УДК 004.056.55

МЕТОД АВТОМАТИЗОВАНОГО ПОШУКУ НЕСАНКЦІОНОВАНОГО МАЙНІНГУ КРИПТОВАЛЮТИ У КОНТЕЙНЕРАХ СЕРВЕРНИХ ОС

Приймак Андрій, Карпінець Василь, Яремчук Яна
Вінницький національний технічний університет

METHOD OF AUTOMATED SEARCH OF UNAUTHORIZED CRYPTOCURRENCY MINING IN SERVER OPERATING SYSTEM CONTAINERS

Pryimak Andrii; Karpinets Vasyl; Yaremchuk Yana
Vinnytsia National Technical University

Анотація: **Розглянуто проблему несанкціонованого майнінгу криптовалюти на серверах. Проведено дослідження процесів генерування криптовалюти в серверних операційних системах та запропоновано метод автоматизованого пошуку несанкціонованих процесів майнінгу, що складається з п'яти основних блоків: пошуку за назвою процесу, пошуку за сигнатурою та пошуку за майнінгом пулу, зупинки роботи контейнера, оповіщення адміністратора системи. Проведено порівняння запропонованого методу з існуючими, яке показало його перевагу – на відміну від відомих рішень він моніторить та аналізує підозрілі процеси у контейнерах серверних ОС з хостової віртуальної машини, що значно спрощує та автоматизує процес пошуку для великих топологій і, як результат, підвищує захист серверу.**

Ключові слова: **Інформаційна безпека, криптовалюта, несанкціонований майнінг, контейнери серверних операційних систем.**

Summary: **This paper considers the problem of unauthorized cryptocurrency mining on servers. The research of cryptocurrency generation processes in server operating systems is carried out and the method of automated search of unauthorized mining processes was proposed, which consists of 5 main blocks: search by process name, search by signature and search by mining pool, stop of container operation, notification of system administrator. A comparison of the proposed method with analogues showed its advantage - unlike to known solutions, it monitors and analyzes suspicious processes in server OS containers from the host virtual machine, which greatly simplifies and automates the search process for large topologies and as a result increases server security.**

Keywords: **Information security, cryptocurrency, unauthorized mining, containers of server operating systems, cryptojacking.**

Вступ

Зі зростанням популярності технології блокчейн та криптовалюти з'являється багато бажаючих заробляти на цьому кошти. У зв'язку з цим активізуються хакери, що використовують чужі ресурси для легкої наживи (криптоджекінг). Існує три основні типи майнерів [1]:

1. Виконувані файли: це типові шкідливі або потенційно небажані програми, виконувані файли (.exe), розміщені на комп'ютері та призначені для майнінгу криптовалют.

2. Браузерні майнери криптовалют: ці майнери, запрограмовані мовою JavaScript (або подібних технологіях), виконують свою роботу в Інтернет-браузері, споживаючи ресурси, поки браузер залишається відкритим.

3. Розширені безфайлові майнери: зловмисне програмне забезпечення, яке виконує свою роботу в пам'яті комп'ютера, неправильно використовуючи законні інструменти, такі як PowerShell. Одним із прикладів є MSH.Bluwimps, який окрім майнінгу здійснює додаткові шкідливі дії.

Зазвичай персональні комп'ютери користувачів вразливіші до атак, зокрема і криптомайнінгу, але це не приносить великого доходу зловмисникам. Тому набуває поширення несанкціоноване генерування криптовалюти на серверах

хостинг провайдерів, що є більш прибутковим, оскільки сервери потужніші. Це завдає шкоди провайдеру послуг та іншим користувачам, оскільки страждає продуктивність [2-3].

Несанкціоновані процеси генерування криптовалюти спричиняють надмірне навантаження системи, через що страждає продуктивність. Також надмірне навантаження системи може впливати на інших користувачів, що критично для бізнесу, який надає послуги у сфері інформаційних технологій, наприклад хостинг. Бувають випадки, коли програма для майнінгу супроводжує шкідливе програмне забезпечення, що робить його серйозною проблемою для інформаційної безпеки [4].

Без відповідних засобів захисту зрозуміти, що пристрій використовується зловмисником для несанкціонованого майнінгу криптовалюти майже неможливо. На сьогодні існує багато різнотипних інструментів для захисту ПК користувача (табл. 1).

