

УДК 004.056.55

Бережний О.Ю.¹, Корольков Р.Ю.²

¹ асп. НУ «Запорізька політехніка»

² канд. техн. наук, доц. НУ «Запорізька політехніка»

ДОСЛІДЖЕННЯ МЕТОДІВ ОБХОДУ АНТИВІРУСНОГО ЗАХИСТУ MICROSOFT DEFENDER

У сучасних умовах зростання кіберзагроз, пов'язаних як з діяльністю організованих злочинних угруповань, так і зі спеціалізованими державними кіберструктурами, ефективний захист інформаційних систем набуває критичного значення [1]. Найпоширеніша у світі ОС Windows оснащена вбудованим антивірусним засобом Microsoft Defender, здатність якого виявляти сучасні техніки компрометації має вирішальне значення для безпеки користувачів і організацій. У дослідженні перевірено здатність Microsoft Defender виявляти як типові, так і складні методи запуску шкідливого коду у вигляді зворотної оболонки (reverse shell). Експериментальне тестування виконувалося у віртуальному середовищі на базі Windows 11 з активованим Microsoft Defender та Kali Linux як атакуючої машини.

Було реалізовано низку технік, зокрема запуск PowerShell-скриптів, обфускацію команд через кодування в Base64, fileless-виконання, використання легітимних системних компонентів Windows (LOLBins) – таких як regsvr32.exe і msbuild.exe, а також створення кастомного виконуваного .exe-файла з вбудованим корисним навантаженням на C#.

Експерименти показали, що Microsoft Defender ефективно виявляє більшість типових методів запуску зворотної оболонки, зокрема тих, що використовують команду Invoke-Expression, параметр -EncodedCommand, обфусковані PowerShell-скрипти та fileless-техніки виконання. Більшість

таких методів блокуються або на етапі запуску, або за рахунок інтеграції з інтерфейсом AMSI (Antimalware Scan Interface). Найбільш ефективним методом обходу антивірусного захисту виявився запуск шкідливого коду за допомогою msbuild.exe, який є частиною .NET Framework. У цьому випадку XML-файл із вбудованим C#-кодом успішно виконував шкідливий код, який ініціював встановлення зворотного TCP-з'єднання, без виявлення з боку Defender. Додаткове використання режиму прихованого запуску (-w hidden) дозволило здійснити експлуатацію без видимих ознак для кінцевого користувача. Зазначимо, що подібні техніки застосовуються в реальних атаках. Наприклад, хакерські групи Carbanak та FIN7, які спеціалізуються на атаках проти фінансового сектору та підприємств ритейлу, використовували msbuild.exe для прихованого запуску шкідливого C#-коду, що унеможливлювало сигнатурне виявлення з боку Defender [2].

Зведене порівняння протестованих методів, їх виявлення Defender та причин блокування або обходу наведено в таблиці 1.

Таблиця 1 – Порівняння ефективності методів обходу Defender

Метод	Тип виконання	Виявлення Defender	Причина виявлення
msfvenom PowerShell	+ .ps1 reverse shell	Так	Сигнатурне виявлення PowerShell-пейлоаду
Base64 + runner.ps1	Шифрований скрипт + Invoke-Expression	Так	Використання IEX і декодування Base64
TCP reverse shell (чистий PowerShell)	Fileless-скрипт	Так	Поведінковий аналіз + виявлення AMSI
EncodedCommand (.bat)	Прихований запуск PowerShell	Так	Декодування Base64 + команда TCP-клієнта
regsvr32 + .sct (JScript)	LOLBin + скриптова вставка	Так	Активність scriptlet-файлу з TCP-з'єднанням
msbuild + XML (inline C#)	XML із вбудованим C#-кодом	Ні	Відсутність сигнатур на кастомний C#
msbuild + -w hidden	Тихий запуск PowerShell	Ні	Приховане виконання без видимих ознак

Таким чином, отримані результати демонструють наявність реальних векторів обходу захисту Microsoft Defender через легітимні інструменти

Windows. Це підтверджує доцільність впровадження багаторівневої моделі безпеки (Defense in Depth). Такий підхід передбачає використання EDR-рішень із поведінковим аналізом, впровадження політик AppLocker або Windows Defender Application Control (WDAC), обмеження запуску утиліт типу msbuild.exe у середовищах, де їх використання не передбачено, ізоляцію інструментів розробки та виконання коду, а також навчання персоналу виявляти загрози, пов'язані з використанням легітимних системних утиліт (LOLBins) у шкідливих цілях.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. CISA. Russian GRU Cyber Actors Conduct Global Infrastructure Attacks [Електронний ресурс]. – 2024. – Режим доступу: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-249a> – Дата доступу: 03.04.2025.
2. Trend Micro. Carbanak and FIN7 Attack Techniques [Електронний ресурс]. – 2021. – Режим доступу: https://www.trendmicro.com/en_us/research/21/d/carbanak-and-fin7-attack-techniques.html – Дата доступу: 04.04.2025.