УДК 004.056.5 **DOI:10.30837/rt.2024.2.217.05**

К.М. ШУЛІКА, Д.С. БАЛАГУРА, канд. техн. наук, З.М. СИДОРЕНКО

АНАЛІЗ МЕТОДІВ ОБХОДУ СУЧАСНИХ СИСТЕМ ЗАХИСТУ КІНЦЕВИХ ТОЧОК

Вступ

Сьогодні неможливо уявити захист даних без використання комплексних рішень для захисту кінцевих точок інформаційної системи організації: серверів і робочих станцій. Вимоги до подібних рішень включають забезпечення прозорості моніторингу процесів і автоматизований пошук аномалій в системах, а також можливість реагувати на інциденти безпеки для спеціалістів команд кібербезпеки [1, 2]. Метою статті є огляд та аналіз методів обходу комплексних рішень для захисту кінцевих точок (EDR), які широко використовуються зловмисниками. В статті виділяються та описуються визначні риси кожного з методів обходу EDR та наводяться рекомендації з протидії ним.

Endpoint Detection and Response

EDR (Endpoint Detection and Response) є типом кросплатформенного програмного забезпечення, що наразі найчастіше використовується для моніторингу подій, формування та формалізації інцидентів безпеки та реагування на інциденти на кінцевих точках інформаційної системи організації. EDR часто використовуються в SOC (Security Operational Center) для забезпечення безпеки в масштабі інфраструктури, але існує можливість обходу і цих комплексних рішень [1, 3, 4].

Метод обходу Anti-Malware Scan Interface (AMSI)

Першим і одним з найпоширеніших методів є обхід AMSI. AMSI – це структура Microsoft, яка дозволяє стороннім рішенням для захисту від шкідливих програм мати доступ до компонентів і програм Microsoft, таких як PowerShell, механізми сценаріїв, .NET Framework і WMI. EDR використовують цю структуру для сканування файлів, пам’яті та потоків на наявність зловмисного корисного навантаження. Зловмисники можуть використовувати кілька різних методів, щоб обійти AMSI, наприклад «відображення» (reflection), перехоплення COM-сервера та коригування пам’яті [5].

Схему роботи AMSI наведено на рис. 1.

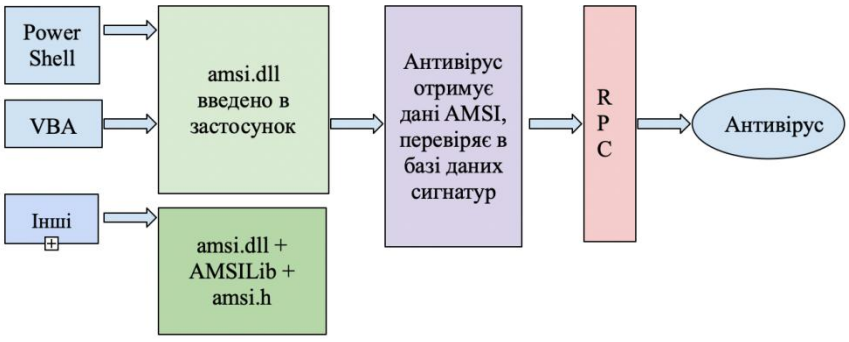

Рис. 1 Схема роботи AMSI

Прикладом нещодавньої атаки з використанням методів обходу AMSI є троян віддаленого доступу Agent Tesla (RAT), який використовував метод коригування пам’яті, щоб уникнути виявлення завантажувача другого етапу атаки та кінцевого корисного навантаження. Перший етап нової версії зловмисного програмного забезпечення включає програму-завантажувач на основі .NET. Завантажувач збирає обфускований код із таких веб-сайтів, як Pastebin і Hastebin. Потім програма встановлення Agent Tesla намагається перезаписати код у

AMSI Microsoft. Спочатку завантажувач намагається отримати адресу пам'яті AmsiScanBuffer (функція Microsoft, також відома як amsi.h, яка сканує буфер на наявність шкідливих програм). Це робиться шляхом виклику amsi.dll Windows за допомоги функції Windows LoadLibraryA, щоб отримати базову адресу DLL. Потім він використовує функцію GetProcAddress для отримання базової адреси та процедуру «AmsiScanBuffer» для отримання адреси функції. Коли Agent Tesla отримує адресу AmsiScanBuffer, він виправляє перші 8 байтів функції в пам'яті. Це змушує AMSI повертати помилку (код 0x80070057), через що всі сканування пам'яті AMSI видаються недійсними. Це блокує програмне забезпечення для захисту кінцевих точок із підтримкою AMSI, фактично змушуючи їх пропускати подальше сканування AMSI для динамічно завантажуваних вузлів у процесі Agent Tesla. Оскільки це відбувається на ранній стадії роботи завантажувача першого етапу, він попереджає виявлення AMSI будь-яких компонентів завантажувача, завантажувача другого етапу та самого корисного навантаження.

