BOLETÍN INFORMATIVO 05-11ENE2024

CONCIBER

Comité Nacional de Seguridad Cibernética

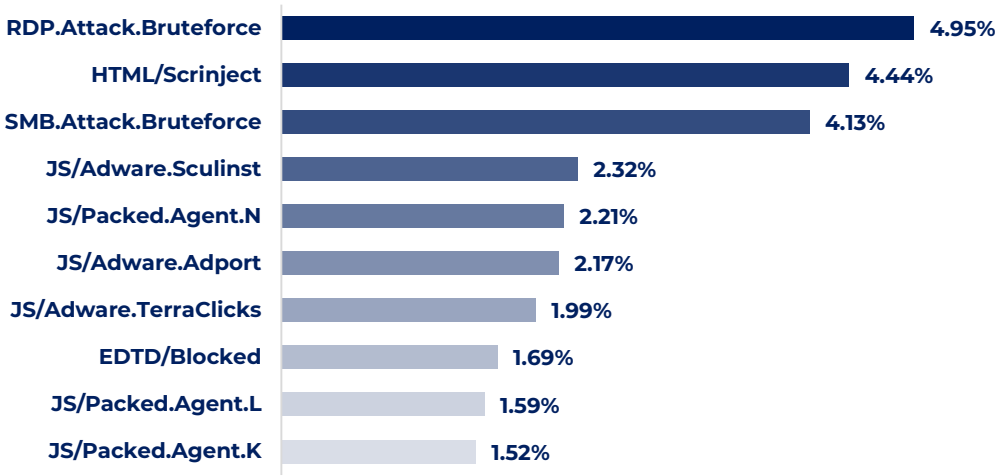
Boletín de Ciberseguridad

Amenazas cibernéticas en Guatemala

IMPORTANTE

05-11ENE2024 Según el reporte semanal de Virus Radar de ESET sobre las ciberamenazas más utilizadas por ciberdelincuentes en Guatemala, la amenaza RPD.Attack.Bruteforce (4.95 %) registró mayor incidencia; seguida de HTML/Scrinject (4.44 %) y SMB.Attack.Bruteforce (4.13 %).

Principales amenazas cibernéticas en Guatemala



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

kaspersky	Amenazas de tipo ransomware en Guatemala	IMPORTANTE

05-11ENE2024 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.MSIL.Agent.gen (40.74 %); seguido de trojan-ransom.win32.Blocker.dap (18.52 %).

Principales troyanos de tipo ransomware en Guatemala

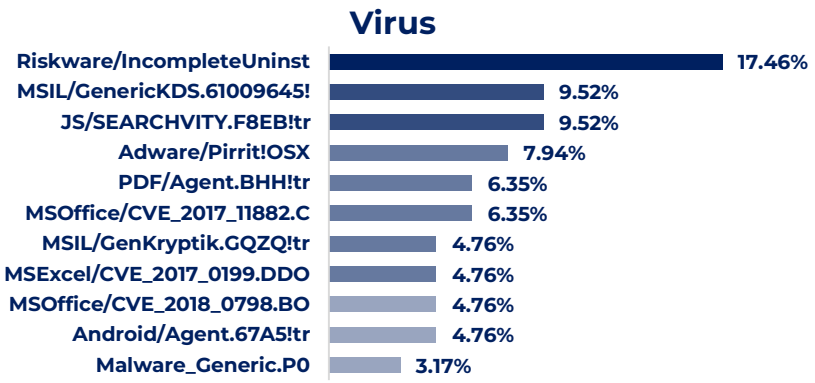
Ransomware	Frecuencia
Trojan-Ransom.MSIL.Agent.gen	40.74%
trojan-ransom.win32.Blocker.dap	18.52%
Trojan-Ransom.Win32.Autoit.b	18.52%
trojan-ransom.win32.Crypen.gen	11.11%
Trojan-Ransom.Win32.Stop.a	3.70%
Trojan-Ransom.MSIL.Blocker.gen	3.70%
Trojan-Ransom.Win32.Locky.gen	3.70%

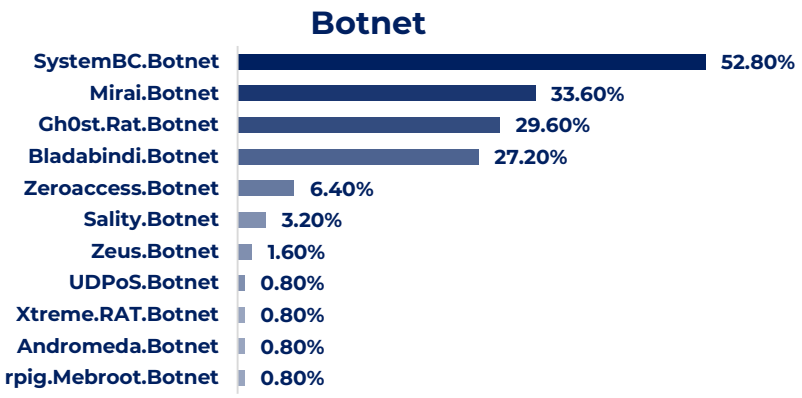
Fuente: CYBERMAP
https://cybermap.kaspersky.com/es/stats#country=38&type=RMW&period=w

