УДК 621
Лізунов С.І.[1]
Верещака М.П.[2]
[1]Лізунов С.І. – канд. техн. наук, проф. ЗНТУ
[2]Верещака М.П. – студент магістратури ЗНТУ

ПРИХОВАНИЙ МАЙНІНГ ТА ЗАХИСТ ВІД НЬОГО

Майнінг - це діяльність по створенню нових структур для забезпечення функціонування криптовалютних платформ.

Для видобутку криптовалюти можливо не тільки використання власного комп'ютера, але і безлічі чужих машин [1].

Наприклад, у магазині Google Play знайшли додаток під назвою Vilny.net, що працює як VPN-сервіс, проте в той же час використовує ресурси смартфонів, щоб майніти криптовалюту Monero [2].

На сьогоднішній день прихований майнінг може зробити будь-який користувач. Для цього досить лише завантажити готову програму, написати номер свого електронного гаманця і все. Програма модифікована так, що вона не відрізняється від троянського вірусу: вона може поширюватися в мережі, копіювати сама себе на зовнішній накопичувач, приховувати свої процеси в диспетчері завдань і використовувати комп'ютер коли ним ніхто не користується.

Для прихованого видобутку криптовалюти не потрібно зламувати комп'ютер і встановлювати троян. Поки у користувача в браузері відкрита сторінка з шкідливим скриптом, процесор буде непомітно майніти.

І необов'язково, що навантаження на відеокарту або процесор має зрости до 100% - зловмисники обережні і не стануть навантажувати машину учасника своєї мережі в нерозумних межах. Ви можете, в принципі, і не помітити великої різниці, якщо у вас досить потужна техніка. Це важлива умова для збереження прихованої роботи майнера.

"Підвисання" на комп'ютері, які зникають, якщо розірвати з'єднання з інтернетом є ознакою, що ресурси вашого комп'ютера витрачаються із зовні. Варто обірвати з'єднання і шукати проблеми в системі.

Найчастіше програму майнінг ховають під системний процес svchost.exe. Для того, щоб знайти цю програму необхідно зробити наступне[3]:

1. Svchost.exe повинен завжди виконуватися від імені системи, network і local сервісів. Якщо він запущений від імені будь-якого користувача, то варто перевірити його директорію на жорсткому диску. Істинний файл знаходиться у папці Windows/system32 і ніяк інакше.

2. Слід перевірити таблицю автозавантаження Windows. У цій таблиці не повинен знаходитися файл svchost.exe. Цей процес операційна система повинна запускати самостійно, без участі користувача або шкідливої програми, яка занесла цю програму до списку автозавантажень.

Якщо програму майнінг знайдено, необхідно її видалити. Для цього слід використовувати програму Process Hacker. Криптовані процеси або упаковані процеси - найчастіше приховані. Майнер виступає саме як "упакований процес" в svchost.exe або іншій програмі, який відображається рожевим кольором в Process Hacker (packet procces). Слід відшукати такі процеси і проаналізувати їх директорію на жорсткому диску. Найчастіше вони ховаються від імені cmd.exe (прихованого командного рядка). Коли цей процес знайдено, перед тим як його зупинити, слід знайти місце розташування цього процесу. Після того, як ця програма зупинена, необхідно її видалити з жорсткого диску і, бажано, просканувати системний реєстр на посилання на цю директорію.

Якщо програму майнінгу модифікувати, то можливе знімання інформації про всі дії користувача. Тому, для захисту інформації, слід обов'язково знищувати програми майнінгу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Скрытый майнинг: найти и уничтожить [Електронний ресурс]. – Режим доступу: https://bitnovosti.com/2017/08/16/skritiy-mayning-nayti-unichtojit/

2. В украинском приложении VPN нашли майнинговый вирус [Електронний ресурс]. – Режим доступу: http://mignews.com.ua/society/19587813.html

3. Как обезопасить себя от скрытого майнинга криптовалют [Електронний ресурс]. – Режим доступу: https://tjournal.ru/59579-kak-obezopasit-sebya-ot-skrytogo-mayninga-kriptovalyut