Загребельний В.В., здобувач
Кльоц Ю.П., к.т.н., доцент
Хмельницький національний університет

ВИЯВЛЕННЯ МАЙНЕРІВ ЗА ДОПОМОГОЮ АНТИВІРУСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Виявлення вірусів-майнерів є доволі складним завданням для сучасного антивірусного програмного забезпечення (далі – АВПЗ). Майнери використовують ресурси комп'ютера для видобутку криптовалюти, дуже часто діють приховано, мінімізуючи всі видимі ознаки своєї активності. Незважаючи на те що, АВПЗ постійно оновлюється, існують суттєві недоліки у виявленні та нейтралізації ними вірусів-майнерів. Недоліки часто зумовлені такими факторами як: постійна еволюція шкідливого коду, маскуванні та адаптації вірусів, обходом евристичного аналізу та постійне використання нових методів обходу систем захисту [1, 4].

Однією з проблем виявлення майнерів, є їх здатність до маскування. Майнери часто імітують системні процеси, що значно ускладнює їх виявлення та ідентифікацію. Крім того, такі віруси постійно еволюціонують адаптуючись до нових методів виявлення. Це означає, що антивірусні бази швидко стають застарілими [1].

Ще одним викликом є дуже низька помітність майнерів. На відміну від відомих вірусів, які діють активно, майнери можуть діяти тихо, мінімізуючи використання ресурсів комп'ютера. Це дозволяє майнерам залишатися непоміченими протягом доволі тривалого часу, особливо на потужних комп'ютерах, де невелике навантаження яке спричиняє майнер, може бути непомітним [2].

Окрему проблему також становить криптоджекінг. Криптоджекінг використовує JavaScript для майнингу в браузері. Антивіруси дуже часто не здатні відрізнити легітимний код від шкідливого, так як він використовується в межах веб-сайтів. Таким чином криптоджекінг несе особливу загрозу, вражаючи користувачів які відвідують навіть довірені та відомі ресурси [2].

Ефективність АВПЗ часто обмежена ресурсами комп'ютера. Постійне сканування на наявність нових загроз значно вповільнює роботу системи, тому АВПЗ постійно шукають баланс між безпекою та продуктивністю. В результаті, майнери, що застосовують технології маскування, можуть залишатися непоміченими, якщо АВПЗ не проводить глибокий аналіз [3, 4].

Ефективне вирішення проблеми потребує комплексного підходу до проблеми. Вдосконалення евристичного аналізу з використанням штучного інтелекту та машинного навчання, дозволить більш точно виявляти аномальну поведінку. Посилення захисту браузерів з використанням спеціалізованих розширень та обмеження виконання ненадійних та не легітимних скриптів є критично важливим кроком в боротьбі з криптоджекінгом та мінімізують зараження вірусом-майнером. Постійний моніторинг мережевого трафіку для виявлення підозрілих пул-з'єднань майнінгу, та постійний моніторинг з контролем використання ресурсів комп'ютера, зокрема відеокарти та процесора. Системи моніторингу які надають інформацію в режимі реального часу та надсилають сповіщення в разі аномального збільшення використання ресурсу комп'ютера, дозволять швидко виявляти та реагувати на майнер [5, 6].

У підсумку, боротьба з вірусами-майнерами вимагає постійного вдосконалення АВПЗ та впровадження інноваційних рішень для протидії таким загрозам. Головними аспектами успішного виявлення та нейтралізації майнера є не лише вдосконалення АВПЗ, але й активний підхід, який включає в себе моніторинг, аналіз поведінки та різні превентивні заходи безпеки. Лише багатошаровий та комплексний захист, який враховує різноманітні вектори атаки та зараження вірусом, здатен забезпечити ефективний захист від прихованої загрози вірусів-майнерів.

Список використаних джерел:

1. Незаконний майнінг. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/nezakonnyy-mayning/. (дата звернення: 10.03.2025).
2. Прихований майнінг. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/skrytyy-mayning/. (дата звернення: 10.03.2025).
3. Захист від вірусів. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/zashchita-ot-virusov/. (дата звернення: 10.03.2025).
4. Шкідливі програми. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/vredonosnyye-programmy/. (дата звернення: 10.03.2025).
5. Як знайти та видалити вірус-майнер з комп'ютера. URL: https://www.binance.com/uk-UA/square/post/97665. (дата звернення: 10.03.2025).
6. Вас "майнять": як виявити і знешкодити прихований майнінг. URL: https://epravda.com.ua/publications/2018/04/20/636181/. (дата звернення: 10.03.2025).