Розробка методу автоматизованого пошуку несанкціонованих процесів генерування криптовалюти в контейнерах серверних операційних систем

Робота студентки
Жмуцької Наталії

Науковий керівник
Карпінець В.В.

Актуальність та мета роботи

Зі зростанням популярності технології блокчейн та криптовалюти, все частіше з'являється проблема несанкціонованого генерування криптовалюти на серверах провайдерів хостингу. Це завдає шкоди провайдеру послуг та іншим користувачам, оскільки спричиняє надмірне навантаження системи та страждає продуктивність.

На сьогодні існують засоби захисту персональних комп'ютерів від несанкціонованих процесів майнінгу, проте немає відомих засобів захисту для серверних операційних систем. Тому питання виявлення і блокування майнерських процесів на серверних ОС стає все більш актуальним.

Метою роботи є дослідження процесів генерування криптовалюти в серверних операційних системах та розробка методу автоматизованого пошуку несанкціонованих процесів генерування криптовалюти в контейнерах серверних операційних систем.

Поняття криптовалюти та майнінгу

- Блокчейн — розподілена база даних, що зберігає впорядкований ланцюжок записів (так званих блоків), що постійно довшає. Дані захищено від підробки та спотворення. Кожен з цих блоків даних захищений і прив'язаний один до одного за допомогою криптографічних принципів (тобто ланцюжка).
- Криптовалюта – це цифрові гроші, фіатного аналога яким немає. Криптовалюта відрізняється від інших електронних валют тим, що захищена і зашифрована за допомогою спеціальних криптографічних алгоритмів. Головною особливістю криптовалюти вважається її децентралізованість, незалежність від єдиного центру управління. Всі ці особливості забезпечує технологія блокчейн, на принципах роботи якої і функціонує криптовалюта.
- Найпоширенішим способом видобутку криптовалюти вважається майнінг (від mining - добувати). Головна мета майнінгу – пошук криптографічного підпису до блоку у вигляді хешу. Як тільки він підібраний – блок закривається. А майнер за це отримує винагороду у вигляді криптовалюти.

Використання моделі Platform as a Service для генерування криптовалюти

- PaaS або платформа як послуга (англ. Platform as a service) – це один із способів надання клієнту готового програмного середовища. Постачальник PaaS будує і забезпечує стійке і оптимізоване середовище, на якому користувачі можуть встановлювати додатки і набори даних. Користувачі можуть зосередитися на створенні та запуску додатків, а не на створенні і обслуговуванні базової інфраструктури і служб.
- В PaaS ресурси надаються через інфраструктуру, розміщену у хмарного провайдера. Користувачі зазвичай отримують доступ до послуг Platform as a service через веб-браузер.
- В моделі PaaS користувачам часто надаються для користування контейнери серверних операційних систем. І майнінг здійснюється саме в цих контейнерах.
- Контейнеризація – це легка віртуалізація і ізоляція ресурсів на рівні операційної системи, яка дозволяє запускати додаток і необхідний йому мінімум системних бібліотек в повністю стандартизованому контейнері, що з'єднують з хостом або чим-небудь зовнішнім по відношенню до нього за допомогою певних інтерфейсів.
- Контейнери – незалежні середовища виконання з власними центральним процесором, пам'яттю, блоком введення-виведення і мережевими ресурсами, які використовують ядро гостьової ОС. На виході виходить щось на зразок віртуальної машини, яка працює як надбудова гостьової ОС.

Метод автоматизованого пошуку несанкціонованих процесів генерування криптовалюти в контейнерах серверних операційних систем

Пошук несанкціонованого процесу майнінгу здійснюється за наступними параметрами:
- назва запущеного процесу;
- наявність з'єднання з майнерським пулом;
- бінарна сигнатура.

