BOLETÍN INFORMATIVO 17-23NOV2023

CONCIBER

Comité Nacional de Seguridad Cibernética

CONCIBER
Comité Nacional de Seguridad Cibernética

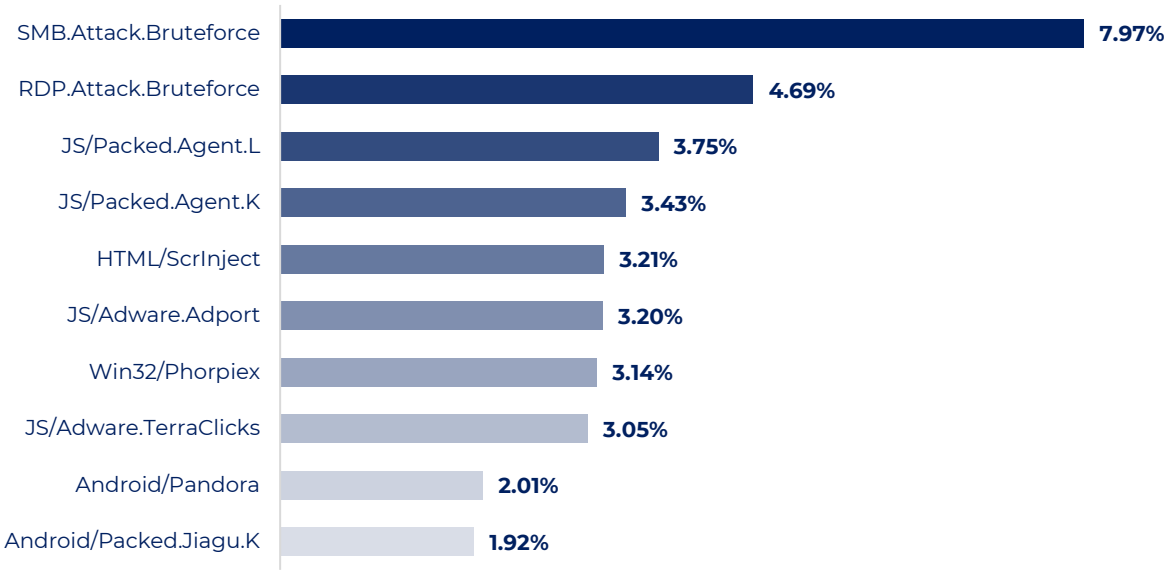
Boletín de Ciberseguridad

Amenazas cibernéticas en Guatemala

IMPORTANTE

17-23NOV2023 Según el reporte semanal de Virus Radar de ESET sobre las ciberamenazas más utilizadas por ciberdelincuentes en Guatemala, permanece la amenaza SMB.Attack.Bruteforce (7.97 %) con mayor incidencia; seguida de RDP.Attack.Bruteforce (4.69 %).

Principales amenazas cibernéticas en Guatemala



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

kaspersky	Amenazas de tipo ransomware en Guatemala	IMPORTANTE

17-23NOV2023 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.Convagent.gen» (18%); seguido de Trojan-ransom.win32.Polyransom.a (18%).

Principales troyanos de tipo ransomware en Guatemala

Ransomware	Frecuencia
Trojan-Ransom.Win32.Blocker	18%
Trojan-ransom.win32.Polyransom.a	18%
Trojan-Ransom.Win32.Blocker.a	18%
Trojan-Ransom.Win32.Convagent.gen	16%
Trojan-ransom.win32.Blocker.dap	10%
Trojan-Ransom.Win32.Autoit.b	8%
Trojan-Ransom.Win32.Stop.a	6%
Trojan-Ransom.Win32.Wanna	2%
Trojan-ransom.win32.Crypren.gen	2%
Trojan-Ransom.Win32.PornoBlocker.ejtx	2%