Так, наприклад, MinerBlock, No Coin та Malwarebytes - це ефективні розширення браузерів, які зосередженні на блокуванні несанкціонованих майнерів криптовалют, що виконуються безпосередньо у браузері користувача.

Ці розширення використовують два різні підходи до блокування майнерів. Перший заснований на блокуванні запитів або скриптів, завантажених із чорного списку. Це традиційний підхід, який застосовується більшістю антивірусних програм. Іншим підходом, який робить вищезгадані розширення більш ефективним проти криптоджекінгу, є виявлення потенційної поведінки майнінгу всередині завантажених сценаріїв та їх негайне знищення [5].

Основним недоліком таких розширень є те, що вони захищають користувача лише від браузерного криптоджекінгу і ніяк не впливають на виконувані файли (.exe), розміщені на комп'ютері.

Іншими відомими інструментами є Windows Defender, Norton, Avast і Comodo. Вони спрямовані на захист ПК користувача від виконуваних файлів. Крім того, деякі з них є також ефективними у боротьбі з браузерним криптоджекінгом.

Найпопулярнішим та найбільш функціональним на сьогодні є пакет антивірусного програмного забезпечення Clam AntiVirus (Clam AV). Він підтримує багато операційних систем, включаючи Unix-подібні ОС, Windows ОС та серверні ОС (OpenVMS). До основних його переваг відносять:

– управління з командного рядка;

– можливість використання з більшістю поштових серверів, включаючи реалізацію milter-інтерфейсу для Sendmail;

– сканер у вигляді бібліотеки C;

– сканування файлів і пошти «на льоту»;

– відкритий код.

Таблиця 1.

Існуючі інструменти захисту від несанкціонованого майнінгу

Назва інструменту	**Браузер**	**Windows ОС**	**Unix-подібні ОС**	**Контейнери серверних ОС**
Miner Block	+	–	–	–
No Coin	+	–	–	–
Malwarebytes	+	–	–	–
Windows Defender	–	+	–	–
Norton	–	+	+	–
Avast	–	+	+	–
Clam AV	–	+	+	+
Comodo	+	+	+	–

Не зважаючи на всі свої переваги, Clam AV має суттєвий недолік при роботі з серверними ОС – механізм захисту передбачає запуск пошуку вірусного програмного забезпечення у кожному з контейнерів, а оскільки таких контейнерів може бути тисяча, то це значно сповільнює процес самого пошуку та додатково навантажує систему.

Представлені у таблиці 1 існуючі засоби захисту персональних комп'ютерів та серверів від несанкціонованих процесів

майнінгу включають в себе браузерні інструменти та засоби захисту для Windows, Unix-подібних та серверних ОС, проте немає відомого механізму для захисту серверних ОС, який би додатково не перенавантажував роботу системи та був одночасно ефективним.

Постановка задачі

Для вирішення задачі захисту серверних операційних систем від криптоджекінгу необхідно виконати дослідження можливості пошуку процесів несанкціонованого майнінгу криптовалют у контейнерах з хостової віртуальної машини для спрощення та автоматизації виконання антивірусних заходів для великих топологій і, як результат, зменшення навантаження на систему та підвищення захисту сервера.

Для ефективного вирішення поставленої задачі необхідно обрати оптимальні параметри, за якими буде відбуватись пошук несанкціонованого процесу майнінгу в контейнерах.

Розробка методу пошуку несанкціонованих процесів майнінгу в контейнерах серверних ОС

Пошук несанкціонованого процесу майнінгу доцільно проводити за декількома параметрами, оскільки використання лише одного параметра може не принести бажаного результату і не виявити процес майнінгу криптовалюти.

У запропонованому методі пошук несанкціонованого процесу майнінгу здійснюється за такими трьома параметрами:

– назва запущеного процесу;

– наявність з'єднання з майнерським пулом;

– бінарна сигнатура.

Найпростішим, але найменш ефективним пошуком є пошук за назвою процесу. Для цього необхідно переглянути всі запущені процеси на сервері та знайти назви, які можуть бути пов'язані з майнінгом та криптовалютою. Прикладами таких процесів є:

– XMRig;
– Cryptoloot;
– Cryptominer.

Найменш ефективним цей спосіб є тому, що процес, швидше за все, буде замаскований під якийсь системний процес або досить відому програму: chrome.exe, skype.exe і т.д.

