Министерство цифрового развития, связи и массовых коммуникаций

Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет телекоммуникаций и информатики»

(СибГУТИ)

Кафедра ИКСС

Индивидуальное задание по дисциплине: «Операционные системы»

вариант – 23

Выполнил: студент группы АП-103

Седельников А. С.

Проверил:

Квиткова И. Г.

Новосибирск, 2022 г.

**СОДЕРЖАНИЕ**

СОДЕРЖАНИЕ...........................................................................................2  
ВВЕДЕНИЕ..................................................................................................3  
1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ МАЙНИНГА.......................................4

* 1. Понятие майнинга, принципы работы, виды, скрытый майнинг...................................................................................................4

2. ПРОЦЕСС МАЙНИНГА В СИСТЕМЕ................................................5  
2.1 Обнаружение процесса в системе........................................................6

2.2 Поиск исходных каталогов и файлов майнера в системе..................6

2.3 Принудительное завершение процесса майнера и удаление всех следов, связанных с процессом майнера.................................................10

ЗАКЛЮЧЕНИЕ.........................................................................................11

БИБЛИОГРАФИЧЕСКИЙ СПИСОК......................................................12

**ВВЕДЕНИЕ**

**Актуальность темы исследования.** В современное время люди пытаются найти новые пути к получению обогащения, такими как фриланс, свой бизнес и т. д., но также существует один вид обогащения, это майнинг. С ростом курса криптовалют, всё чаще стали использовать программы, которые «добывают» ту самую криптовалюту, а программы называются «майнерами». Но не все люди используют свою технику для «добычи», поэтому со словом «майнер» сейчас ассоциируется вирус-программа или процесс, которая «добывает» криптовалюту без ведома зараженного пользователя. Этим обусловлена актуальность данной темы.

**Объектом исследования** является майнинг.

**Целью дополнительного задания** является обнаружение и полное удаление из системы, как самого майнера, так и его следов.

Реализация данной цели поставила несколько задач:

* рассмотреть понятие, принципы работы и виды майнинга
* способ обнаружения майнера в системе
* способ полного удаления майнера из системы и его следов
* способы обезопасить в будущем систему от такого рода уязвимостей

**Степень разработанности проблемы.** Теоретической и методологической основой исследования являются труды ведущих зарубежных и отечественных специалистов в сфере кибербезопасности, чьи исследования тем или иным образом касаются проблемы вирусов-майнеров.

**Информационной базой исследования** послужили открытые источники в сети Интернет связанные с проблемой обнаружения майнера в системе и способы борьбы с уже обнаруженным майнером.

**Практическая значимость исследования** заключается в выработке способов обнаружения вируса и полного удаления файлов и следов в других местах системы на майнер.

Дополнительное задание на тему варианта №23 состоит из введения, двух глав, 4 параграфов, заключения и библиографического списка.

1. **ТЕОРЕТИЧЕСКИЕ ОСНОВЫ МАЙНИНГА**
   1. **Понятие, принципы работы, виды**

Майнинг, также добыча (от англ. mining — добыча полезных ископаемых) — деятельность по созданию новых структур (обычно речь идёт о новых блоках в блокчейне) для обеспечения функционирования криптовалютных платформ.

За создание очередной структурной единицы обычно предусмотрено вознаграждение за счёт новых (эмитированных) единиц криптовалюты и/или комиссионных сборов. Обычно майнинг сводится к серии вычислений с перебором параметров для нахождения хеша с заданными свойствами. Разные криптовалюты используют разные модели вычислений, но они всегда достаточно длительны по времени для нахождения приемлемого варианта и быстры для проверки найденного решения. Такие вычисления используются алгоритмами криптовалют для обеспечения защиты от повторного расходования одних и тех же единиц, а вознаграждение стимулирует людей расходовать свои вычислительные мощности и поддерживать работу сетей.

Майнинг разных криптовалют может использовать разные процедуры для подтверждения выполнения работы. Для ряда криптовалют, в том числе и для Биткойна, были созданы специализированные процессоры (ASIC), которые из-за лучшей производительности и относительной экономичности вытеснили другие способы майнинга. В других случаях подобный подход оказался не столь эффективным. По состоянию на конец 2017 года майнинг ряда криптовалют, в том числе Ethereum, остаётся более эффективным с использованием процессоров видеокарт. Значительное повышение цен на криптовалюты привело к повышению спроса на майнинговое оборудование, в том числе на видеокарты. Это подтолкнуло Sapphire и Asus выпустить линейку специализированных комплектующих для майнинга.

