разом з іншими рішеннями для обмеження браузерного криптоджекінгу [3].

Список бібліографічних посилань

1. Eskandari S., Leoutsarakos A., Mursch T., Clark J. A First Look at Browser-Based Cryptojacking. University College London, 2018. 9 p.
2. Hong G., Zhang L., Yan M. How You Get Shotinthe Back: A Systematical Study about Cryptojacking in the Real World. URL.: http://www.cs.ucr.edu/~zhiyunq/pub/ccs18_cryptojacking.pdf (дата звернення: 26.04.2020).
3. Ілляшенко О. М. Виявлення прихованого криптоджекінгу на веб-сторінках : дипломна робота. Київ : Нац. тех. ун-т України «Київський політехнічний інститут імені Ігоря Сікорського», 2019. 57 с.

Одержано 27.04.2020