В останніх версіях трояну він має додаткову можливість розгортання клієнта Tor для приховування своїх комунікацій, а також використання месенджеру Telegram для викрадання даних. Ці додаткові функції ускладнюють і динамічний, і статичний аналіз антивірусних рішень нового покоління, а також виявлення індикаторів компрометації шкідливого програмного забезпечення (такі як IP-адреси, домени, хеші) для аналітиків з кібербезпеки.

В цьому прикладі варто звернути увагу на те, що механізм обходу EDR може бути вбудований в файли, що мають механізм самозапуску і додавання в автозавантаження при ввімкненні пристрою, тому етап обходу антивірусного ПЗ в системі таким чином перегукується з етапом закріплення на комп'ютері жертви [6, 7].

Зазвичай шкідливе ПЗ Agent Tesla надходить під виглядом вкладення у фішинговий електронний лист. За статистикою Sophos у грудні 2020 р. на Agent Tesla припадало 20 % шкідливих вкладень в електронні листи, а це 1/5 від кількості фішинг-листів, що потрапляють до користувачів Windows. Враховуючи, що Windows наразі залишається найбільш використовуваною операційною системою в світі (69 % всіх користувачів, для порівняння – macOS користується лише 21 % користувачів), а це приблизно 1.4 білліони активних пристроїв, ризик натрапити саме на цей тип трояну із вбудованим обходом AMSI наближається до 1:1 – 45 %.

Запобігання методам обходу AMSI

Методам обходу AMSI можна запобігти, обираючи для корпоративної інфраструктури EDR рішення із вбудованим механізмом захисту, який припиняє процеси, що націлені на компрометацію AMSI, одним із наступних методів: перехопити функцію .NET SetValue, тобто заборонити прямий доступ до змінних amsiInitFailed\amsiSession\amsiContext, або перехопити AmsiUnInitialize() та перехопити PowerShell до та після виконання ScriptBlock, тобто виявити внесення змін в змінну amsiInitFailed (з «False» на «True»), яка не була викликана AmsiUnInitialize(). Про наявність подібного захисту можливо уточнити у постачальника програмного рішення EDR або протестувати самостійно під час тест-драйву.

Також варто розглянути альтернативний шлях: наразі все більше компаній переходять з продуктів Microsoft на інші платформи, такі як macOS та Linux, оскільки вони менш поширені і містять менше вбудованих інструментів, що за своєю архітектурою сприятливі для компрометації [8].

Метод «зняття з крючка» (unhooking)

Наступна техніка, «зняття з крючка» (unhooking) експлуатує той факт, що Windows використовує набір API (наприклад, системний виклик), які можна викликати для виконання інструкцій, що вимагають прямого доступу до системи або рівня ядра. Більшість рішень EDR використовують шлюз ntdll.dll шляхом «зачеплення» до нього, щоб спостерігати за підозрілими зверненнями до пам'яті.

«Зняття з крючка» зловмисники можуть використовувати для завантаження нової непідключеної версії ntdll.dll після того, як Windows завантажила підключену версію в EDR під час запуску процесу. У цей момент EDR не бачить будь-якого коду, який виконується, і не може відстежувати адресу повернення для будь-яких викликів API, що створює так звану «сліпу зону» роботи антивірусного рішення. Якщо зловмисник піде ще далі, то «повторно зачепить» EDR наприкінці своєї операції, щоб приховати факт індикатори своєї присутності [9, 10].

На цьому прикладі зробимо припущення, чому існують методи обходу EDR, майже однакові для рішень від різних вендорів? Тому що EDR використовують однакові шляхи оптимізації роботи агентів і системи в цілому, за рахунок таких рішень забезпечується швидкість їх роботи, але в результаті можуть бути створені подібні «пробоїни».