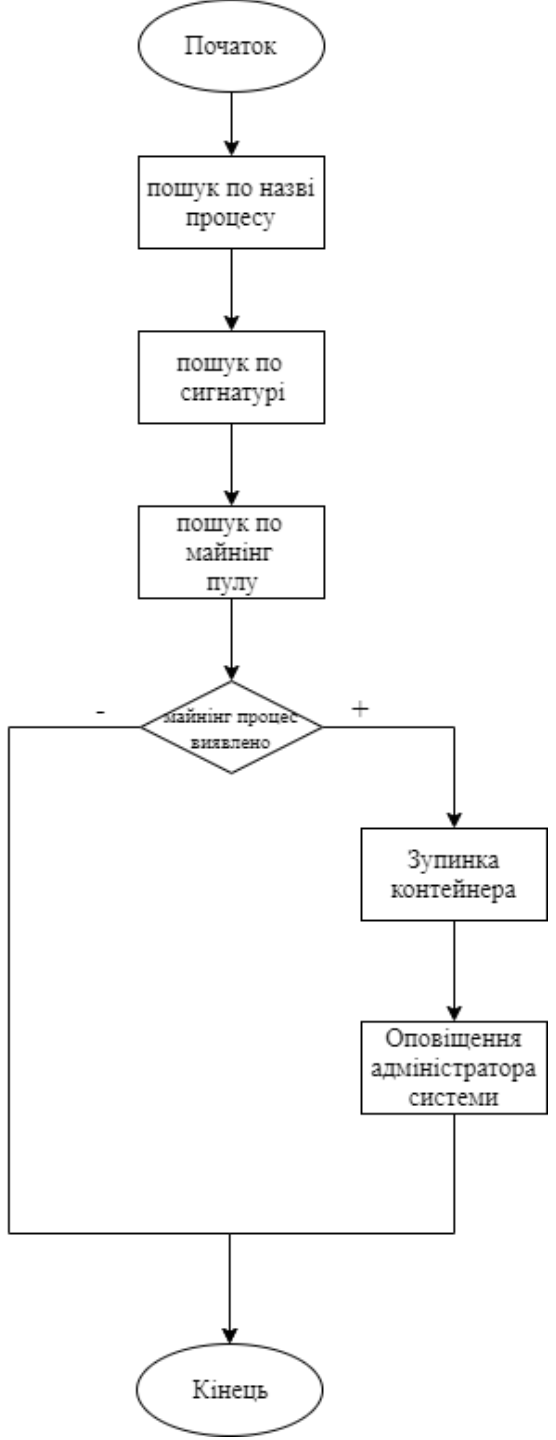
Для пошуку та порівняння бінарних сигнатур, назв зловмисних процесів та процесів з'єднання з пулом для майнінгу використовуються відкриті бази даних, які містять всі ці дані та постійно оновлюються.

Після виявлення несанкціонованих процесів майнінгу криптовалюти програма зупиняє контейнер, де здійснювався майнінг та надсилає сповіщення на пошту адміністратора системи.

В разі виявлення несанкціонованого процесу майнінгу адміністратор системи отримує лист з детальною інформацією про процес, а саме:
- ID контейнера;
- IP - адреса контейнера;
- назва процесу;
- пул для майнінгу.

Процес пошуку автоматично запускається кожну годину.

Алгоритм роботи методу



	Браузер Chrome	Windows OS	Linux OS	Контейнери
Coin Miner Block	+	-	-	-
DetectMiner	+	-	-	-
cryptoTab	+	-	-	-
Windows Defender	-	+	-	-
Kaspersky Antivirus	-	+	-	-
Avast	-	+	-	-
Clamav	-	-	+	-
Comodo	-	-	+	-
Розроблений метод	-	-	-	+

