BOLETÍN INFORMATIVO 01-07DIC2023

CONCIBER

Comité Nacional de Seguridad Cibernética

CONCIBER
Comité Nacional de Seguridad Cibernética

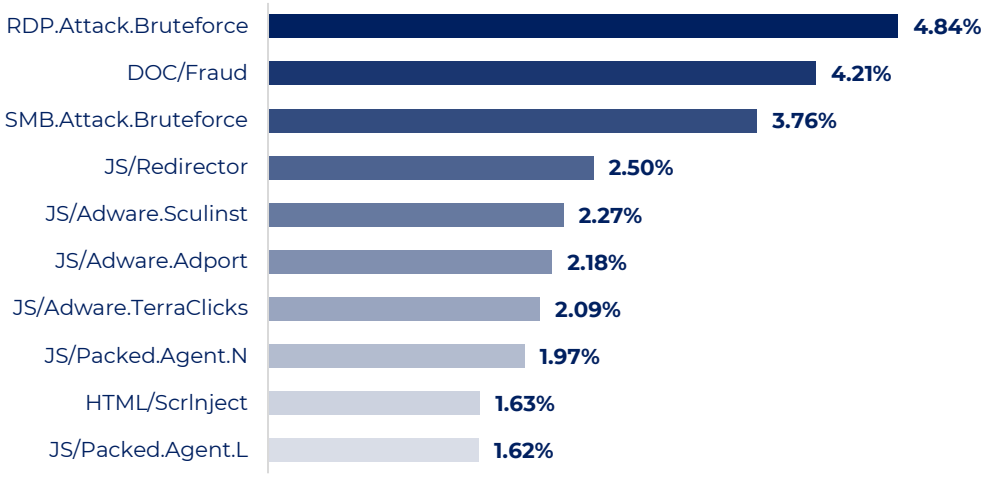
Boletín de Ciberseguridad

Amenazas cibernéticas en Guatemala

IMPORTANTE

01-07DIC2023 Según el reporte semanal de Virus Radar de ESET sobre las ciberamenazas más utilizadas por ciberdelincuentes en Guatemala, la amenaza RPD.Attack.Bruteforce (4.84 %) registró mayor incidencia; seguida de DOC/Fraud (4.21 %).

Principales amenazas cibernéticas en Guatemala



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

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

01-07DIC2023 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.Blocker.pef (25 %); seguido de Trojan-Ransom.MSIL.Blocker.gen (12.5 %).

Principales troyanos de tipo ransomware en Guatemala

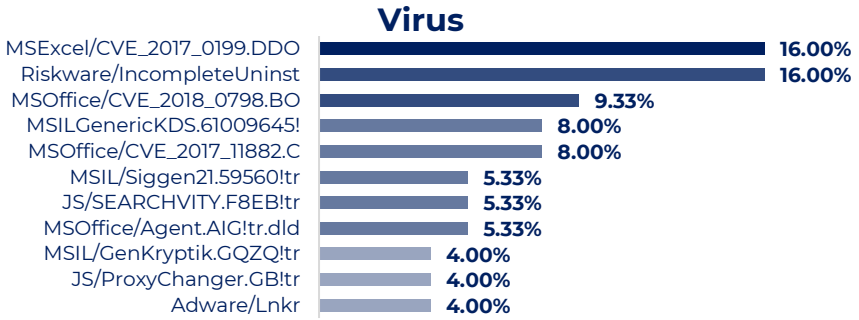
Ransomware	Frecuencia
Trojan-Ransom.Win32.Blocker.pef	25%
Trojan-Ransom.MSIL.Blocker.gen	12.5%
Trojan-Ransom.Win32.Blocker	12.5%
Trojan-Ransom.Win32.Stop.gen	12.5%
trojan-ransom.nsis.Onion.pef	12.5%
Trojan-Ransom.Win32.PornoBlocker.ejtx	12.5%
Trojan-Ransom.Win32.Locky.avt	12.5%

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

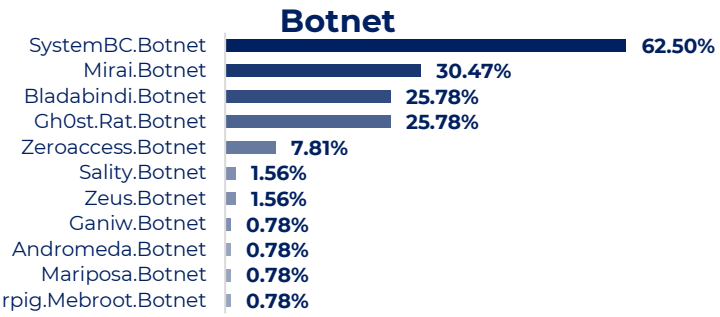
FORTINET	**Reporte de amenazas cibernéticas en Guatemala**	IMPORTANTE

01-07DIC2023 Principales amenazas cibernéticas en Guatemala, según reporte semanal de FORTIGUARD.

