

АНАЛІЗ ПАРАМЕТРІВ БЕЗПЕКИ MICROSOFT EDGE

Вінницький національний технічний університет

Анотація

Запропоновано аналіз параметрів безпеки нового браузеру Microsoft Edge, що дозволило оцінити якість та рівень безпеки користувачів у web-просторі.

Ключові слова: Windows, Edge, Microsoft, web-загрози.

Abstract

A study of the security parameters of a new browser from Windows - Microsoft Edge, which allowed to assess the quality and security of users in the web-space.

Keywords: Windows, Edge, Microsoft, web threats.

Вступ

Windows 10 постачається з двома вбудованими браузерами: Microsoft Edge та Internet Explorer. Новий браузер Microsoft Edge побудований на основі проекту з відкритим вихідним кодом Chromium - того ж проекту на якому заснований Google Chrome та Opera. Такий вибір передбачає, що в основі Microsoft Edge закладені перевірені рішення безпеки, дизайну та архітектури [1].

Метою роботи є дослідження параметрів безпеки браузеру Microsoft Edge та аудит основних технологій, що забезпечують захист кінцевих користувачів.

Результати дослідження

Microsoft Edge розроблений з урахуванням підвищених вимог безпеки, допомагаючи захищати користувачів від все більш витончених і поширених мережових атак на Windows. Microsoft Edge розроблений як універсальний застосунок для Windows, змінюючи концепцію браузеру на застосунок, розробники докорінно змінили модель процесу, і тепер весь контент живе в ізольованому програмному середовищі контейнера додатку.

Microsoft Edge підтримує можливості апаратної ізоляції [2]. Як частина Windows 10 Pro або Enterprise, Application Guard в Захиснику Windows (Application Guard) ненадійні сайти опрацьовуються в ядрі, ізольованому від локального пристрою і внутрішніх мереж. Ненадійні сайти працюють в «контейнері», тому при виникненні атаки вони ізольовані від решти програмних застосунків користувача та інших учасників мережі.

Microsoft Edge працює в 64-розрядній версії за замовчуванням [1, 2]. Так як Microsoft Edge не підтримує застарілі елементи ActiveX або сторонні виконавчі розширення, більше немає причини запускати 32-розрядні процеси на 64-розрядній системі. Перевагами такого рішення є :

- відмова від підтримки елементів ActiveX, VBScript и Browser Helper Objects, що значно зменшує можливість реалізації атак зловмисників;
- використання технології рандомізації адресного простору Windows (ASLR) що перешкоджає зловмисникам отримати точні адреси вразливих місць пам'яті [3].

Edge реалізований з підтримкою функції біометричної автентифікації [1] з використанням можливостей утиліти Windows Hello таких як, розпізнавання обличчя та відбитку пальця.

За результатами незалежного дослідження NSS Labs [4] вбудований в Microsoft Edge SmartScreen блокує більше спроб фішингу та шкідливих програм, ніж безпечний перегляд Google Chrome (рис. 1). SmartScreen забезпечує перевірку репутації сайтів і завантаження в режимі реального часу, коли користувачі працюють в мережі, і є частиною Microsoft Intelligent Security Graph, який збирає сигнали і аналітичні дані, отримані з глобальної мережі глобальних активів, дослідників і партнерів Microsoft. Виконуючи перевірки динамічних хмарних списків небезпечних сайтів і завантажень, Microsoft Edge допомагає виявляти і блокувати навіть ефемерні загрози, які швидко зникають [4].