Приклад роботи програми

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

Інформація про контейнери до початку роботи скрипта

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

Запуск скрипта для пошуку процесів майнінгу

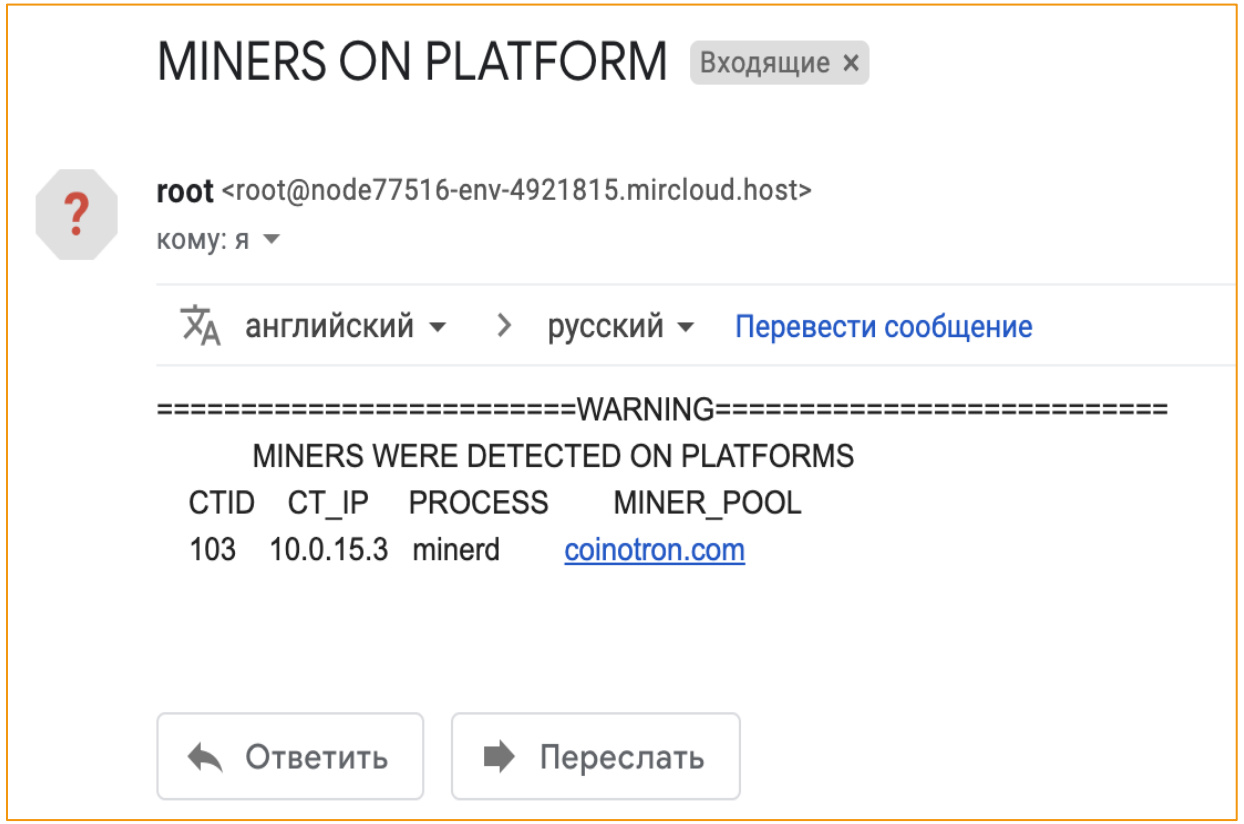
```
top - 13:36:51 up 7 min,  0 users,  load average: 0.00, 0.00, 0.00
Tasks:  22 total,   1 running,  21 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.0%us,  0.0%sy,  0.0%ni,100.0%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:    262144k total,    84052k used,   178092k free,        0k buffers
Swap:   524288k total,        0k used,   524288k free,    61612k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
    1 root      20   0  2900 1420 1240 S  0.0  0.5   0:00.00 init
    2 root      20   0     0    0    0 S  0.0  0.0   0:00.00 kthreadd/103
    3 root      20   0     0    0    0 S  0.0  0.0   0:00.00 khelper/103
  121 root      16  -4  2468  600  356 S  0.0  0.2   0:00.00 udevd
  645 root      20   0 36028 1356 1004 S  0.0  0.5   0:00.00 rsyslogd
  665 root      20   0  8708  968  440 S  0.0  0.4   0:00.00 sshd
  676 root      20   0  2896  884  700 S  0.0  0.3   0:00.00 xinetd
  688 root      20   0  8992  792  308 S  0.0  0.3   0:00.00 saslauthd
  690 root      20   0  8992  540   56 S  0.0  0.2   0:00.00 saslauthd
  710 root      20   0 12616 1940  720 S  0.0  0.7   0:00.00 sendmail
  719 smmsp     20   0 12400 1728  648 S  0.0  0.7   0:00.00 sendmail
  731 root      20   0 11128 3268 1828 S  0.0  1.2   0:00.00 httpd
  734 apache    20   0 11128 2168  708 S  0.0  0.8   0:00.00 httpd
  744 root      20   0  3616 1180  608 S  0.0  0.5   0:00.00 crond
  752 root      20   0  2008  520  460 S  0.0  0.2   0:00.00 mingetty
  753 root      20   0  2008  524  460 S  0.0  0.2   0:00.00 mingetty
  757 root      20   0 27560  764  516 S  0.0  0.3   0:00.00 vzctl
  758 root      20   0  3148 1592 1340 S  0.0  0.6   0:00.01 bash
  777 root      20   0  3144 1256  832 S  0.0  0.5   0:00.00 screen
  778 root      20   0  3048 1448 1212 S  0.0  0.6   0:00.00 sh
  779 root      20   0 64372 2548 1880 S  0.0  1.0   0:00.00 minerd
  785 root      20   0  2572 1080  892 R  0.0  0.4   0:00.00 top
```