Більш ефективним способом пошуку процесів майнінгу є пошук за майнерським пулом – об'єднання майнерів для видобутку криптовалюти, при цьому потужності пристроїв кожного з учасників становлять загальний хешрейт (обчислювальну потужність) пулу. Чим вище загальний хешрейт пулу, тим вище і його «удача» – шанс підписання нового блоку. Тому великі пули працюють значно ефективніше дрібних.

Оскільки пули для майнінгу бувають різними і можуть відрізнятися один від одного за цілою низкою критеріїв, то при розробці методу необхідно було врахувати усі їх особливості.

Для виявлення з'єднань з майнерським пулом, необхідно дослідити список усіх наявних з'єднань в системі, що можна зробити за допомогою стандартних утиліт операційних систем. Серед наявних з'єднань потрібно знайти з'єднання з майнерським пулом, назви яких можна знайти у відкритому доступі.

Варто зазначити, що на сьогодні пулів для майнінгу існує вже понад тисячу і з огляду на зростаючу складність обчислювальних задач, їх стає все більше і більше.

Прикладами відомих пулів для майнінгу є suprnova.cc, nanopool.org, zpool.ca, miningrigrentals.com.

Іншим параметром для пошуку несанкціонованого процесу майнінгу в контейнерах є магічне число, або сигнатура, – цілочисельна або текстова константа, яка використовується для однозначної ідентифікації ресурсу або даних.

В UNIX-подібних операційних системах тип файлу зазвичай визначається за сигнатурою файлу, незалежно від

розширення його назви. Для інтерпретації сигнатури файлу в них передбачається стандартна утиліта file.

Виявлення, що базується на сигнатурах, – метод роботи антивірусів і систем виявлення вторгнень, при якому програма, переглядаючи файл або пакет, звертається до словника з відомими вірусами, складеного авторами програми. У разі відповідності будь-якої ділянки коду програми, яка переглядається, відомому коду (сигнатурі) вірусу в словнику, програма антивірус може зайнятися виконанням видалення чи відновлення файлу.

Для досягнення досить тривалого успіху при використанні цього методу необхідно періодично поповнювати словник відомих вірусів новими визначеннями (в основному в онлайн режимі).

Недоліком синтаксичних сигнатур та майнінг пулів є те, що вони вимагають регулярного і вкрай оперативного оновлення. Для пошуку та порівняння бінарних сигнатур, назв зловмисних процесів та процесів з'єднання з пулом для майнінгу було використано відкриті бази даних, які містять всі ці дані та постійно оновлюються (btc.com, Clam AV БД і blockchain.info).

Таким чином, на основі трьох проаналізованих параметрів, було запропоновано метод для автоматизованого пошуку несанкціонованого процесу майнінгу в контейнерах серверних ОС (рис. 1), що складається з п’яти таких етапів:

1. Пошук несанкціонованих процесів генерування криптовалюти за назвою процесу. Здійснюється порівняння назв запущених процесів з назвами майнінгових процесів. Якщо є збіг, це свідчить про виявлення процесів майнінгу.

2. Пошук по бінарній сигнатурі. Здійснюється порівняння сигнатур процесів у контейнерах з сигнатурами відомих процесів майнінгу. Збіг свідчить про наявність несанкціонованих процесів генерування криптовалюти.

3. Пошук за з'єднанням з пулом для майнінгу. Якщо майнінг здійснюється у пулі, то підтримується постійний зв'язок з пулом. Здійснюється пошук на наявність з'єднання з відомими пулами. Наявність збігання свідчить про виявлення процесу майнінгу.

4. Виявлення процесу несанкціонованого майнінгу і зупинка контейнера, в якому був виявлений процес майнінгу.

Рис. 1 – Схема роботи запропонованого методу пошуку несанкціонованих процесів майнінгу в контейнерах

5. Оповіщення адміністратора системи про виявлення несанкціонованих процесів генерування криптовалюти.

Схему роботи за цими етепами представлено на рис. 1.

Після виявлення несанкціонованих процесів майнінгу криптовалюти відувається зупинка контейнера, де здійснювався майнінг, та надсилається сповіщення на пошту адміністратора системи.

