BOLETÍN INFORMATIVO 29DIC-04ENE2024

CONCIBER

Comité Nacional de Seguridad Cibernética

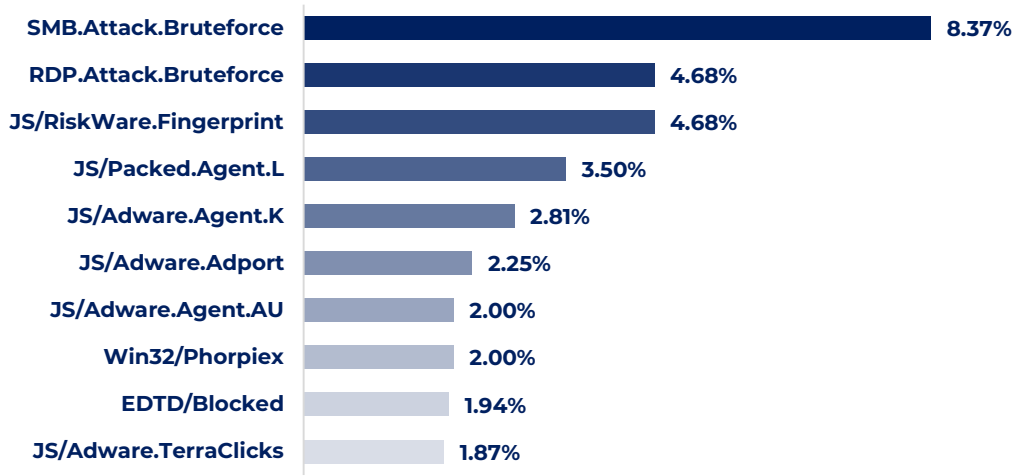
Boletín de Ciberseguridad

Amenazas cibernéticas en Guatemala

IMPORTANTE

29DIC-04ENE2024 Según el reporte semanal de Virus Radar de ESET sobre las ciberamenazas más utilizadas por ciberdelincuentes en Guatemala, la amenaza SMB.Attack.Bruteforce (8.37 %) registró mayor incidencia; seguida de RPD/Attack.Bruteforce (4.68 %) y JS/RiskWare.Fingerprint (4.68 %).

Principales amenazas cibernéticas en Guatemala



Fuente: Virus Radar
https://virusradar.com/en/statistics/10

kaspersky	Amenazas de tipo ransomware en Guatemala	IMPORTANTE

29DIC-04ENE2024 El mapa en tiempo real de ciberamenazas de KASPERSKY mostró que en Guatemala el software malicioso con mayor incidencia durante la semana fue el troyano Trojan-Ransom.Win32.Stop.gen (50.00 %); seguido de Trojan-Ransom.Win32.Blocker.gen (16.67 %).

Principales troyanos de tipo ransomware en Guatemala

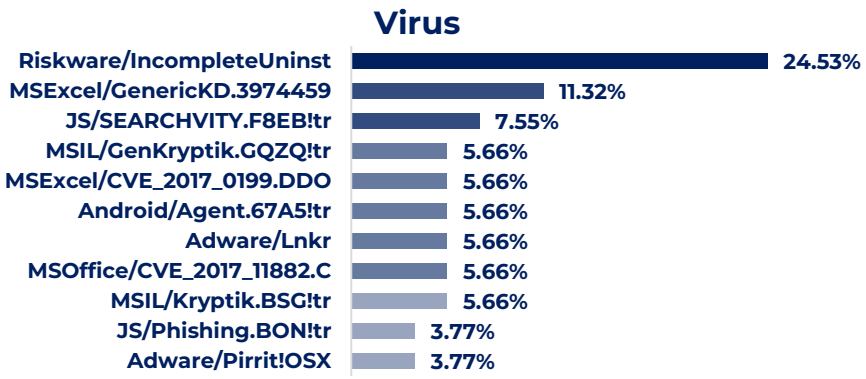
Ransomware	Frecuencia
Trojan-Ransom.Win32.Stop.gen	50.00%
Trojan-Ransom.Win32.Blocker.gen	16.67%
trojan-ransom.win32.Crypen.gen	16.67%
Trojan-Ransom.Win32.PornoBlocker.ejtx	16.67%

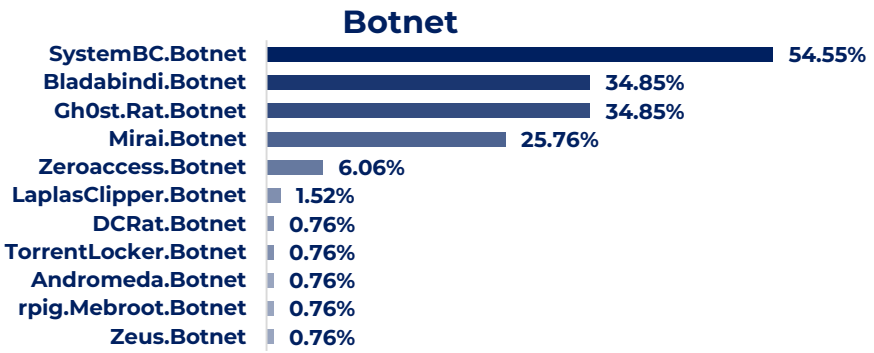
Fuente: CYBERMAP
https://cybermap.kaspersky.com/es/stats#country=38&type=RMW&period=w

FORTINET	Reporte de amenazas cibernéticas en Guatemala	IMPORTANTE

29DIC-04ENE2024 Principales amenazas cibernéticas en Guatemala, según reporte semanal de FORTIGUARD.