Перелік запущених процесів в контейнері

```
[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 ~]# _
```

Інформація про контейнери після завершення роботи скрипта



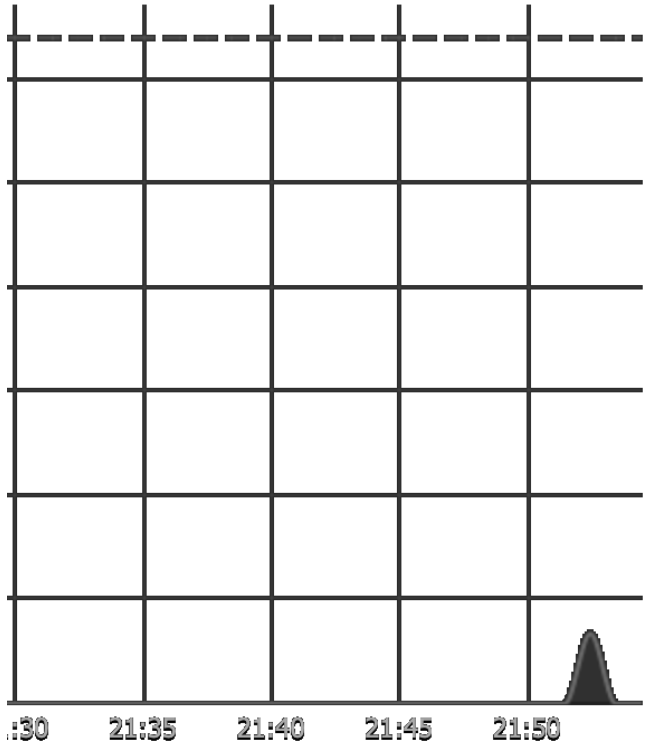
Вигляд листа про виявлення процесу майнінгу

Тестування програмного засобу

```
[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 /]# _
```

Результати тесту на час виконання скрипта



Тестування навантаження на сервер

Висновок

В роботі розроблено метод автоматизованого пошуку несанкціонованих процесів генерування криптовалюти в контейнерах серверних операційних систем з хостової машини за трьома параметрами: назва процесу, бінарна сигнатура та наявність з’єднання з пулом для майнінгу.

Також розроблено програмний засіб для реалізації розробленого методу з опціями зупинки контейнера, де виявлено несанкціонований процес та сповіщення адміністратора системи.

Скрип протестовано на швидкість роботи та навантаження системи. В ході тестування виявлено, що скрипт працює швидко та не навантажує систему.

Проведено економічний аналіз розробки. На основі отриманих економічних розрахунків, можна говорити про потенційну зацікавленість інвесторів у фінансуванні розробки та допустимі терміни окупності продукту.

Таким чином, використання даного ресурсу доцільне для захисту від несанкціонованого майнінгу криптовалюти в контейнерах серверних операційних систем. Тому можна вважати, що в результаті виконання роботи було реалізовано поставлені задачі та досягнуто бажаної мети.

Дякую за увагу!