УДК 004.056.055

А. В. Борусевич
А. В. Остапенко-Боженова

МЕТОДИ ВИЯВЛЕННЯ ЗАГРОЗ MICROSOFT WINDOWS DEFENDER

Вінницький національний технічний університет

Анотація

Розглянуто методи хмарного виявлення загроз, що дозволяють зменшити час реакції на нове шкідливе програмне забезпечення.

Ключові слова: хмарний захист, шкідливе програмне забезпечення.

Abstract

Methods of cloud threat detection was analyzed, which allows the reaction time to new malicious software to be reduced.

Keywords: cloud security, malicious software.

Вступ

Сьогодні можна спостерігати тенденції зменшення випадків масового зараження шкідливими програмними засобами великих компаній та підприємств, та збільшення їх матеріальних збитків через простій чи сповільнення роботи обладнання в процесі протидії таким програмам. Потужність ПК кінцевих користувачів не дозволяє швидко та зручно здійснювати сканування антивірусним програмним забезпеченням. Одним із сучасних рішень є застосування хмарного захисту [1, 2].

Метою роботи є дослідження методів виявлення загроз Block at first/second sight у Microsoft Windows Defender, що дозволяють зменшити час виявлення та протидії новому шкідливому програмному забезпеченню (ПЗ).

Результати дослідження

Block at first sight [1] («блокування при першому виявленні») - один із двох методів пришвидшення реакції на нові види шкідливого ПЗ. Головною метою даного методу є запобігання зараження «нульового пацієнта», тобто пристрою користувача, з якого розпочнеться зараження та розповсюдження шкідливого ПЗ.

Коли користувач намагається завантажити файл з Інтернету (виконуваний по типу .exe, .js, .vbs або макрос), хеш-значення надсилається до Microsoft Intelligent Security Graph (центр аналізу) на перевірку. В разі, якщо центр аналізу надає відповідь, що файл безпечний, користувач має змогу запустити файл.

Block at second sight [1] («блокування при другому виявленні») - другий метод пришвидшення реакції на нові віруси. «Зібрати, проаналізувати, зробити висновок синхронно по відношенню до файлу, який вперше побачили» - головна мета даного методу.

Якщо під час аналізу у хмарі система не може надати однозначну відповідь щодо безпеки робити з досліджуваним об’єктом, користувачу дають змогу запустити файл, але лише після того, як копія цього файлу буде надіслана до хмари. Після отримання копії файлу, у хмарі виконується детальний та більш тривалий аналіз, в результаті якого буде сформована відповідь для майбутніх запитів щодо цього файлу .

Схематично робота методу Block at second sight представлена на рис. 1.

З рис. 1 випливає, що першого користувача буде «заражено» шкідливим ПЗ, проте наступний користувач буде в безпеці, оскільки система матиме змогу детально проаналізувати роботу невідомого ПЗ.

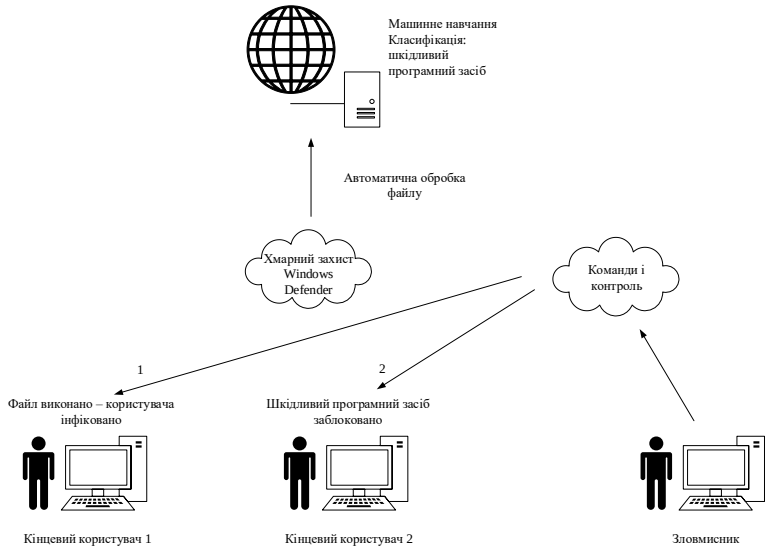

Рис. 1. Результат роботи методу «Block at second sight»

Використовуючи комплексну роботу досліджуваних методів захисту, можна значно зменшити час реакції на нові віруси, оскільки при спрацюванні «блокування при другому виявленні» система матиме екземпляр шкідливого програмного забезпечення [2].

Висновки

Встановлено, що розглянуті методи, при комплексному використанні, дозволяють швидше створювати нові сигнатури шкідливого ПЗ і, відповідно, зменшити кількість заражених пристроїв, оскільки тепер час реакції зменшується з кількох годин до кількох секунд [2].

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. How to Enable or Disable Windows Defender Block at First Sight in Windows 10 : веб-сайт. URL: https://www.tenforums.com/tutorials/70329-enable-windows-defender-block-first-sight-windows-10-a.html, вільний – Назва з екрана.

2. Использование технологий следующего поколения в защитнике Microsoft Defender Antivirus с помощью облачной защиты : веб-сайт. URL: https://docs.microsoft.com/ru-ru/windows/security/threat-protection/microsoft-defender-antivirus/utilize-microsoft-cloud-protection-microsoft-defender-antivirus, вільний – Назва з екрана.

Борусевич Артур Вячеславович — студент групи 1БС-17б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: borusevych.av@gmail.com

Остапенко-Боженова Аліна Василівна — асистент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця. e-mail: ostapenko-bozhenova_a_v@vntu.edu.ua

Borusevych Artur V. — Faculty for Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : borusevych.av@gmail.com

Ostapenko-Bozhenova Alina V. — assistant of the department of information security, Vinnytsia National Technical University, Vinnytsia, e-mail: ostapenko-bozhenova_a_v@vntu.edu.ua