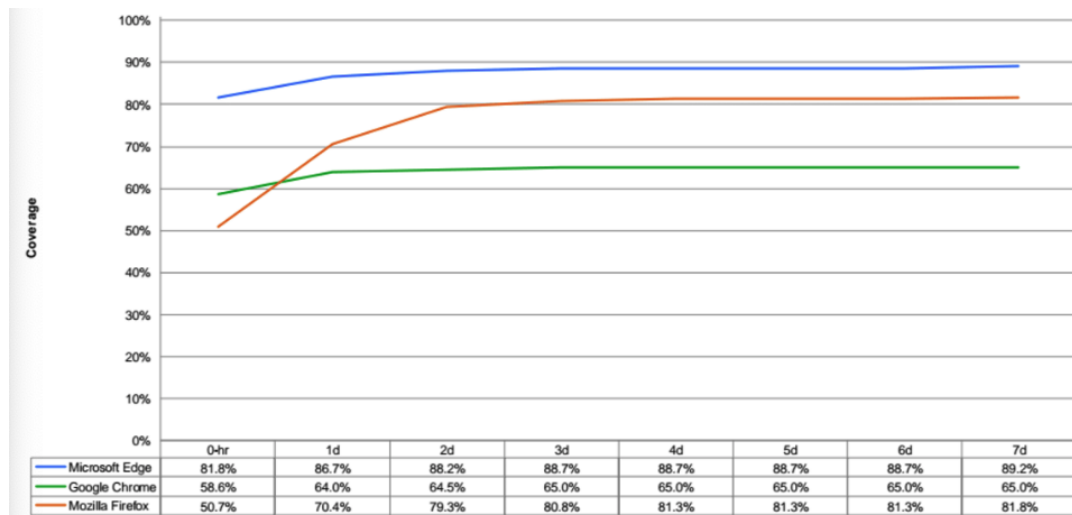


Рис. 1. Дослідження заблокованого шкідливого забезпечення [4].

Аналізуючи результати наведені в рис.1 можна бачити, що Microsoft Edge з фільтром SmartScreen заблокував 95,5% спроб фішингу та 98,5% шкідливих програмних застосунків в порівнянні з показниками режиму безпечного перегляду в Google Chrome 86,9% і 86,0% відповідно [4].

Microsoft Edge і ОС Windows 10 застосовують нову концепцію продукції – поняття сервісу [1]. Це означає, що продукт постійно знаходиться в процесі удосконалення, в ньому з'являються нові функції і можливості. У випадку з Edge така концепція є виправданою, тому що браузер досить «молодий» і пропонує не всі функції та інструменти, які можна знайти в аналогах, наприклад в Google Chrome. В той же час, з точки зору запропонованих параметрів, Microsoft Edge задає новий рівень вимог до безпеки у своєму сегменті.

Висновки

Проведене дослідження дає підстави робити висновки, що Microsoft Edge має високий рівень захисту, порівняно з аналогами, та низку додаткових функцій захисту від інтернет загроз які працюють в тандемі з операційною системою Windows 10.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Вопросы и ответы для ИТ-специалистов [Електронний ресурс]. - Режим доступу: URL: <https://docs.microsoft.com/ru-ru/microsoft-edge/deploy/microsoft-edge-faq> - Назва з екрану
2. Защита от веб-угроз в контексте целевых атак [Електронний ресурс]. - Режим доступу: URL: <https://www.kaspersky.ru/blog/kwts-enterprise-6/26167/> - Назва з екрану
3. ASLR [Електронний ресурс]. - Режим доступу: URL: <https://www.zdnet.com/article/microsoft-says-aslr-behavior-in-windows-10-is-a-feature-not-a-bug/> - Назва з екрану
4. NSS Lab find Edge on Windows 10 [Електронний ресурс]. - Режим доступу: URL: <https://mspoweruser.com/nss-labs-find-edge-windows-10-s-safer-chrome-chromebooks/> - Назва з екрану

Лавров Вадим Валерійович — студент групи 2БС-17б, факультет інформаційних технологій комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: vadosssss228@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

Lavrov V. V. - student of group 2BS-17b, Faculty of Information Technologies of Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: vadosssss228@gmail.com

Ostapenko-Bozhenova A. V. - assistant. Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, e-mail: ostapenko-bozhenova_a_v@vntu.edu.ua