BOLETÍN INFORMATIVO 08-14DIC2023

CONCIBER

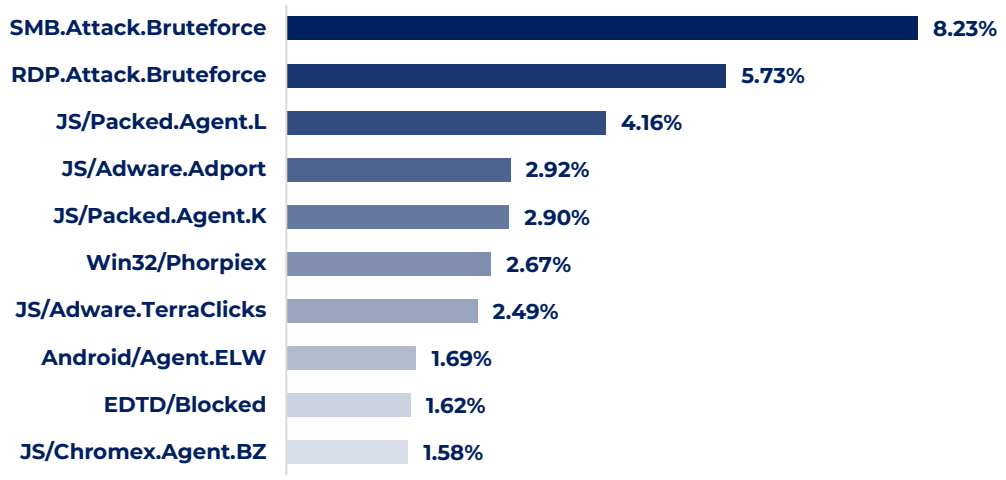
Comité Nacional de Seguridad Cibernética

Amenazas cibernéticas en Guatemala

IMPORTANTE

08-14DIC2023 Según el reporte semanal «Virus Radar» de ESET sobre las ciberamenazas más utilizadas por ciberdelincuentes en Guatemala, la amenaza SMB.Attack.Bruteforce (8.23 %) registró mayor incidencia; seguida de RPD/Attack.Bruteforce (5.73 %).

Principales amenazas cibernéticas en Guatemala



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

kaspersky	**Amenazas de tipo ransomware en Guatemala**	**IMPORTANTE**

08-14DIC2023 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.Crypen.gen (42.11 %); seguido de Trojan-Ransom.MSIL.Agent.gen (21.05 %).

Principales troyanos de tipo ransomware en Guatemala

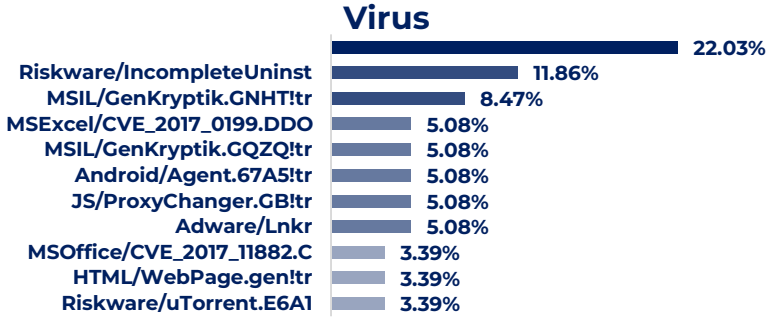
Ransomware	Frecuencia
trojan-ransom.win32.Crypen.gen	42.11%
Trojan-Ransom.MSIL.Agent.gen	21.05%
Trojan-Ransom.MSIL.Blocker.gen	10.53%
Trojan-Ransom.Win32.Stop.gen	5.26%
Trojan-Ransom.Win32.Blocker.gen	5.26%
Trojan-Ransom.Win32.Crypen.afmu	5.26%
trojan-ransom.nsis.Onion.pef	5.26%
Trojan-Ransom.Python.Agent.a	5.26%

