DOI: 10.37791/2687-0649-2023-18-1-96-110

Программное обеспечение обнаружения «скрытых майнеров» в браузерной среде

Б.Р. Камалов[1*]***, М.В. Тумбинская***[1]

[1]*Казанский национальный исследовательский технический университет им. А.Н. Туполева, Казань, Россия*

[*]*1bulat_kamalov_1999@mail.ru*

Аннотация. В настоящее время распространение получает новый тип угроз информационной безопасности – скрытый майнинг, использующий вычислительные ресурсы пользователей через браузеры. Вредоносное программное обеспечение на основе файлов WebAssembly несанкционированно использует вычислительные ресурсы пользователей компьютерных систем. Существующие способы обнаружения «скрытых майнеров» в браузерной среде основаны: на алгоритмах динамического анализа, однако имеют ряд ограничений, например требуется, чтобы вредоносное программное обеспечение для скрытого майнинга работало в течение определенного периода времени, характеризуются большим количеством ложных срабатываний; алгоритмах работы расширений браузера, которые используют черные списки для предотвращения несанкционированного доступа к браузерной среде пользователей, однако злоумышленники часто меняют имена своих доменов и др. Актуальность использования специальных средств защиты от браузерных криптомайнеров не вызывает сомнений. Целью данного исследования является повышение уровня защищенности браузерной среды пользователей компьютерных систем. Достижение поставленной цели возможно путем решения главной задачи – своевременное автоматизированное обнаружение «скрытых майнеров» в браузерной среде и предотвращение несанкционированного майнинга. В статье описано программное обеспечение, которое не зависит от используемого браузера или операционной системы, устойчиво к попыткам обхода защиты со стороны злоумышленников и позволит пользователям достоверно распознавать «скрытых майнеров» и тем самым повысить уровень информационной безопасности компьютерной системы. В основу программного обеспечения заложены алгоритмы классификации, реализуемые на базе сверточной нейронной сети. Результаты исследования и экспериментальные данные показали, что в результате апробации программного обеспечения точность распознавания «скрытых майнеров» в браузерной среде составляет 91,37%.

Ключевые слова: скрытый майнинг, программное обеспечение, браузерный криптомайнер, уязвимость, злоумышленник, угроза

Для цитирования: *Камалов Б.Р., Тумбинская М.В.* Программное обеспечение обнаружения «скрытых майнеров» в браузерной среде // Прикладная информатика. 2023. Т. 18. № 1. С. 96–110. DOI: 10.37791/2687-0649-2023-18-1-96-110

Software for detecting “hidden miners” in a browser environment

B. Kamalov[1*], ***M. Tumbinskaya***[1]
[1]*Kazan National Research Technical University named after A. N. Tupolev, Kazan, Russia*
[*]*1bulat_kamalov_1999@mail.ru*

Abstract. Currently, a new type of information security threat is spreading – hidden mining, which uses the computing resources of users through browsers. Malicious software based on WebAssembly files unauthorizedly uses the computing resources of users of computer systems. The existing methods for detecting “hidden miners” in the browser environment are based on: dynamic analysis algorithms, however, they have a number of limitations, for example, it is required that malicious software for hidden mining work for a certain period of time, they are characterized by a large number of false positives; algorithms of browser extensions that use blacklists to prevent unauthorized access to the user’s browser environment, however, attackers often change their domain names, etc. The relevance of using special protection tools against browser-based cryptominers is beyond doubt. The purpose of this study is to increase the level of security of the browser environment of users of computer systems. Achieving this goal is possible by solving the main task - the timely automated detection of “hidden miners” in the browser environment and the prevention of unauthorized mining. The article describes software that does not depend on the browser or operating system used, is resistant to attempts to circumvent protection by intruders, will allow users to reliably recognize “hidden miners”, and increase the level of information security of a computer system. The software is based on classification algorithms implemented on the basis of a convolutional neural network. The results of the study and experimental data showed that as a result of testing the software, the recognition accuracy of “hidden miners” in the browser environment is 91.37%.

Keywords: hidden mining, software, browser-based cryptominer, vulnerability, intruder, threat

For citation: Kamalov B., Tumbinskaya M. Software for detecting “hidden miners” in a browser environment. *Prikladnaya informatika*=Journal of Applied Informatics, 2023, vol.18, no.1, pp.96-110 (in Russian). DOI: 10.37791/2687-0649-2023-18-1-96-110

Введение

Рыночный спрос увеличил коммерческую ценность криптовалют, каждая из которых предлагает механизмы подключения к сети Proof-of-Work (PoW) с помощью системного программного обеспечения (ПО), условно-бесплатного ПО или вебскрипта [1]. Легкость подключения к сети конкурентов в области криптообработки позволяет злоумышленникам несанкционированно использовать чужие вычислительные машины (подобные атаки называются «скрытый майнинг», или «криптоджекинг») [2].

Атаки скрытого майнинга можно разделить:

- на майнинг на основе двоичных файлов – выполняется с помощью вредоносных программ, доставляемых через спам, наборы эксплойтов или «трояны». Как только устройство заражено, оно загружает и запускает двоичный (исполняемый) файл майнинга. Вредоносное ПО для криптомайнинга обычно представляет собой вариант легитимного клиента для майнинга с открытым исходным кодом, с настраиваемыми параметрами конфигурации [3];