и найдем стационарное решение c_{1s}, соответствующее положению равновесия, которое совпадает с (8).

Рассмотрим отклонение от положения равновесия

$$c_1 = c_{1s} + x(t) \qquad (17)$$

Подставим формулу (17) в уравнение (15). Учтем, что c_{1s} удовлетворяет уравнению (16). В результате получим уравнение возмущенного движения

$$\frac{dx}{dt} = -(k_1 + k_2)\, x \qquad (18)$$

Приравняем нулю производную в уравнении (18) и получим частное решение

$$x = 0, \qquad (19)$$

которое отвечает положению равновесия.

Исследуем устойчивость положения равновесия (19), которое соответствует стационарному состоянию уравнения (15). Выберем в качестве функции Ляпунова функцию

$$V(x) = \frac{1}{2}\, x^2. \qquad (20)$$

Функция (20) положительно определенная. Производная функции в силу уравнения (18) равна

$$\frac{dV}{dt} = -(k_1 + k_2)\, x^2 \qquad (21)$$

Производная (21) определенно отрицательна. Из теоремы Ляпунова об асимптотической устойчивости невозмущенного движения [1,2] следует, что положение равновесия (19) асимптотически устойчиво.

СПИСОК ЛИТЕРАТУРЫ

1. Вольтер Б.В. Устойчивость режимов работы химических реакторов / Вольтер Б.В., Сальников И.Е. – Москва: "Химия", 1981. – 200 с.

2. Меркин Д.Р. Введение в теорию устойчивости движения / Меркин Д.Р. – Москва: "Наука", 1987. – 304 с.

УДК 004.032.26 : 004.056.5 : 004.492.3

Черниговский Александр Валерьевич,
аспирант кафедры «Вычислительные машины, комплексы, системы и сети»,
ФГБОУ ВО «Ангарский государственный технический университет»,
тел. 89041112385, e-mail: chernigovsky.alex@gmail.com
Кривов Максим Викторович,
к.т.н., доцент, зав. кафедрой «Вычислительные машины, комплексы, системы и сети»,
ФГБОУ ВО «Ангарский государственный технический университет»,
тел. 89025614935, e-mail: vmk@angtu.ru

ПРОБЛЕМА МАЙНИНГА В КОРПОРАТИВНОЙ СРЕДЕ

Chernigovskiy A.V., Krivov M.V.

THE PROBLEM OF MINING IN THE BUSINESS ENVIRONMENT

Аннотация. *В статье рассмотрено явление майнинга и связанные с ним проблемы, в особенности проблема информационной безопасности. Отдельное внимание уделено проблеме криптоджекинга в условиях корпоративной сети. Рассмотрены существующие способы ее решения. Выявлено, что наиболее перспективным в этом плане будет централизованное решение, основанное на методах машинного обучения.*

Ключевые слова: *майнинг, криптоджекинг, искусственные нейронные сети, информационная безопасность.*

Abstract. *In this paper we discuss the phenomenon of mining and the problems associated with it. In particular, much attention is considered to the problem of information security. Special attention is paid to the problem of cryptojacking in a corporate network. The existing methods of its solution are considered. It was revealed that the most promising in this regard will be a centralized solution based on machine learning methods.*

Keywords: *mining, cryptojacking, artificial neural networks, cyber security.*

В 2008 году в статье [1] впервые была описана концепция криптовалюты, которая базировалась на технологии блокчейна. По сути, блокчейн представляет собой реестр транзакций, записанный в виде цепочки последовательных блоков. Каждый блок в ней имеет свой порядковый номер и представляет собой хэшированную (зашифрованную) информацию о текущем блоке и хэш-сумму предыдущего блока (проверка на правильность блока). Изменение хэш-суммы блока приводит к изменениям хэш-сумм всех последующих блоков, при этом предыдущие блоки остаются неизменными.

Особенностью данной технологии является то, что такая система транзакций является децентрализованной и не зависит от финансовых регуляторов. Именно эта концепция была взята за основу при формировании первой криптовалюты – Bitcoin, которая появилась уже в 2009 году.

С этого момента возникла совершенно новая отрасль – майнинг, целью которой стало использование вычислительных мощностей отдельных компьютеров (ПК) для нахождения хэш-суммы блока. С учетом того, что подобные вычисления достаточно сложны, и их сложность постоянно увеличивается, майнеры стали объединять свои мощности в серверы-координаторы – пулы – с тем, чтобы ускорять расчеты путем распараллеливания вычислений между всеми участниками пула. В случае расшифровки хэш-суммы блока пул получает комиссию в виде криптовалюты, которая определенным образом распределяется между участниками, внесшими вклад в данную расшифровку. Таким образом, не только поддерживалась работоспособность сети криптовалюты, но и появлялась возможность добывать новые блоки, за которые назначалось вознаграждение майнерам, первым нашедшим новый блок.