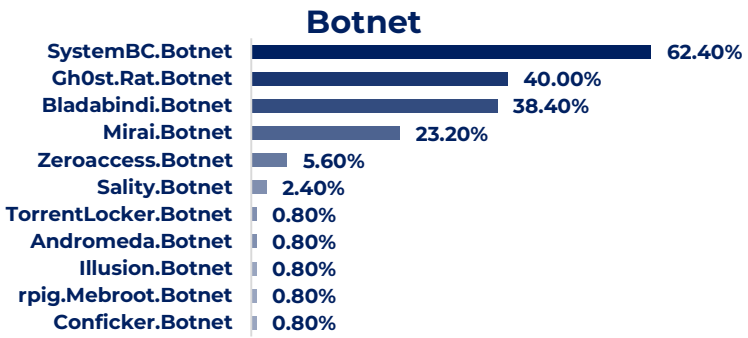
Fuente: CYBERMAP
https://cybermap.kaspersky.com/es/stats#country=38&type=RMW&period=w

FORTINET	**Reporte de amenazas cibernéticas en Guatemala**	**IMPORTANTE**

08-14DIC2023 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

08-14DIC2023 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	703,963
2	EE.UU.	341,169
3	India	299,302
4	Indonesia	182,185
5	Algeria	153,778
6	Brasil	134,162
7	Tailandia	109,683
8	Vietnam	78,377
9	Pakistán	73,150
10	Egipto	70,179

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

	**Fallos del módem 5G afectó dispositivos iOS y Android**	**IMPORTANTE**

08DIC2023 Una colección de fallas de seguridad en la implementación del firmware de los módems de redes móviles 5G, afectaron a cientos de modelos de teléfonos inteligentes con Android e iOS. Los ataques intentan engañar a un teléfono inteligente o un dispositivo habilitado para 5G para conectar una estación base no autorizada (gNB), generando consecuencias no deseadas.

https://thehackernews.com/2023/12/new-5g-modems-flaws-affect-ios-devices.html

	**Múltiples Vulnerabilidades afectaron a productos Apple**	**CRÍTICO**

11DIC2023 Apple emitió una alerta sobre múltiples vulnerabilidades identificadas como CVE-2020-19185, CVE-2020-19186, CVE-2020-19187, CVE-2020-19188, CVE-2020-19189, CVE-2020-19190, CVE-2023-5344, CVE-2023-42842, CVE-2023-42874, CVE-2023-42882, CVE-2023-42883, CVE-2023-42884, CVE-2023-42886, CVE-2023-42890, CVE-2023-42891, CVE-2023-42894, CVE-2023-42897, CVE-2023-42898, CVE-2023-42899, CVE-2023-42900, CVE-2023-42901, CVE-2023-42902, CVE-2023-42903, CVE-2023-42904, CVE-2023-42905, CVE-2023-42906, CVE-2023-42907, CVE-2023-42908, CVE-2023-42909, CVE-2023-42910, CVE-2023-42911, VE-2023-42912, CVE-2023-42914, CVE-2023-42916, CVE-2023-42917, CVE-2023-42919, CVE-2023-42922, CVE-2023-42923, CVE-2023-42924, CVE-2023-42926, CVE-2023-42927, CVE-2023-42932, CVE-2023-45866, que afecta a las tecnologías; «versiones anteriores a iOS 16.7.3 y iPadOS 16.7.3, versiones anteriores a iOS 17.2 y iPadOS 17.2, versiones anteriores a macOS Monterey 12.7.2, versiones anteriores a macOS Ventura 13.6.3, versiones anteriores a macOS Sonoma 14.2, versiones anteriores a Safari 17.2, versiones anteriores a tvOS 17.2, versiones anteriores a watchOS 10.2»

Un atacante podría aprovechar algunas de estas vulnerabilidades para desencadenar una condición de denegación de servicio, suplantación de identidad, ejecución remota de código y divulgación de información del sistema afectado.

https://support.apple.com/es-es/HT201222
https://www.hkcert.org/security-bulletin/apple-products-multiple-vulnerabilities_20231212

	Apple lanzó actualizaciones de seguridad para corrección de fallas críticas	**CRÍTICO (Puntuación CVSS de 8.8)**

12DIC2023 Apple emitió parches de seguridad para iOS, iPadOS, macOS, tvOS, watchOS y navegador safari para abordar 12 vulnerabilidades que abarcan AVEVideoEncoder, ExtensionKit, Find My, ImageIO, Kernel, Safari Private Browsing y WebKit. Entre las fallas destaca «CVE-2023-45866», un problema de seguridad crítico en Bluetooth que podría permitir a un atacante en una posición privilegiada de la red inyectar pulsaciones de teclas falsificando un teclado.