Principales amenazas





Fuente: FORTIGUARD
https://www.fortiguard.com/threat-research/map/country/GT

SPAMHAUS	Países con más incidencia de botnets	IMPORTANTE

29DIC-04ENE2024 Según reporte semanal de SPAMHAUS, los países con más spam-bots a nivel mundial son: China, EE.UU., India, Indonesia y Algeria. La mayoría de los bots detectados, fueron utilizados como vectores de ataque de spam, phishing, fraude de clics, DDoS y otras actividades maliciosas.

Países con mayor índice de botnets en el mundo

Posición	País	Número de Bots
1	China	628,815
2	EE.UU.	365,105
3	India	239,186
4	Indonesia	125,004
5	Algeria	103,126
6	Tailandia	82,354
7	Vietnam	80,736
8	Brasil	69,409
9	Reino Unido	63,207
10	Egipto	63,030

Fuente: SPAMHAUS
https://www.spamhaus.org/statistics/botnet-cc/

one	**Asamblea de la República de Albania sufrió ataques cibernéticos**	**IMPORTANTE**

29DIC2023 La Asamblea de Albania y la empresa de telecomunicaciones «One Albania», fueron objeto de ataques cibernéticos, según Autoridad Nacional de Certificación Electrónica y Seguridad Cibernética -AKCESK-. La Asamblea es el órgano legislativo de Albania y es responsable de promulgar leyes y supervisar al gobierno. Los ataques podrían haber comprometido la seguridad de la Asamblea y haber puesto en riesgo información confidencial.

https://thehackernews.com/2023/12/albanian-parliament-and-one-albania.html

G	**Malware roba información de Google OAuth para mantener acceso a cuentas**	**IMPORTANTE**

03ENE2024 El malware aprovecha el punto de Google OAuth «MultiLogin», permitiendo el robo de información y mantener el acceso a las cuentas de Google de usuarios, incluso después de que estos reestablezcan sus contraseñas. Lo anterior, permite a los atacantes robar datos sensibles (direcciones de correo electrónico, números de teléfono y contraseñas de otras cuentas). También podrían utilizar las cuentas para realizar actividades maliciosas, como enviar spam o difundir malware.

https://thehackernews.com/2024/01/malware-using-google-multilogin-exploit.html

debian	**Múltiples vulnerabilidades del kernel de Debian Linux**	**ALTO (Puntuación CVSS: 7.0)**

03ENE2024 Se identificaron múltiples vulnerabilidades en el kernel de Debian Linux, identificadas como CVE-2023-6531, CVE-2023-6622, CVE-2023-6817, CVE-2023-6931, CVE-2023-51779, CVE-2023-51780, CVE-2023-51781 y CVE-2023-51782, las cuales afectan las versiones de Debian Bookworm anteriores a 6.1.69-1. Un atacante remoto, podría aprovechar algunas de estas vulnerabilidades para desencadenar una condición de denegación de servicio, elevación de privilegios y divulgación de información confidencial en el sistema objetivo.

https://www.hkcert.org/security-bulletin/debian-linux-kernel-multiple-vulnerabilities_20240103
https://lists.debian.org/debian-security-announce/2024/msg00000.html

android	**Android detectó múltiples vulnerabilidades**	**ALTO (Puntuación CVSS: 7.8)**

03ENE2024 Sistema operativo Android detectó múltiples vulnerabilidades identificadas como CVE-2023-21245, CVE-2023-40085, CVE-2024-0015, CVE-2024-0016, CVE-2024-0017, CVE-2024-0018, CVE-2024-0019, CVE-2024-0020, CVE-2024-0021 y CVE-2024-0023, permitiendo afectar el nivel de parche de seguridad de Android anterior al 05ENE2024. Un atacante podría aprovechar algunas de estas vulnerabilidades para activar la elevación de privilegios y la divulgación de información confidencial en el sistema objetivo.

https://www.hkcert.org/security-bulletin/android-multiple-vulnerabilities_20240104
https://source.android.com/docs/security/bulletin/2024-01-01?hl=es

	Múltiples vulnerabilidades de Google Chrome	**ALTO (Puntuación CVSS: 7.3)**

04ENE2024 Google Chrome identificó múltiples vulnerabilidades identificadas como CVE-2024-0222, CVE-2024-0223, CVE-2024-0224 y CVE-2024-0225, las cuales afectan a las tecnologías Google Chrome anteriores a 120.0.6099.199 (Linux), 120.0.6099.199 (Mac), 120.0.6099.199/200 (Windows) y 120.0.6099.193 (Android). El atacante remoto podría aprovechar algunas de estas vulnerabilidades para desencadenar la ejecución remota de código y una condición de denegación de servicio en el sistema objetivo.

https://www.hkcert.org/security-bulletin/google-chrome-multiple-vulnerabilities_20240104
https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop.html