Maestría en

CIBERSEGURIDAD

Trabajo previo a la obtención de título de

Magister en CIBERSEGURIDAD

AUTOR/ES:

Lalon Yanza Víctor Stalin

Martínez Jurado Andrés Damián

Tamayo Rosero Diego Francisco

Troya Proaño Hernán Augusto

TUTOR/ES:

Alejandro Cortés López

TEMA:

Análisis evolutivo y técnicas de propagación del Malware Mirai: Variantes, métodos de infección y su impacto en la ciberseguridad de dispositivos IoT

Quito - Ecuador

2024– 2025

REINVENTEMOS EL FUTURO

RESUMEN

El malware Mirai se ha consolidado como una de las amenazas más significativas a nivel global, debido a su capacidad para comprometer dispositivos IoT y conformar extensas redes de bots utilizadas en ataques de denegación de servicio distribuido (DDoS). Desde su aparición en 2016, Mirai ha evolucionado generando múltiples variantes con capacidades cada vez más sofisticadas en cuanto a evasión, persistencia y explotación, lo que dificulta su mitigación.

Con el objetivo de reducir la propagación del malware Mirai en dispositivos IoT, se analiza su comportamiento, las técnicas de propagación que emplea, así como sus distintas variantes, con el propósito de fortalecer la seguridad y prevenir posibles ataques.

Para su estudio, se llevó a cabo un análisis teórico sobre el funcionamiento del malware, complementado con una evaluación práctica en entornos controlados mediante el uso de sandboxing y honeypots, lo que permitió observar su comportamiento real sin comprometer infraestructuras legítimas. Además, se valoraron herramientas de detección y mitigación como Wireshark, Suricata, Snort y Cuckoo Sandbox, con el fin de establecer recomendaciones sobre su aplicación en entornos con dispositivos IoT.

Este trabajo busca generar conocimiento técnico y proponer estrategias efectivas de detección y mitigación, contribuyendo así a mejorar las prácticas de protección en entornos digitales vulnerables.

Palabras Claves: Malware, IoT, sandbox, honeyspot, DDOS, infraestructura, Wireshark, Suricata, Snort y Cuckoo

ABSTRACT

Mirai malware has become one of the most significant global threats due to its ability to compromise IoT devices and form extensive botnets used in Distributed Denial of Service (DDoS) attacks. Since its emergence in 2016, Mirai has evolved, generating multiple variants with increasingly sophisticated capabilities in terms of evasion, persistence, and exploitation, which complicates mitigation efforts.

In order to reduce the spread of Mirai malware in IoT devices, this study analyzes its behavior, the propagation techniques it employs, as well as its different variants, with the aim of strengthening security and preventing potential attacks.

For this purpose, a theoretical analysis of the malware's operation was conducted, complemented by a practical evaluation in controlled environments using sandboxing and honeypots. This allowed the observation of real-world behavior without putting legitimate infrastructures at risk. Furthermore, detection and mitigation tools such as Wireshark, Suricata, Snort, and Cuckoo Sandbox were evaluated to provide recommendations for their use in environments with IoT devices.

This work aims to generate technical knowledge and propose effective detection and mitigation strategies, thereby contributing to the improvement of protection practices in vulnerable digital environments.

Keywords: Malware, IoT, sandbox, honeypot, DDoS, infrastructure, Wireshark, Suricata, Snort, Cuckoo