Впоследствии стали появляться и другие виды криптовалюты – альткоины. Они были основаны на той же концепции, что и первая криптовалюта, но использовали улучшенные алгоритмы и технологии. В отличии от Bitcoin, добыча которых возможна только на специальных интегральных устройствах (ASIC), создатели ряда криптовалют напротив сознательно делали в алгоритмах ограничения, позволяющие использовать для майнинга вычислительные мощности графических процессоров (GPU) или только центрального процессора (CPU) [2]. Таким образом, авторы добивались привлечения большего числа пользователей для добычи выбранных альткоинов.

С развитием блокчейн-технологии, простотой настройки и доступностью программного обеспечения для добычи криптовалюты, майнинг стал широко распространен, а в 2017 году вместе с ростом цен на криптовалюту превратился в общемировой тренд. В 2021 году произошел очередной бум майнинга. При этом наблюдается рост не только объемов добычи криптовалюты, но и рост числа самих криптовалют – по данным [3] на октябрь 2021 года их известно более 6000. На сегодняшний день одними из самых распространённых помимо Bitcoin являются: Etherium, Litecoin, Ripple, Dogecoin, Monero и ряд других альткоинов [4].

Сам по себе майнинг не является криминальным или асоциальным видом деятельности. По своим принципам работы его можно сравнить с предпринимательством, который использует вычислительные мощности компьютеров для получения финансовой выгоды. Асоциальным видом деятельности майнинг стал считаться вследствие того, что в ряде регионов подключение майнинговых «ферм» к электрическим сетям реализуется незаконными способами, а это приводит, в том числе, к угрозе пожара и большому экономическому ущербу поставщиков электроэнергии [5].

Еще одна незаконная сторона майнинга – это использование недобросовестными сотрудниками вычислительных ресурсов организации для излечения личной выгоды и прибыли [6]. Такие действия могут привести к более быстрому износу оборудования, а также к дополнительным финансовым затратам на его обслуживание и на электроэнергию [7]. Кроме того, подобные действия могут подорвать систему безопасности организации, что может быть причиной компрометации системы и впоследствии привести к утечке информации. Таким образом, открывается иная сторона угрозы майнинга – угроза информационной безопасности [8].

В этой области более серьезную опасность в последние годы представляет так называемый криптоджекинг. Под данным термином понимают незаконное использование вычислительных ресурсов ПК пользователя без его ведома с целью добычи криптовалюты для владельца посещаемого веб-ресурса. Изначально технология майнинга через брау-

зер продвигалась сайтами как альтернатива монетизации рекламных вставок. Однако сейчас это стало одной из самых быстрорастущих угроз кибербезопасности в Интернете. В данном случае криптоджекинг-атака рассматривается не только как угроза незаконной добычи криптовалюты, но и как возможность скомпрометировать пользователя или организацию. Аналитики отмечают, что подобный всплеск активности криптоджекинга в настоящее время стал повсеместной проблемой. По данным [9] за 2018 год количество сетевых атак увеличилось на 4000 %. В связи с вышеуказанными угрозами крайне важным является раннее обнаружение и предотвращение подобных сценариев в корпоративной среде.

Изучая проблему майнинга, исследователи разделили его на два вида: майнинг на основе веб-браузера (криптоджекинг) и переносимый двоичный исполняемый файл (PE) [10]. Для использования майнинга на веб-странице используют технологию JavaScript asm.js и WebAssembly [11]. Вместо этого возможна установка двоичного криптомайнинга с использованием модифицированных версий программного обеспечения XMrig [12].

Несмотря на различия в технологии создания, принцип работы данных алгоритмов в целом похож. Независимо от вида майнинга (обычный майнинг или криптоджекинг), вида криптовалюты, вычислительного устройства и алгоритма ее добычи, компьютер, на котором производится майнинг, производит непрерывный обмен данными с пулом. Так как подобная сетевая активность происходит непрерывно, для определения майнинга, независимо от условий, могут использоваться методы обнаружения, основанные на анализе сетевой активности ПК.