Запобігання методу «зняття з крючка»

Подібно до прямих системних викликів, метод «зняття з крючка» допомагає зловмиснику уникнути виявлення антивірусом, перешкоджаючи роботі EDR. Цю проблему можна вирішити, запобігаючи модифікації «крючків» (hooks) агента, відстежуючи зміни в цих областях пам'яті. Будь-які спроби отримати доступ до цих областей пам'яті вважатимуться зловмисними та мають блокуватись – про наявність відповідних модулів захисту більше інформації можна отримати від постачальника ПЗ.

Метод завантаження рефлективної DLL

Завантаження рефлективної DLL – це техніка віддаленого запуску коду, використання якої дозволяє зловмиснику завантажити DLL із пам'яті в існуючий процес замість завантаження її з диска. Рішення EDR зазвичай захищають систему, відстежуючи DLL тільки під час їх завантаження з диска, тому завантаження рефлективної DLL забезпечує ще один спосіб уникнення радару EDR. Цей метод часто використовується в поєднанні з одним або декількома іншими техніками та присутній в рамках відомих фреймворків CobaltStrike і Metasploit, які є вагомою частиною інструментарію сучасного хакера. Оскільки обидва фреймворки є надзвичайно поширеними як серед етичних хакерів, так і серед зловмисників, використання інструментів для експлуатації методу завантаження рефлективної DLL є більш ніж доступним за наявності достатніх теоретичних знань.

Запобігання методу завантаження рефлективної DLL

Захиститись від експлуатації цього методу можливо, відстежуючи виділення локальних областей пам'яті, які використовуються під час завантаження рефлективної DLL, і запобігаючи спробам завантаження PE (Portable Executable) файлів із цих областей пам'яті.

Розглянуті в роботі методи обходу EDR та механізми захисту від них представлено в табл. 1.

Таблиця 1

Методи обходу EDR та механізми захисту

Методи обходу EDR	**Механізми захисту**
Обхід Anti-Malware Scan Interface (AMSI)	Захист від перехоплення функції. NET SetValue або перехоплення AmsiUnInitialize() та PowerShell до та після виконання ScriptBlock.
«Зняття з крючка» (unhooking)	Вбудований захист від модифікації «крючків» (hooks) агента.
Завантаження рефлективної DLL	Вбудований захист від виділення локальних областей пам'яті, використовуваних під час завантаження рефлективної DLL, і запобігання спробам завантаження Portable Executable файлів із цих областей пам'яті.

Рекомендації щодо протидії обходу EDR

Якщо постачальник програмного забезпечення не може надати документацію, в якій надано підтвердження стійкості рішення вказаним атакам, то варто розглянути можливість підключення внутрішньої команди компанії для тестування. Узагальнено, тестування EDR рішення на предмет вразливості до описаних типів обходу може бути виконано спеціалістами з тестування на проникнення, а також представниками SOC команди – аналітиками та слідчими з пошуку загроз (threat hunters).

Всі наведені методи можна віднести до стадій атаки Виконання (Execution) та Ухилення від захисту (Defense Evasion) по методології матриці MITRE ATT&CK.

Наведено лише деякі з багатьох способів, за допомогою яких зловмисники можуть обійти захист системи, маючи набір правильних інструментів які легко знайти та застосувати.

Хоча рішення EDR чудово підходять для виявлення відомих зловмисних загроз та їх активності для ідентифікації атаки, коли під час атаки зловмисник намагається викрасти дані та завдати шкоди існує велика прогалина в зупиненні шкідливих процесів та їх підпроцесів, а також в механізмах пошуку перших ознак невідомих загроз, перш ніж вони зможуть потрапити на кінцеву точку. EDR найкраще підходить для виявлення і виконання первинного блокування файлових атак на фізичних комп'ютерах, саме тому не варто розглядати EDR як єдиний інструмент захисту корпоративної мережі.

Роль EDR полягає у виявленні зловмисної поведінки після того, як загроза потрапила у середовище, що надто пізно, щоб зупинити такі складні атаки, як завантаження програми із вбудованим механізмом обходу захисту, тому як загальну рекомендацію можна виділити необхідність доповнювати інструментарій додатковими продуктами для тестування на проникнення, форензики, аналізу мережевого трафіка, зовнішніми та внутрішніми сканерами вразливостей, системами менеджменту корпоративного поштового клієнта, системами автоматизованого реагування на загрози тощо. Також варто звернути увагу на те, що будь-яке антивірусне рішення повинно мати захист від видалення агенту, встановленого на кінцевій точці (tampering protection), що деактивується унікальним токеном. Це дозволить як мінімум отримати не скомпрометовані логи системи, що були передані в консоль EDR, і як максимум – отримати віддалений доступ до скомпрометованої системи для реагування і пошуку слідів зловмисника, без ризику що він видалить агент, маючи права адміністратора пристрою [11].