Запропонований метод автоматично виявляє несанкціоновані процеси майнінгу криптовалюти. На відміну від існуючих інструментів розроблений метод здійснює пошук у контейнерах з хостової віртуальної машини, для того, щоб не було потреби запускати пошук у кожному з контейнерів, яких може бути сотні та навіть тисячі і, як результат, зменшити навантаження на систему. Також процес запускається через певні проміжки часу (на вибір адміністратора) автоматично для ефективності перевірки і для своєчасного виявлення криптоджекінгу.

Алгоритм реалізації запропонованого методу пошуку несанкціонованого процесу майнінгу в контейнерах серверних ОС на програмному рівні буде таким.

Крок 1. Початок роботи.

Крок 2. Завантаження при першому запуску програми (далі просто оновлення) відкритих баз даних для отримання актуальних назв пулів для майнінгу, бінарних сигнатур та назв процесів.

Крок 3. Пошук несанкціонованих процесів генерування криптовалюти за назвою процесу.

Крок 4. Пошук за бінарною сигнатурою.

Крок 5. Пошук за з'єднанням з пулом для майнінгу.

Крок 6. Виявлення процесу несанкціонованого майнінгу.

Якщо у кроках 3-5 було виявлено процес майнінгу, то виконується перехід до кроку 7. Якщо не виявлено, то до кроку 9.

Крок 7. Зупинка контейнера, в якому був виявлений процес майнінгу.

Крок 8. Оповіщення адміністратора системи про виявлення несанкціонованих процесів генерування криптовалюти.

Крок 9. Кінець роботи.

Якщо по жодному з параметрів не було виявлено несанкціонованих процесів майнінгу, тоді програма завершує роботу і повторна перевірка розпочинається, наприклад, через годину.

Блок-схема додатку відповідно до представленого алгоритму буде мати вигляд, який наведено на рис. 2.

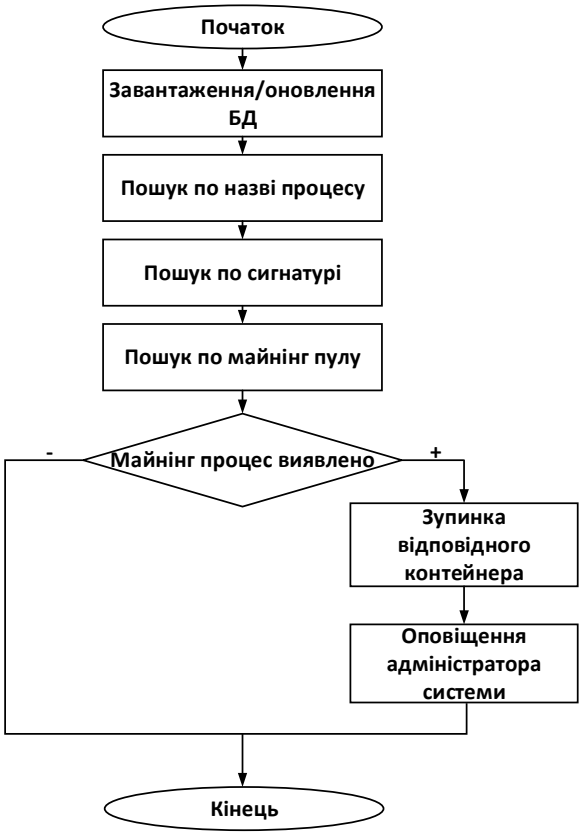
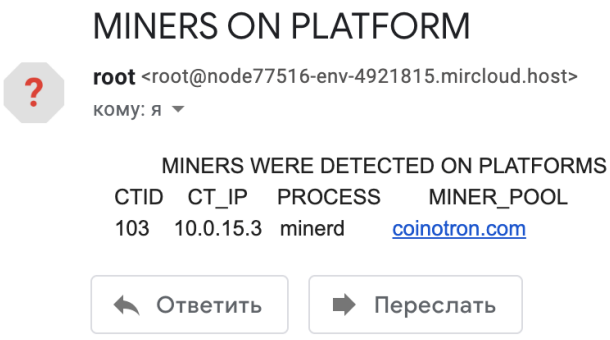


Рис. 2 – Блок-схема роботи алгоритму реалізації запропонованого методу

В кінці роботи, якщо є збіг за будь-яким із параметрів і були виявлені несанкціоновані процеси майнінгу криптовалюти в будь-якому з контейнерів серверної операційної системи, програма зупиняє роботу контейнера, де був виявлений процес, та відсилає на пошту адміністратора лист з детальною інформацією про процес (рис. 3), а саме ID контейнера, IP - адреса контейнера, назва процесу, пул для майнінгу.