В мае 2021 года существенно (в 2—3 раза) вырос спрос на SSD и HDD больших объемов, который аналитики связывают с запуском криптовалюты Chia (англ.). Созданная автором протокола BitTorrent Брэмом Коэном сеть Chia Network использует алгоритмы консенсуса Proof-of-Space и Proof-of-Time (доказательства пространства и времени)

Скрытым называют майнинг, при котором используются чужие ресурсы, например запуск майнинга работниками на корпоративных серверах или внедрение кода для майнинга в состав вирусов и троянов. В июне 2011 года Symantec сообщила, что майнинг может быть запущен на ботнетах. В отчёте за второй квартал 2011 года Лаборатория Касперского сообщила о троянском модуле, который занимался скрытым майнингом. В апреле 2013 была зафиксирована крупная эпидемия вирусного распространения через текстовые сообщения в Skype троянских программ, целью которых был поиск и кража файлов криптовалютных кошельков (wallet.dat) и скрытый майнинг на CPU. До 2011—2013 годов встречался скрытый майнинг биткойнов (до массового появления майнинга на GPU и специализированных процессорах типа ASIC). Позже скрытный майнинг применялся для получения иных криптовалют. При установке торрент-клиента μTorrent (версия 3.4.2 build 28913 и позднее) предлагается установить дополнительную программу EpicScale, которая позволяет использовать ресурсы компьютера во время простоя для распределённых вычислений. Представители μTorrent заверяют, что в настоящее время сеть EpicScale используется для майнинга криптовалюты (без уточнения названия), часть полученных средств идёт на финансирование компании, часть — на благотворительность. Согласно ряду публикаций, EpicScale майнит биткойны. В других публикациях сообщается о майнинге Litecoin. В 2017 году появились сообщения о ряде сайтов, содержащих JavaScript скрытого майнинга некоторых криптовалют (такой вид майнинга в русском языке стали называть «браузерным майнингом», а в английском — «криптоджекингом»). Сходные компоненты были обнаружены в нескольких дополнениях к браузерам. По данным сентябрьского отчёта IBM X-Force, за 8 месяцев 2017 года в 6 раз увеличилось число компьютеров, заражённых вредоносным ПО для майнинга.

**2. ПРОЦЕСС МАЙНИНГА В СИСТЕМЕ**

**2.1 Обнаружение процесса в системе**

Вводим команду – top, чтобы включился мониторинг процессов в системе, в данном мониторинге отображается:

- ID процесса (PID)

- Кем он был запущен (USER)

- Приоритет (NI)

- Процент использования процессора (%CPU)

- Процент использования памяти (%MEM)

- …

- Название (COMMAND)

Теперь смотрим, есть ли в системе какой-то процесс, который загружает процессор и память (Рис.1).

  
Рис.1 - Обнаруженный майнер в системе

Обычно майнеры маскируются под существующий системный процесс (Рис.2).



Рис.2 – Майнер (kswapd0) с ID процесса 3222 замаскировался под системный процесс (kswapd0) с ID процесса 27

**2.2 Поиск исходных каталогов и файлов майнера в системе**

После обнаружения процесса майнера необходимо найти все упоминания на него в системе (Рис.3).

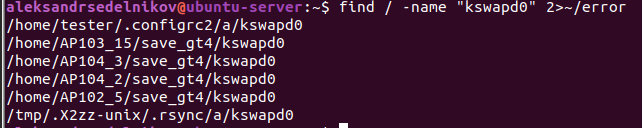


Рис.3 – С помощью команды find нашли все упоминания данного процесса

Приведённый в данном исследовании майнер называется Multios.Coinminer.Miner и хранит свои данные в каталогах .configrc2 и .rsync.

Поэтому переходим в данные каталоги и смотрим что в них расположено.