В исследованиях предлагаются различные способы определения криптоджекинга. Изначально к криптоджекингу использовали тот же подход, который используется для анализа статических сигнатур вредоносных программ. Однако в данном случае результат не отличается высокой скоростью и надежностью [13]. Также были попытки анализа угрозы на основе статистической сигнатуры поступающей сетевой информации, однако они не были эффективны для работы в реальном времени и также не дали надежных результатов [14]. Этот подход оказался неэффективным против криптоджекинга из-за использования методов обфускации.

Другим вариантом решения проблемы является способ, основанный на использовании списков IP-адресов известных пулов майнинга для последующей блокировки исходящих от них угроз [15]. Такой способ является достаточно простым в плане организации и в плане определения угрозы. Однако с ростом популярности криптовалют и появлением новых альткоинов, а, соответственно, и новых пулов поддерживать в актуальности базы IP-адресов пулов и оперативно пополнять их новыми данными стало затруднительно. Как следствие, данный метод также был признан неэффективным.

Более высокую эффективность показал метод, основанный на глубокой проверке пакетов (DPI) [16]. В данном случае предполагается не только проверка заголовка передаваемого пакета данных, но и содержимого самих пакетов данных. Достоинством данного метода является его достаточная высокая надежность по сравнению с методом, основанным на анализе IP-адресов пулов. Однако для данного метода необходимо высокопроизводительное оборудование, которое зачастую есть только у самых крупных поставщиков услуг интернет-связи. Поэтому для отдельных компаний и организаций данный метод также неприемлем.

В связи с этим большой интерес представляют исследования, основанные на машинном обучении. Как правило, такие системы показывают высокий результат в процессах классификации. Например, авторы [17] используют динамический анализ кода, чтоб обнаружить криптомайнинг на основе браузера. Точность такого анализа составляет более 99 %.

В работе [18] авторы изучили поведение майнинга с помощью стека, обученного на рекуррентной нейронной сети после анализа 1159 вредоносных образцов. Согласно полученным результатам, нейронная сеть распознавала исходные образцы с вероятностью 98 %, а в случае, если они были зашифрованы, вероятность их обнаружения достигала 93 %.

Авторы [14] разработали расширение браузера под названием CMBlock, способное обнаруживать и блокировать скрипты майнинга, содержащиеся на веб-страницах. Предлагаемое решение сочетает в себе две разные методологии: занесение в черный

список и метод обнаружения поведения при майнинге.

Однако для реализации любого из предложенных способов необходимо не только установить данное решение для каждого пользователя на каждый компьютер сети, но и поддерживать его в актуальном и работоспособном состоянии. При этом работа любого из расширений будет затрачивать ресурсы отдельного компьютера, что при определённых условиях может существенно замедлить ПК. Поэтому для корпоративных сетей данный метод неприемлем ввиду больших временных затрат на его обслуживание и ресурсных затрат на его реализацию.

Альтернативным решением данной проблемы стала попытка централизации процесса анализа сетевого трафика на угрозу криптоджекинга не на отдельном компьютере, а на одном из узловых маршрутизаторов компьютерной сети. Например, в работе [19] авторы исследовали корпоративный трафик сеансового уровня, проходящий через узловой маршрутизатор корпоративного сегмента сети. Сбор данных осуществлялся с помощью протокола NetFlow. В качестве криптовалюты был выбран альткоин Monero. По результатам обучения нейронная сеть смогла идентифицировать майнинг Monero с точностью 98,94 %, однако для анализа других видов криптовалюты данная система не обладает достаточной гибкостью алгоритма работы.

На основании проведенных исследований можно сделать вывод, что задача определения майнера посредством его сетевой активности является достаточно новой, поэтому универсального способа ее решения еще нет. Учитывая результаты проведенных в этой области исследований, можно выявить основные требования к разрабатываемому решению:

1. Решение должно являться централизованным и иметь возможность анализировать трафик с узлового маршрутизатора сети;
2. В основе данного решения должны лежать принципы машинного обучения (а именно – нейронной сети) с целью повышения ее прогностической мощности;
3. Данное решение должно быть универсальным, то есть с одинаково высокой эффективностью определять криптоджекинговые и майнинговые угрозы различных типов.

В целом, можно отметить, что исследования на основе анализа сетевого трафика, позволяющие централизованно идентифицировать активность майнеров, представляются перспективным направлением. Своевременное обнаружение аномальной сетевой активности позволит снизить угрозу информационной безопасности и минимизировать нецелевую и незаконную эксплуатацию вычислительной собственности компаний.