Профілактика має бути першою лінією захисту, щоб зупинити відомі та виявити ще невідомі загрози, активність програм-вимагачів та загроз нульового дня.

Під профілактикою розуміємо:

1) побудову комплексу з рішень для моніторингу та реагування на інциденти безпеки (XSOAR, в складі якого EDR або XDR, SIEM, IDS/IPS, сканери вразливостей тощо);
2) покращення існуючих процесів, налаштування існуючих інструментів;
3) патч-менеджмент;
4) проведення навчання з кібергігієни для спеціалістів, проведення тестових фішинг-розсилок;
5) ризик-менеджмент та оцінку активності зловмисників в сфері діяльності компанії для попередження невідомих атак;
6) тестування на проникнення і закриття всіх відомих шляхів входу на кінцеві точки компанії;
7) оцінку безпеки партнерів для попередження атаки ланцюга поставок (supply chain).

При дотриманні зазначених рекомендацій можна розраховувати на кращі показники ефективності EDR та покращення загальної стійкості інфраструктури до майбутніх кібератак із використанням методів обходу EDR.

Висновки

Для розуміння наявних ризиків і шляхів їх зниження у статті наведено і проаналізовано три методи обходу EDR що використовуються найчастіше: AMSI обхід, «зняття з крючка»

(unhooking), та завантаження рефлективної DLL. Наведено опис кожного метода, приклади використання в ході атаки на інфраструктуру, а також надані рекомендації щодо протидії та запобіганню використання зловмисниками описаних методів.

Представлені рекомендації можуть бути використані в ході формування процесів в команді з кібербезпеки, для покращення процесів роботи з наявним рішенням EDR, також під час проведення менеджменту ризиків та оцінки профілю інформаційної безпеки організації.

Список літератури:

1. Когут Ю.І. Кібервійна та безпека об'єктів критичної інфраструктури : практ. посіб. Київ : Консалтингова компанія «Сідкон, 2021, С. 132–214.
2. Ушатов В., Сєвєрінов О.В. Проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки. 2019.
3. Sievierinov O., Ovcharenko M., Vlasov A. Enterprise Security Operations Center // Computer and information systems and technologies. 2021.
4. Баклан Я.А., Сєвєрінов О.В. Аналіз систем захисту кінцевих точок від складних загроз EDR // Endpoint Detection and Response. 2022.
5. Antivirus Bypass Techniques: Learn practical techniques and tactics to combat, bypass, and evade antivirus software. Yehoshua Nir, 2021.
6. Malware Tech Blog [Електронний ресурс]. Режим доступу: https://malwaretech.com/2023/12/silly-edr-bypasses-and-where-to-find-them.html.
7. Malware Tech Blog [Електронний ресурс]. Режим доступу: https://malwaretech.com/2023/12/an-introduction-to-bypassing-user-mode-edr-hooks.html.
8. Infosec Write-Ups Blog [Електронний ресурс]. Режим доступу: https://infosecwriteups.com/exploring-antivirus-and-edr-evasion-techniques-step-by-step-part-1-6459563b12ea.
9. IRed Team Blog [Електронний ресурс]. Режим доступу: https://www.ired.team/offensive-security/defense-evasion/bypassing-cylance-and-other-avs-edrs-by-unhooking-windows-apis.
10. Evading EDR: The Definitive Guide to Defeating Endpoint Detection Systems. Matt Hand, 2023.
11. GitHub репозиторій Awesome EDR Bypass [Електронний ресурс]. Режим доступу: https://github.com/tkmru/awesome-edr-bypass.

Надійшла до редколегії 30.05.2024

Відомості про авторів:

Шуліка Катерина Максимівна – Харківський національний університет радіоелектроніки, магістр кафедри безпеки інформаційних технологій; Україна; e–mail: kateryna.shulika@nure.ua

Балагура Дмитро Сергійович – канд. техн. наук, Харківський національний університет радіоелектроніки, доцент кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління; Україна; e-mail: dmytro.balahura@nure.ua; ORCID: https://orcid.org/0009-0006-9839-3317

Сидоренко Зоя Михайлівна – Харківський національний університет радіоелектроніки, аспірантка кафедри безпеки інформаційних технологій; Україна; e–mail: zoia.sydorenko@nure.ua; ORCID: https://orcid.org/0000-0002-0104-6807