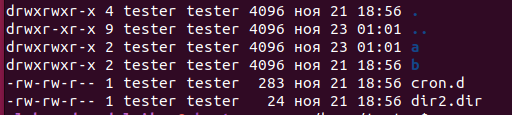


Рис.4 – Файлы в каталоге .configrc2

Начнём с каталога .configrc2.  
В нём расположены каталоги a,b и файлы cron.d и dir2.dir (Рис.4)

Каталоги a,b (Рис.5,Рис.6) хранят конфигурации майнера, но сам главный скрипт расположен в каталоге a, в файле cron.d прописана инъекция в cron системы для запуска майнера как задачи после перезагрузки (Рис.7), dir2.dir хранит путь к каталогу .configrc2 (Рис.8)



Рис.5 – Файлы в каталоге a



Рис.6 – Файлы в каталоге b

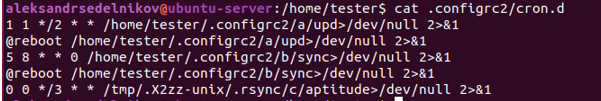


Рис.7 – Содержимое файлa cron.d



Рис.8 – Содержимое файла dir2.dir

Теперь перейдём в каталог /tmp

В данном каталоге необходимо ввести ls -all для отображения всех директорий и файлов (Рис.9).

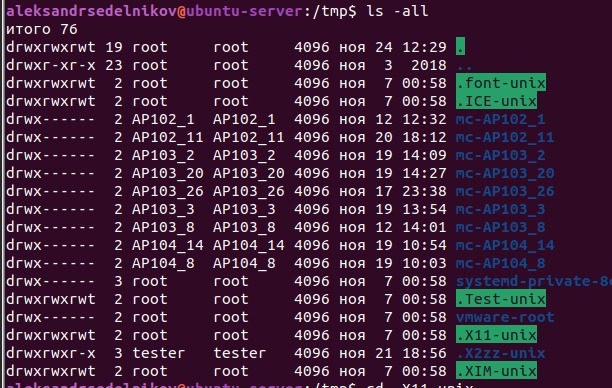


Рис.9 – Содержимое директории /tmp

Здесь мы видим, что существует какая-то директория, название, которое было в пути к скрипту майнера (а также данная директория была создана заражённым пользователем)

Переходим в данную директорию и смотрим её содержимое аналогичным образом (Рис.10).

Изображение выглядит как текст

Автоматически созданное описание

Рис.10 – Содержимое директории .X2zz-unix

В данной директории хранится сам первоисточник майнера – архив dota3.tar.gz содержащий папку .rsync и все её файлы (Рис.11).