https://thehackernews.com/2023/12/apple-releases-security-updates-to.html

Microsoft	**Microsoft emitió boletín mensual de actualización de seguridad**	**Importante**

13DIC2023 Microsoft lanzó una actualización de seguridad para los productos; Browser (EDGE), Windows Systems, Microsoft Dynamics, Microsoft Office, Extended Security Updates (ESU), Azure, System Center. Un atacante podría aprovechar las vulnerabilidades existentes en las tecnologías afectadas para desencadenar una condición de denegación de servicio, suplantación de identidad, ejecución remota de código, falsificación y divulgación de información del sistema afectado.

https://learn.microsoft.com/en-us/previous-versions/dn602597(v=msdn.10)?redirectedfrom=MSDN
https://www.hkcert.org/security-bulletin/microsoft-monthly-security-update-december-2023

	Ataque cibernético afectó al mayor operador de telecomunicaciones en Ucrania	**IMPORTANTE**

13DIC023 Kyivstar, el mayor operador de telecomunicaciones de Ucrania, sufrió un ciberataque que interrumpió el acceso de clientes a los servicios móviles y de Internet. La empresa presta servicios a aproximadamente 25 millones de suscriptores móviles y a más de 1 millón de clientes de Internet residencial. Además, señaló que el ataque fue «el resultado» de la guerra con Rusia y que notificó a las autoridades y a los servicios especiales estatales.

https://thehackernews.com/2023/12/major-cyber-attack-paralyzes-kyivstar.html

Ubuntu	**Múltiples vulnerabilidades afectan a la distribución de Ubuntu**	**CRÍTICO (Puntuación CVSS de 9.2)**

14DIC2023 Múltiples vulnerabilidades identificadas como CVE-2023-3773, CVE-2023-5090, CVE-2023-5158, CVE-2023-5178, CVE-2023-5345, CVE-2023-5717, CVE-2023-6039, CVE-2023-20593, CVE-2023-25775, 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-2023-45862, CVE-2023-45871, CVE-2023-46813, CVE-2023-46862 afectan al kernel (núcleo) de Ubuntu. Atacantes remotos podrían aprovechar algunas de estas vulnerabilidades para desencadenar la manipulación de datos, denegación de servicio, ejecución remota de código, elevación de privilegios y la divulgación de información confidencial. Sistemas afectados: Ubuntu 14.04 ESM, Ubuntu 16.04 ESM, Ubuntu 18.04 ESM, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, Ubuntu 23.04v

https://www.hkcert.org/security-bulletin/ubuntu-linux-kernel-multiple-vulnerabilities_20231201

FORTINET	**Múltiples vulnerabilidades afectan a productos FORTINET**	**CRÍTICO (Puntuación CVSS de 8.4)**

14DIC2023 Fortinet informó sobre múltiples vulnerabilidades identificadas como CVE-2023-36639, CVE-2023-41678 y CVE-2023-47536, que afectan a las tecnologías; FortiOS 6.0 (todas las versiones), FortiOS (versión 6.2.0 a 6.2.15), FortiOS 6.4 (todas las versiones), FortiOS 7.0 (todas las versiones), FortiOS (versión 7.2.0), FortiOS (versión 7.4.0), FortiProxy 2.0 (todas las versiones), FortiProxy 7.0 (todas las versiones), FortiProxy 7.2 (todas las versiones), FortiPAM (versión 1.1.0 a 1.1.1), FortiPAM 1.0 (todas las versiones). Un atacante remoto podría aprovechar algunas de estas vulnerabilidades para desencadenar la ejecución remota de código y eludir las restricciones de seguridad en el sistema objetivo.

https://www.hkcert.org/security-bulletin/fortinet-products-multiple-vulnerabilities_20231214

SQL	**«GambleForce» atacó empresas de la región Asia-Pacífico mediante ataques de inyección SQL**	**IMPORTANTE**

14DIC2023 Grupo de piratas informáticos «GambleForce» están vinculados a una serie de ataques de inyección SQL y explotación de sistemas de gestión de sitios web vulnerables hacia empresas de la región Asia-Pacífico. El grupo se dirigió a 24 organizaciones de los sectores de juegos de azar, gobierno, comercio minorista y viajes, en países como Australia, Brasil, China, India, Indonesia, Filipinas, Corea del Sur y Tailandia.

https://thehackernews.com/2023/12/new-hacker-group-gambleforce-tageting.html