Principales amenazas



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



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

SPAMHAUS	**Países con más incidencia de botnets**	IMPORTANTE

01-07DIC2023 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	741,172
2	EE.UU.	327,650
3	India	281,530
4	Indonesia	180,957
5	Algeria	154,877
6	Tailandia	108,745
7	Brasil	99,091
8	Egipto	73,287
9	Pakistán	72,112
10	Vietnam	71,216

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

Microsoft	**Vulnerabilidades afectan a sistemas Android**	**CRÍTICO (Puntuación CVSS de 9.2)**

01DIC2023 Microsoft emitió una alerta sobre vulnerabilidades identificadas como CVE-2023-36035 y CVE-2022-24477 que afectan a Microsoft Exchange Server en las versiones 2016 y 2019, en sistemas basados en la arquitectura de 64 bits. La explotación exitosa de estas vulnerabilidades posibilitaría a un atacante a acceder, enviar, leer y descargar archivos de los buzones de correo de los usuarios de Exchange

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36035
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24477

Android	**Múltiples vulnerabilidades afectan a sistemas Android**	**CRÍTICO (Puntuación CVSS de 8)**

04DIC2023 Múltiples vulnerabilidades identificadas como CVE-2023-21267, CVE-2023-21394, CVE-2023-35668, CVE-2023-40073, CVE-2023-40074, CVE-2023-40075, CVE-2023-40076, CVE-2023-40077, CVE-2023-40078, CVE-2023-40079, CVE-2023-40080, CVE-2023-40081, CVE-2023-40082, CVE-2023-40083, VE-2023-40084, CVE-2023-40087, CVE-2023-40088, CVE-2023-40089, CVE-2023-40090, CVE-2023-40091, CVE-2023-40092, CVE-2023-40094, CVE-2023-40095, CVE-2023-40096, CVE-2023-40097, CVE-2023-40098, CVE-2023-40103, CVE-2023-45773, CVE-2023-45774, CVE-2023-45775, CVE-2023-45776, CVE-2023-45777, CVE-2023-45781, CVE-2023-45866 afectan a sistemas Android. Atacantes remotos podrían aprovechar algunas de estas vulnerabilidades para desencadenar una condición de denegación de servicio, elevación de privilegios, ejecución remota de código y divulgación de información confidencial. Los sistemas afectados están relacionados al parche de seguridad de Android del 04DIC2023.

https://www.hkcert.org/security-bulletin/android-multiple-vulnerabilities_20231205

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

05DIC2023 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

Outlook	**Microsoft advirtió que «APT28» explotó una vulnerabilidad crítica de Outlook**	**CRÍTICO (Puntuación CVSS de 9.8)**

05DIC2023 Microsoft detectó actividad del actor de amenazas «Forest Blizzard», apoyado por el estado ruso, que explotó una vulnerabilidad crítica de seguridad (CVE-2023-23397) en su servicio de correo electrónico Outlook. El grupo utilizó esta vulnerabilidad para obtener acceso no autorizado a las cuentas de las víctimas dentro de los servidores Exchange con el objetivo de obtener información confidencial de entidades públicas y privadas en Europa.

https://thehackernews.com/2023/12/microsoft-warns-of-kremlin-backed-apt28.html

	**Ciberataque a hospital israelí**	**IMPORTANTE**

06DIC023 Agencias oficiales del gobierno israelí anunciaron que un ciberincidente afectó a la red del hospital «Ziv en Safed». El grupo hacktivista «Malek Team» asumió la responsabilidad del ataque y afirmó haber extraído 500 GB de datos médicos de pacientes de los servidores del hospital, incluyendo alrededor de 700,000 archivos. Según fuentes, es la tercera vez que el Centro Médico es víctima de un ciberataque en solo cuatro meses.

https://www.escudodigital.com/ciberseguridad/hackers-iranies-datos-masivos-hospital-israeli_57411_102.html

Bluetooth SPECIAL INTEREST GROUP	**Falla de Bluetooth podría permitir a piratas informáticos apoderarse de diferentes sistemas operativos**	**CRÍTICO**

07DIC2023 Una vulnerabilidad crítica de seguridad de Bluetooth permite a los actores de amenazas tomar el control de dispositivos Android, Linux, macOS e iOS. CVE-2023-45866 tomando el control de dispositivos vulnerables sin necesidad de privilegios de ejecución adicionales. Además, permitiría realizar una amplia gama de ataques, incluyendo la instalación de malware, el robo de datos y el control remoto de dispositivos.

https://thehackernews.com/2023/12/new-bluetooth-flaw-let-hackers-take.html

CONCIBER
Comité Nacional de Seguridad Cibernética

Múltiples vulnerabilidades afectan a Google Chrome

CRÍTICO (Puntuación CVSS de 9.6)

07DIC2023 Google emitió una alerta para informar sobre múltiples vulnerabilidades identificadas como CVE-2023-6508, CVE-2023-6509, CVE-2023-6510, CVE-2023-6511, CVE-2023-6512. La explotación exitosa de una de estas fallas podría permitir a un atacante remoto la ejecución remota de código y la denegación de servicio en el sistema objetivo.

https://www.hkcert.org/security-bulletin/google-chrome-multiple-vulnerabilities_20231206