FORTINET	Reporte de amenazas cibernéticas en Guatemala	IMPORTANTE

05-11ENE2024 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

05-11ENE2024 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	676,435
2	EE.UU.	402,306
3	India	275,674
4	Indonesia	147,021
5	Algeria	120,548
6	Tailandia	94,750
7	Brasil	85,814
8	Vietnam	83,743
9	Egipto	69,976
10	Pakistán	64,972

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

macOS	**Nueva amenaza de puerta trasera para macOS procedente de hackers norcoreanos**	**IMPORTANTE**

05ENE2024 Investigadores de ciberseguridad descubrieron nueva puerta trasera de Apple macOS «SpectralBlur», que comparte similitudes de malware atribuido a actores de amenazas norcoreanos. SpectralBlur es capaz de cargar/descargar archivos, ejecutar un shell, actualizar su configuración, eliminar archivos, hibernar o suspender, basándose en comandos emitidos desde el servidor de comando y control. Además, podría utilizarse para robar datos confidenciales, instalar otros malware o comprometer aún más la seguridad de un sistema macOS.

https://thehackernews.com/2024/01/spectralblur-new-macos-backdoor-threat.html

SAMSUNG	**Múltiples vulnerabilidades de productos Samsung**	**ALTO (Puntuación CVSS: 7.8)**

05ENE2024 Múltiples vulnerabilidades en productos Samsung identificadas como CVE-2023-33063, CVE-2023-33106 y CVE-2023-33107, las cuales afectan a los sistemas Android 11, 12, 13 y 14. Un atacante remoto podría aprovechar algunas de estas vulnerabilidades para provocar denegación de servicio, elevación de privilegios, ejecución remota de código, manipulación de datos y divulgación de información confidencial en el sistema objetivo.

https://www.hkcert.org/security-bulletin/samsung-products-multiple-vulnerabilities_20240105
https://security.samsungmobile.com/securityUpdate.smsb

	**Grupo de hackers pro Irán atacó a Albania con malware «Wiper»**	**IMPORTANTE**

06ENE2024 Grupo de operaciones iraní «Homeland Justice» lleva a cabo una serie de ciberataques contra organizaciones albanesas (empresas privadas, instituciones gubernamentales y el parlamento albanés) desde JUL2022 hasta la actualidad. Los atacantes utilizan un limpiador llamado No-Justice para borrar los datos de las máquinas afectadas. El borrado de datos podría provocar la pérdida de información crítica, aunado a la interrupción de operaciones y daños financieros.

https://thehackernews.com/2024/01/pro-iranian-hacker-group-targeting.html

	Microsoft Edge detectó múltiples vulnerabilidades	**ALTO (Puntuación CVSS: 8.8)**

09ENE2024 Microsoft Edge identificó múltiples vulnerabilidades identificadas como CVE-2024-0222, CVE-2024-0223, CVE-2024-0224 y CVE-2024-0225 afectando a la tecnología Microsoft Edge anterior a 120.0.2210.121. Un 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/microsoft-edge-multiple-vulnerabilities_20240109
https://msrc.microsoft.com/update-guide/vulnerability/

	Vulnerabilidad de omisión de restricciones de seguridad de Google Chrome	**ALTO (Puntuación CVSS: 7.3)**

10ENE2024 Google Chrome identificó una vulnerabilidad identificada como CVE-2024-0333, la cual afecta a las tecnologías Google Chrome anterior a 120.0.6099.216 (Linux), anterior a 120.0.6099.216 (Mac) y anterior a 120.0.6099.216/217 (Windows). Un atacante remoto podría aprovechar esta vulnerabilidad para activar la omisión de restricciones de seguridad en el sistema objetivo. Se recomienda actualizar a la versión 120.0.6099.216 (Linux) o posterior, versión 120.0.6099.216 (Mac) o posterior y a la versión 120.0.6099.216/217 (Windows) o posterior.

https://www.hkcert.org/security-bulletin/google-chrome-security-restriction-bypass-vulnerability_20240110
https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_9.html

ubuntu	**Múltiples vulnerabilidades del kernel de Ubuntu Linux**	**MEDIO (Puntuación CVSS: 5.5)**

11ENE2024 Múltiples vulnerabilidades en productos Ubuntu identificados como; CVE-2023-3006, CVE-2023-3773, CVE-2023-4244, CVE-2023-5090, CVE-2023-5158, CVE-2023-5178, CVE-2023-5345, CVE-2023-5633, CVE-2023-5717, CVE-2023-6111, CVE-2023-6176, CVE-2023-20588, CVE-2023-31085, CVE-2023-37453, CVE-2023-39189, CVE-2023-39192, CVE-2023-39193, CVE-2023-39194, CVE-2023-39198, CVE-2023-42754, CVE-2023-45863, CVE-2023-45898. Dichas fallas afectan a los sistemas Ubuntu 16.04 ESM, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS y Ubuntu 23.10. Un atacante remoto podría aprovechar algunas de estas vulnerabilidades para desencadenar una condición de denegación de servicio, ejecución remota de código y divulgación de información confidencial en el sistema objetivo.

https://www.hkcert.org/security-bulletin/ubuntu-linux-kernel-multiple-vulnerabilities_20240111
https://ubuntu.com/security/notices/USN-6548-4