MINERS ON PLATFORM

root <root@node77516-env-4921815.mircloud.host>
кому: я

MINERS WERE DETECTED ON PLATFORMS

CTID	CT_IP	PROCESS	MINER_POOL
103	10.0.15.3	minerd	coinotron.com

Ответить Переслать

Рис. 3 – Повідомлення адміністратору системи про виявлений процес майнінгу

Сукупність даних параметрів допоможе адміністратору системи чітко виявити місцезнаходження несанкціонованого процесу, який здійснював генерування криптовалюти.

Після виявлення процесу несанкціонованого майнінгу криптовалюти, додаток зупиняє контейнер, де здійснювався процес майнінгу.

Стан контейнерів після завершення роботи додатку зображений на рисунку 4.

```
[root@localhost ~]# vzlist -a
      CTID      NPROC STATUS    IP_ADDR         HOSTNAME
       101         19 running   10.0.2.101      -
       102         19 running   10.0.2.102      -
       103          - stopped   10.0.2.103      -
[root@localhost ~]# _
```

Рис. 4 – Інформація про контейнери після завершення роботи додатку

Як можна побачити, контейнер 103, де був запущений процес, має статус "stopped", що означає, що він зупинений.

Оскільки додаток запускається автоматично через певні проміжки часу, наприклад кожну годину, що досить часто, він не має перенавантажувати систему, відповідно час його виконання має бути невеликим. Тому варто провести тест на швидкодію роботи додатка, що працює на основі запропонованого методу.

Результати тесту на час виконання додатку зображені на рисунку 5.

```
[root@localhost /]# time ./antiminer.sh
=========================WARNING==========================
            MINERS WERE DETECTED ON PLATFORMS
    CTID    CT_IP     PROCESS        MINER_POOL
    103    10.0.15.3   minerd        coinotron.com

real    0m2.585s
user    0m0.013s
sys     0m0.057s
[root@localhost /]# _
```

Рис. 5 – Результати тесту на швидкодію додатку

Результати показали, що час виконання перевірки контейнерів додатком є менше 3 секунд (2.585 с), що є досить гарним результатом, тому можна зробити висновок, що метод швидко працює та не перенавантажує систему.

Висновки

Для вирішення проблеми несанкціонованого майнінгу криптовалюти на серверах проведено дослідження існуючих інструментів захисту, описано їх переваги та недоліки. Основним недоліком є те, що механізм захисту передбачає запуск пошуку вірусного програмного забезпечення в кожному з контейнерів, а оскільки таких контейнерів може бути тисяча, то це значно сповільнює процес самого пошуку та додатково навантажує систему.

Виходячи з проведеного аналізу поставлено задачу та проаналізовано три параметри пошуку несанкціонованих процесів генерування криптовалюти (пошук підозрілих процесів за назвою, за бінарною сигнатурою та за з'єднанням з пулом для майнінгу), на основі яких було запропоновано принципово новий метод, що складається з п’яти основних етапів. Для ефективного пошуку подібних процесів запропоновано використання відкритих баз даних, які містять необхідну інформацію та постійно оновлюються.

На відміну від існуючих інструментів, розроблений метод здійснює пошук у контейнерах з хостової віртуальної машини для того, щоб не було потреби запускати пошук у кожному з контейнерів, яких може бути велика кількість і, як результат, зменшити навантаження на систему.

Крім того, було проведено дослідження швидкодії запропонованого методу. Результати тесту його виконання показали час 2.585 секунд, що відображає швидку роботу та відсутність додаткового перенавантаження на систему.

Перелік посилань

[1] Захист віртуальних машин на основі інструкцій нового покоління процесорів AMD Zen / В. С. Соколовський, В. В. Карпінець, Ю. Є. Яремчук, Д. П. Присяжний, А. В. Приймак // Реєстрація, зберігання і обробка даних. – 2018. – Т. 20,№ 3 – С. 102–111.

[2] Хаменушко И. В. Криптовалюты и их майнинг как экономическая реальность : предпосылки

правового регулирования // Законодательство. – 2017. – № 12.– С. 33 – 42.

[3] Melanie Swan. Blockchain: Blueprint for a New Economy. — O'Reilly Media, Inc., 2015. – 152 с.

