Panorama de amenazas

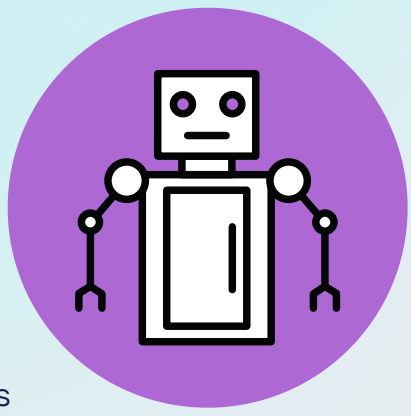
1 ULTIMOS 10 AÑOS

Vulnerabilidades

- Se han dado a conocer **26.447** vulnerabilidades en 2023, superando en más de 1.500 CVEs el número total de vulnerabilidades reveladas en 2022.

2 NUMEROLOGIA

Amenazas de vulnerabilidad para 2023



- En 2023, menos del **1%** de las vulnerabilidades representaron el mayor riesgo y fueron explotadas activamente.
- **109** tenían evidencia conocida de explotación y estaban listadas en el catálogo de Vulnerabilidades Explotadas Conocidas
- **97** vulnerabilidades fueron explotadas en el entorno real pero no estaban incluidas en la lista KEV

PRINCIPALES TIPOS DE VULNERABILIDAD 3

1.Security Feature Bypass.
2.Ejecución Remota De Código.
3.Escalada De Privilegios. Validación Y Cambio De Tipo De Entradas.
4. Manipulación Del Buffer De Memoria.

4 TIEMPO MEDIO PARA EXPLOTAR LAS VULNERABILIDADES

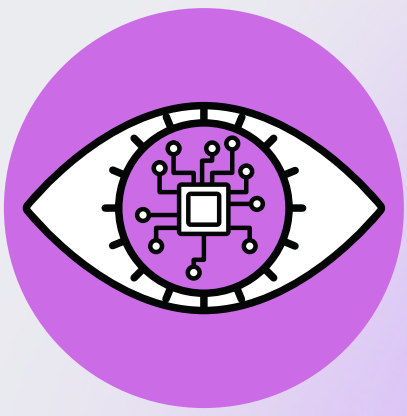
vulnerabilidades de alto riesgo en 2023

El **25%** de las vulnerabilidades de alto riesgo fueron explotadas inmediatamente, con el código de explotación publicado el mismo día en que la vulnerabilidad fue divulgada públicamente.

VULNERABILIDADES EXPLOTADAS POR TIPO DE PRODUCTO 5

Vulnerabilidades explotadas por tipo de producto en 2023

Un tercio de las vulnerabilidades de alto riesgo afectaron a dispositivos de red y aplicaciones web. Esto indica que los atacantes se enfocaron en estos tipos de productos debido a su exposición y potencial impacto.



6 ACTORES DE AMENAZAS Y GRUPOS DE RANSOMWARE

Tipos de actores de amenazas y grupos de ransomware

Los actores de amenazas incluyen grupos de **ransomware** como **LockBit y Cerber**, que explotaron **20 vulnerabilidades en 2023.** Además, grupos de malware y botnets también estuvieron activos, explotando **15 vulnerabilidades.**

7 PRINCIPALES TÉCNICAS Y MÉTODOS

Principales técnicas y métodos de MITRE ATT&CK utilizados en estos exploits

Las principales tácticas de MITRE ATT&CK observadas en 2023 fueron:

- Explotación de servicios remotos.
- Explotación de aplicaciones expuestas públicamente.
- Explotación para escalamiento de privilegios.

VULNERABILIDADES MÁS EXPLOTADAS 8

Algunas de las vulnerabilidades más explotadas en 2023 incluyeron aquellas con código de explotación disponible y que fueron activamente utilizadas por actores de amenazas, malware y grupos de ransomware. Específicamente, **115 vulnerabilidades** fueron explotadas rutinariamente por estos actores.

9 ACTORES DE AMENAZAS MÁS ACTIVOS DE 2023

Grupos de ransomware como **LockBit y Cerber** estuvieron entre los actores de amenazas más activos en 2023, explotando múltiples vulnerabilidades para llevar a cabo sus ataques.

MALWARE MÁS ACTIVO DE 2023 10

Además de los grupos de ransomware mencionados, diversas cepas de malware y botnets estuvieron activas en 2023, explotando 15 vulnerabilidades para comprometer sistemas y redes.

REFERENCIAS

- Abbasi, S. (2024, January 4). 2023 *Threat Landscape Year in Review: If everything is critical, nothing is | Qualys Security Blog. Qualys Security Blog.* https://blog.qualys.com/vulnerabilities-threat-research/2023/12/19/2023-threat-landscape-year-in-review-part-one#2023-statistics
- IT Digital Media Group. (2024, January 19). 2023: *más vulnerabilidades, pero solo un 1% fueron críticas. Actualidad | IT Digital Security.* https://www.itdigitalsecurity.es/actualidad/2024/01/2023-mas-vulnerabilidades-pero-solo-un-1-fueron-criticas