Дальнейшие наши исследования будут направлены на поиск и выбор наиболее оптимального алгоритма обучения нейронной сети для задач идентификации трафика майнинга и предотвращения угроз криптоджекинга.

СПИСОК ЛИТЕРАТУРЫ

1. Satoshi, N. Bitcoin: A Peer-to-Peer Electronic Cash System / N. Satoshi // Cryptography Mailing list. – 2009. – Vol. 3. – pp. 1-9.

2. Cryptocurrencies you can still mine with your CPU/GPU in 2020 [Электронный ресурс] : Cointelligence [сайт] // URL: https://www.cointelligence.com/content/cryptocurrencies-can-still-mine-cpu-gpu-2018/ (дата обращения 10.2021).

3. Все криптовалюты [Электронный ресурс] : Coinmarketcap [сайт] // URL: https://coinmarketcap.com/ru/all/views/all/ (дата обращения 10.2021).

4. Whattomine [сайт] // URL: https://whattomine.com/ (дата обращения 10.2021).

5. В России сгорела секретная криптовалютная ферма, едва не уничтожив десятки автомобилей [Электронный ресурс] : CNews [сайт] // URL: https://www.cnews.ru/news/top/2019-12-19_rossiyanin_skrytno_ majnil (дата обращения 10.2021).

6. Russian nuclear scientists arrested for 'Bitcoin mining plot' [Электронный ресурс] : BBC [сайт] // URL: https://www.bbc.com/-news/world-europe-43003740 (дата обращения 10.2021).

7. Российские майнеры украли электричество на миллионы рублей [Электронный ресурс] : CNews [сайт] // URL: https://www.cnews.ru/news/top/2019-10-15_-

rossijskie_majnery_navorovali (дата обращения 10.2021).

8. PowerGhost: Beware of ghost mining [Электронный ресурс] : Kaspersky [сайт] // URL: https://www.kaspersky.com/blog/power ghost-fileless-miner/23310/ (дата обращения 10.2021).

9. McAfee Labs Threats Report [Электронный ресурс] : McAfee [сайт] // URL: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf (дата обращения 10.2021).

10. Zimba, A. Crypto Mining Attacks in Information Systems: An Emerging Threat to Cyber Security / A. Zimba, Zh. Wang, M. Mulenga, N. H. Odongo // Journal of Computer Information Systems. – 2020. – Vol. 60. – Issue 4. – pp. 297-308.

11. Konoth, R. K. MineSweeper: An In-depth Look into Drive-by Cryptocurrency Mining and Its Defense / R. K. Konoth, E. Vineti, V. Moonsamy, M. Lindorfer, Ch. Krügel, H. Bos, G. Vigna // Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. – 2018. – pp. 1714-1730.

12. On the trail of the XMRig miner [Электронный ресурс] : Securelist [сайт] // URL: https://securelist.com/miner-xmrig/99151/ (дата обращения 10.2021).

13. Alaeiyan M. Analysis and classification of context-based malware behavior / M. Alaeiyan, S. Parsa, M. Conti // Computer Communications. – 2019. – Vol. 136. – pp. 76-90.

14. Razali M. A. CMBlock: In-Browser Detection and Prevention Cryptojacking Tool Using Blacklist and Behavior-Based Detection Method / M. A. Razali, Sh. M. Shariff // Proceedings of the 6th International Visual Informatics Conference IVIC-2019 – 2019. – Vol. 10. – pp. 404-414.

15. Dr. Mine [Электронный ресурс] : GitHub [сайт] // URL: https://github.com/1last-Br3ath/drmine (дата обращения 10.2021).

16. Deep packet inspection (DPI) [Электронный ресурс] : TechTarget [сайт] // URL: https://www.techtarget.com/searchnetworking/definition/deep-packet-inspection-DPI (дата обращения 10.2021).

17. Carlin, D. Detecting cryptomining using dynamic analysis / D. Carlin, O'Kane, P., Sezer, S., Burgess, J. // 16th Annual Conference on Privacy, Security and Trust (PST). – 2018. – pp. 1-6.

18. Liu, J. A Novel Approach for Detecting Browser-Based Silent Miner / J. Liu, Z. Zhao, X. Cui, Z. Wang, Q. Liu // IEEE Third International Conference on Data Science in Cyberspace (DSC). – 2018. – pp. 490-497.

Russo, M. Detection of illicit cryptomining using network metadata / M. Russo, N. Srndi´c, P. Laskov // EURASIP Journal on Information Security. – 2021. – pp. 1-20.