[4] Mathias C. What is Virtualization? Far more than just virtual machines [Електронний ресурс] / Craig Mathias. – 2017. – Режим доступу до ресурсу: https://www.itnews.com/article/3234795/virtualization/what-is-virtualization-definition-virtual-machine-hypervisor.html.

[5] Облачная пирамида: IAAS, PAAS И SAAS [Електронний ресурс] – Режим доступу до ресурсу: https://gigacloud.ua/ru/blog/navchannja/hmarna-piramida-iaas-paas-i-saas

References

[1] Protection of virtual machines based on the instructions of the new generation of AMD Zen processors / VS Sokolovsky, VV Karpinets, YE Yaremchuk, DP Prysyazhny, AV Priymak // Registration, storage and Data Processing. - 2018. - Vol. 20, № 3 - P. 102–111.

[2] Hamenushko IV Cryptocurrencies and their mining as an economic reality: prerequisites for legal regulation // Legislation. - 2017. - № 12.– P. 33 - 42.

[3] Melanie Swan. Blockchain: Blueprint for a New Economy. - O'Reilly Media, Inc., 2015. - 152 p.

[4] Mathias C. What is Virtualization? Far more than just virtual machines [Electronic resource] / Craig Mathias. - 2017. - Resource access mode: https://www.itnews.com/article/3234795/virtualization/what-is-virtualization-definition-virtual-machine-hypervisor.html.

[5] Cloud pyramid: IAAS, PAAS AND SAAS [Electronic resource] - Mode of access to the resource: https://gigacloud.ua/ru/blog/navchannja/hmarna-piramida-iaas-paas-i-saas

Реферат

Приймак Андрій, Карпінець Василь, Яремчук Яна

Метод автоматизованого пошуку несанкціонованого майнінгу криптовалюти у контейнерах серверних ОС

Відомо, що зі зростанням популярності технології блокчейн та криптовалюти з'являється багато бажаючих заробляти на цьому кошти. У зв’язку з цим активізуються хакери, що використовують чужі ресурси для легкої наживи. На сьогодні відомо багато різнотипних інструментів для захисту персональних комп’ютерів користувачів від криптоджекінгу, проте актуальним є ефективний захист для серверних ОС.

У даній роботі виконано дослідження можливості пошуку несанкціонованих процесів майнінгу криптовалюти за трьома параметрами: пошук підозрілих процесів за назвою, за бінарною сигнатурою та за з'єднанням з пулом для майнінгу.

На основі проведеного дослідження запропоновано метод автоматизованого пошуку несанкціонованого майнінгу криптовалюти у контейнерах серверних ОС, що складається з 5 основних етапів:

1. Пошук несанкціонованих процесів генерування криптовалюти за назвою процесу.

2. Пошук за бінарною сигнатурою.

3. Пошук за з'єднанням з пулом для майнінгу.

4. Виявлення процесу несанкціонованого майнінгу і зупинка контейнера, в якому був виявлений процес майнінгу.

5. Оповіщення адміністратора системи про виявлення несанкціонованих процесів генерування криптовалюти.

Варто зазначити, що на відміну від існуючих інструментів, розроблений метод здійснює пошук у контейнерах з хостової віртуальної машини, для того, щоб не було потреби запускати пошук у кожному з контейнерів, яких може бути велика кількість і, як результат, зменшити навантаження на систему.

Також описано блок-схему додатку для реалізації роботи запропонованого методу, а також приведені приклади зупинки контейнера, в якому знайдено несанкціонований процес майнінгу та

відповідне повідомлення адміністратору системи.

Крім того, проведено дослідження швидкодії запропонованого методу. Результати тесту його виконання показали час 2.585 секунд, що відображає швидку роботу та відсутність додаткового перенавантаження на систему.

Приймак Андрей, Карпинец Василий, Яремчук Яна

Метод автоматизированного поиска несанкционированного майнинга криптовалюты в контейнерах серверных ОС

Известно, что с ростом популярности технологии блокчейн и криптовалюты появляется много желающих зарабатывать на этом деньги. В связи с этим активизируются хакеры, использующие чужие ресурсы для легкой наживы. На сегодня известно много разнотипных инструментов для защиты персональных компьютеров пользователей от криптоджекинга, однако актуальной остается эффективная защита для серверных ОС.