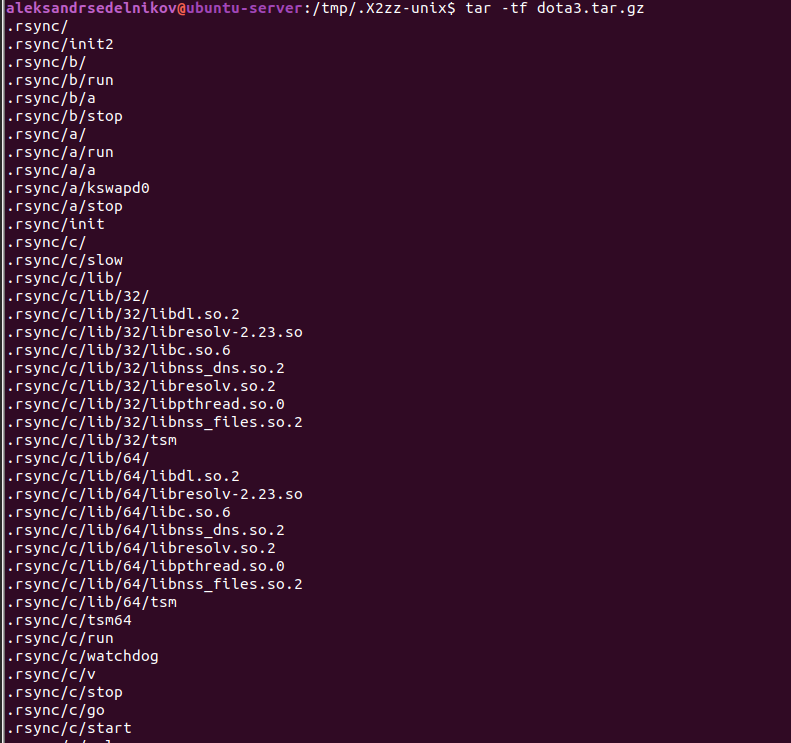


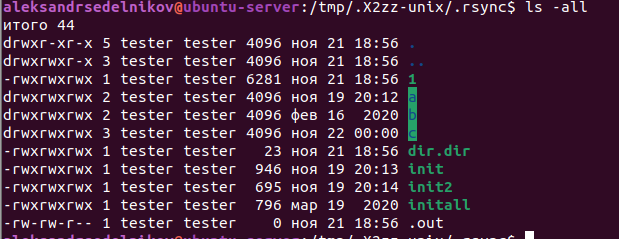
Рис.11 – Содержание архива dota3.tar.gz

Отсюда уже можно понять, что данный майнер распространяется как какая-то игра (существует игра dota2).

После попадания архива он автоматически распаковывается в данную директорию.

Перейдём в директорию .rsync

Смотрим содержимое данной директории (Рис.12)

  
Рис.12 – Содержание директории .rsync

Тут расположены файлы инициализации майнера, его способ работы и другие методы внедрения в систему, а также оригиналы директорий из директории .configrc2

**2.3 Принудительное завершение процесса майнера и удаление всех следов, связанных с процессом майнера**

Чтобы завершить процесс майнера, необходимо прописать команду kill -9 «ID процесса», в нашем случае это будет 3222.

После выполнения данной команды ещё раз смотрим мониторинг и убеждаемся, что скрипт был закрыт и повторно не открылся.

Теперь необходимо удалить все файлы и директории, в которых упоминается данный скрипт с помощью команды rm «название файла» и rm -R «название директории».

После этого нужно удалить инъекции майнера в планировщик задач (cron) с помощью команды crontab -l, пример строчек майнера на Рис.13.

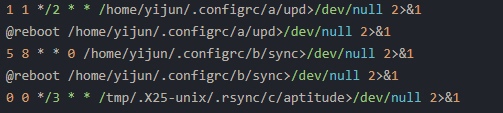


Рис.13 – Строчки майнера в планировщике задач

Последним делом остаётся перезапустить сервер и ещё раз убедиться, что никакой лишний процесс не был запущен.

**ЗАКЛЮЧЕНИЕ**

Сделаем выводы по проведённому исследованию.

Изучив понятие, виды, принцип работы, можно сказать, что добросовестные «добытчики» криптовалюты несомненно являются безобидными, однако существуют и те, которые будут скрыто майнить на вашем устройстве или сервере криптовалюту без вашего ведома, что может привести к заторможенности и сбоям в работе. Проблема скрытого майнинга очень популярна и каждый день создаются новые «заплатки» в уязвимостях систем, но также находятся всё новые уязвимости (так называемые «уязвимости 0-го дня», когда у разработчиков ПО было 0 дней для решения данной уязвимости).

В ходе исследования рассмотрели пример майнера в системе на базе Linux Ubuntu, способ обнаружения и удаления его из системы.

В конце хочется добавить, чтобы не стать жертвой данного вида вирус-программ нужно тщательно проверять ресурсы, с которых вы будете скачивать что угодно, сами скачанные файлы, не игнорировать жалобы антивирусов, даже если авторы говорят отключить их. Если очень нужна программа или файл, используйте виртуальные машины или среды запуска, которые обезопасят ваше устройство, в случае если эти файлы или программы были заражены.

**БИБЛИОГРАФИЧЕСКИЙ СПИСОК**

1. Майнинг - Википедия Свободная энциклопедия [Электронный ресурс]. URL: <https://ru.wikipedia.org/wiki/Майнинг> (дата обращения 24.11.2022)
2. Askubuntu - CPU 100% with kswapd0 process, although no swap is needed [Электронный ресурс]. URL: <https://askubuntu.com/questions/1224927/cpu-100-with-kswapd0-process-although-no-swap-is-needed> (дата обращения 24.11.2022)
3. Programming VIP - kswapd0 process mining Trojan [Электронный ресурс]. URL: <https://programming.vip/docs/kswapd0-process-mining-trojan.html> (дата обращения 24.11.2022)
4. <CODE BLOG> - Почему kswapd0 грузит CPU или как я обнаружил Multios.Coinminer.Miner [Электронный ресурс]. URL: <https://rekunenko.pp.ua/pochemu-kswapd0-gruzit-cpu-ili-kak-ya-obnaruzhil-multios-coinminer-miner> (дата обращения 24.11.2022)