Maestría en

CIBERSEGURIDAD

Trabajo previo a la obtención de título de

Magister en Ciberseguridad

AUTORES:

Albán Alvear, Mónica Mishell

Gamboa Romero, Christian Andrés

Monserrate Pozo, Ronny Bryan

Mora Mora, Sandra Yajaira

TUTOR:

Iván Galo Reyes

TEMA:

Análisis de Técnicas de Evasión y Exfiltración de Datos en Entornos Empresariales: Evaluación de la Eficacia de Sistemas EDR y XDR

REINVENTEMOS EL FUTURO

Resumen

El presente trabajo presenta diferentes técnicas de evasión y exfiltración de datos en un entorno empresarial simulado del sector financiero (Cooperativa de Ahorro y Crédito), con el objetivo de evaluar la eficiencia de los sistemas de seguridad como EDR (Endpoint Detection and Response) y XDR (Extended Detection and Response), debido que en la actualidad existen muchas Cooperativas que sufren múltiples amenazas a diario y que, en muchas ocasiones a pesar de contar con estas herramientas de seguridad no suelen detectar todos las técnicas de evasión y exfiltración.

En este proyecto se diseñó un entorno de pruebas, en donde se simuló técnicas avanzadas para evadir protecciones reales, utilizando equipos con sistemas operativos que forman parte en los entornos corporativos. Se utilizaron dos plataformas; Sophos Intercept X y Elastic Defend para ejecutar las pruebas.

Se realizaron pruebas como: descarga y ejecución de archivos maliciosos generados con Metasploit y ofuscados, las cuales arrojaron que Sophos EDR/XDR y Elastic Defend si detectaron y bloquearon estos ataques demostrando un buen desempeño ante amenazas conocidas.

Sin embargo, los ataques más avanzados como; revershell mediante Powershell y ataque mediante un archivo malicioso en aplicación de mensajería como WhatsApp, fueron exitosos dado que ambas plataformas no detectaron el ataque y se logró obtener comando y control.

Palabras Claves: EDR, XDR, evasión, exfiltración, ofuscado, Metasploit, Powershell, reverse Shell.

Abstract

This paper presents different data evasion and exfiltration techniques in a simulated business environment in the financial sector (a Savings and Credit Cooperative). The goal is to evaluate the effectiveness of security systems such as EDR (Endpoint Detection and Response) and XDR (Extended Detection and Response). This is because many credit unions currently face multiple threats daily and, despite having these security tools, often fail to detect all evasion and exfiltration techniques.

For this project, a testing environment was designed to simulate advanced techniques for evading real-world protections using computers with operating systems found in corporate environments. Two platforms were used: Sophos Intercept X and Elastic Defend to run the tests. Tests were conducted, including downloading and executing malicious files generated with Metasploit and obfuscated files. These tests showed that Sophos EDR/XDR and Elastic Defend did detect and block these attacks, demonstrating good performance against known threats.

However, more advanced attacks, such as a reverse shell using Powershell and an attack using a malicious file in a messaging app like WhatsApp, were successful, as both platforms failed to detect the attack, and command and control was achieved.

Keywords: EDR, XDR, evasion, exfiltration, obfuscation, Metasploit, Powershell, Reverse Shell.