В данной работе выполнено исследование возможности поиска несанкционированных процессов майнинга криптовалюты по трем параметрам: поиск подозрительных процессов по названию, по бинарной сигнатуре и по соединению с пулом для майнинга.

На основе проведенного исследования предложен метод автоматизированного поиска несанкционированного майнинга криптовалюты в контейнерах серверных ОС, который состоит из 5 основных этапов:

1. Поиск несанкционированных процессов генерирования криптовалюты по названию процесса.
2. Поиск по бинарной сигнатуре.
3. Поиск по соединении с пулом для майнинга.
4. Выявление процесса несанкционированного майнинга и остановка контейнера, в котором был обнаружен процесс майнинга.
5. Уведомление администратора об обнаружении несанкционированных процессов генерирования криптовалюты.

Стоит отметить, что в отличии от существующих инструментов, разработанный метод осуществляет поиск в контейнерах с хостовой виртуальной машины, для того, чтобы не было необходимости запускать поиск в каждом из контейнеров, которых может быть много, и, как результат, уменьшить нагрузку на систему.

Также описано блок-схему приложения для реализации работы предложенного метода, а также приведены примеры остановки контейнера, в котором был обнаружен несанкционированный процесс майнинга, и соответствующее сообщение администратору системы.

Кроме того, проведено исследование быстродействия предложенного метода. Результаты теста его выполнения показали время 2.585 секунд, что отражает быструю работу и отсутствие дополнительного перегрузки на систему.

Pryimak Andrii, Karpinets Vasyl; Yaremchuk Yana

Method of automated search of unauthorized cryptocurrency mining in server operating system containers

It is known that with the growing popularity of blockchain and cryptocurrency technology, many people want to make money on it. As a result, hackers who use other people's resources for easy profit are becoming more active. There are many different tools available today to protect user’s personal computers from cryptojacking, but effective protection for server operating systems are still actual.

This paper investigates the possibility of searching for unauthorized cryptocurrency mining processes by three parameters: search for suspicious processes by name, by binary signature and by connection to the mining pool.

Based on the study, a method of automated search for unauthorized cryptocurrency mining

in server OS containers was proposed, which consists of 5 main stages:

1. Search for unauthorized cryptocurrency generation processes by process name.
2. Search by binary signature.
3. Search for a connection to a mining pool
4. Detection of the process of unauthorized mining and stopping the container in which the mining process was detected.
5. Notification of the system administrator about the detection of unauthorized cryptocurrency generation processes.

It is worth noting that, unlike existing tools, the developed method searches for containers from the host virtual machine, so that there is no need to run a search in each of the containers, as it can be a large number of them and as a result reduce the load on the system.

The block diagram of the application for the implementation of the proposed method was also described, as well as examples of stopping the container in which an unauthorized mining process was found and the corresponding message to the system administrator.

In addition, a study of the speed of the proposed method was conducted. The results of the test showed a time of 2,585 seconds, which reflects the fast operation and the absence of additional overload on the system.

Відомості про авторів

Приймак Андрій Васильович

Освіта: Вища, магістр за спеціальністю "Управління інформаційною безпекою" (2018).

Місце роботи: Вінницький національний технічний університет; кафедра менеджменту та безпеки інформаційних систем, Центр інформаційних технологій та захисту інформації.

Область знань: криптографічний захист інформації, технології програмування, бази даних і знань.

Наукові інтереси: Криптографічний та стеганографічний захист інформації.

Email: *andrii.pryimak@live.com*

Карпінець Василь Васильович

Освіта: магістр за спеціальністю «Комп'ютерні системи та мережі» (2006 р.)

Науковий ступінь: Кандидат технічних наук (2012 р.); доцент (2014 р.).

Місце роботи: Вінницький національний технічний університет, кафедра менеджменту та безпеки інформаційних систем.

Область знань: інформаційна безпека.

Наукові інтереси: криптографічний та стеганографічний захист інформації, безпека інформаційних систем.

E-mail: karpinets@gmail.com

Яремчук Яна Юріївна

Місце роботи: Вінницький національний технічний університет, студент кафедри менеджменту та безпеки інформаційних систем.

Область знань: математика, криптографія, безпека інформаційних систем.

Наукові інтереси: теорія чисел, криптографічний та стеганографічний захист інформації, безпека інформаційних систем.

E-mail: yanunova@hotmail.com