АНАЛІЗ МЕТОДІВ ОБХОДУ СУЧАСНИХ СИСТЕМ ЗАХИСТУ КІНЦЕВИХ ТОЧОК (EDR)

Шуліка К.М., Балагура Д.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Сьогодні неможливо уявити захист даних без використання комплексних рішень для захисту кінцевих точок: серверів і робочих станцій. Вимоги до подібних рішень включають забезпечення прозорості процесів і автоматизований пошук аномалій в системах, а також можливість реагувати на інциденти безпеки для спеціалістів команд кібербезпеки [1, 2].

EDR (Endpoint Detection and Response) є типом кросплатформеного програмного забезпечення, що наразі найчастіше використовується для моніторингу подій, формування та формалізації інцидентів безпеки та реагування на інциденти на кінцевих точках [3].

EDR часто використовуються в SOC (Security Operational Center) для забезпечення безпеки в масштабі інфраструктури, але і ці комплексні рішення можливо обійти [4, 5].

Метою доповіді є огляд та аналіз широко використовуваних зловмисниками методів обходу комплексних рішень для захисту кінцевих точок (EDR).

В доповіді розглядаються три методи обходу EDR о використовуються найбільш широко: AMSI обхід, «зняття з крючка» (unhooking), та завантаження рефлективної DLL.

Наводиться опис кожного метода, приклад використання в ході атаки на інфраструктуру, а також надаються рекомендації щодо протидії та запобігання використанню зловмисниками такого методу.

Ці рекомендацію можуть бути використані в ході формування процесів в команді з кібербезпеки.

Робляться висновки щодо вірогідності використання наведених методів обходу EDR на основі їх доступності для зловмисника у глобальній мережі.

Список літератури

1. Ушатов В., Сєвєринов О.В. (2019). Проблемы оперативного обнаружения и реагирования на инциденты информационной безответственности.

2. "Кібервійна та безпека об'єктів критичної інфраструктури", Юрій Когут, Україна, Сідконб 2021

3. "Evading EDR: The Definitive Guide to Defeating Endpoint Detection Systems", Matt Hand, No Starch Press 2023.

4. Sievierinov O., Ovcharenko M., Vlasov A. Enterprise Security Operations Center. *COMPUTER AND INFORMATION SYSTEMS AND TECHNOLOGIES*, 2021.

5. "Antivirus Bypass Techniques: Learn practical techniques and tactics to combat, bypass, and evade antivirus software", Yehoshua Nir, Packt Publishing 2021