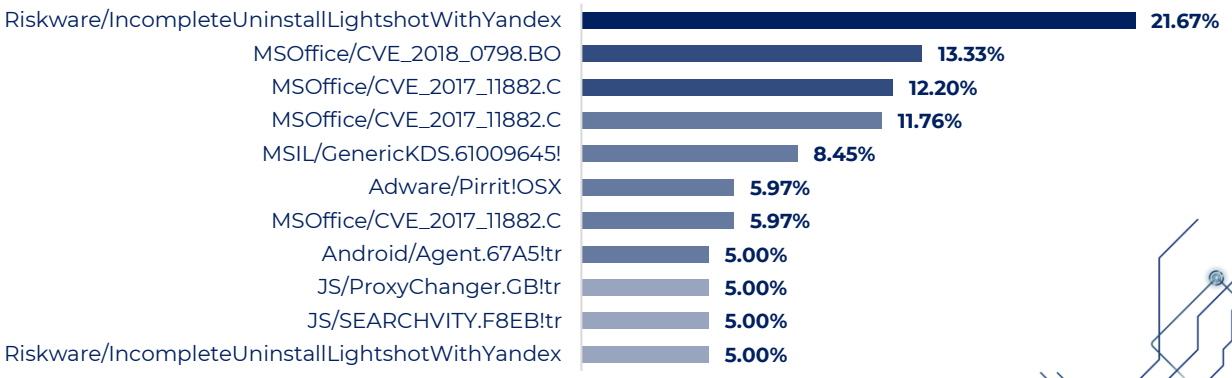
Fuente: CYBERMAP
https://cybermap.kaspersky.com/es/stats#country=38&type=RMW&period=w

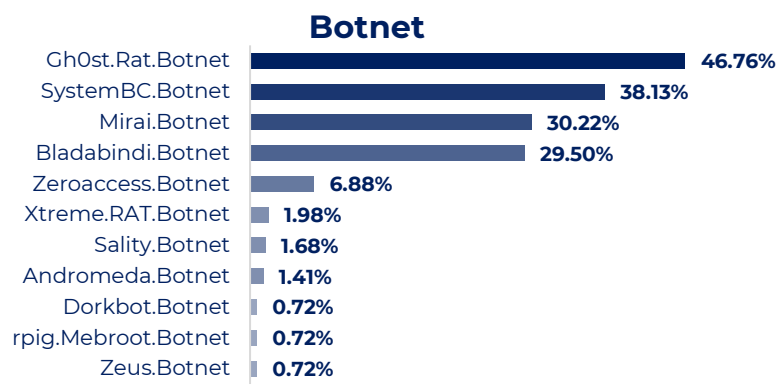
FORTINET	Reporte de amenazas cibernéticas en Guatemala	IMPORTANTE

17-23NOV2023 Principales amenazas cibernéticas en Guatemala, según reporte semanal de FORTIGUARD.

Principales amenazas (virus y botnet)

Virus





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

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

17-23NOV2023 Según reporte semanal de SPAMHAUS, los países más afectados con spam-bots a nivel mundial son: China, EE.UU., India, Indonesia y Argelia. 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	619,244
2	EE.UU.	409,961
3	India	249,115
4	Indonesia	172,072
5	Argelia	134,677
6	Brasil	118,744
7	Tailandia	107,254
8	Egipto	74,431
9	Rusia	73,818
10	Vietnam	68,745

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

Grupo ruso implementó gusanos en ataques a entidades de Ucrania

IMPORTANTE

18NOV2023 Grupo de ciberespionaje «Gamaredon», utilizó un nuevo gusano de propagación «LitterDrifter» para atacar diferentes entidades ucranianas. El gusano se propaga automáticamente a través de unidades USB conectadas y se comunica con los servidores de comando y control (C&C) del actor de la amenaza. Por otro lado, Check Point (firma de ciberseguridad que detectó el gusano) dijo que también detectó signos de posible infección fuera de Ucrania (EE.UU., Vietnam, Chile, Polonia, Alemania y Hong Kong).

https://thehackernews.com/2023/11/russian-cyber-espionage-group-deploys.html

Piratas informáticos chinos atacaron a gobierno de Filipinas

IMPORTANTE

21NOV2023 Grupo vinculado a China «Mustang Panda», lanzó un ciberataque dirigido al gobierno de Filipinas siendo el primer ataque que se conoce dirigido a una entidad gubernamental de un país del sudeste asiático. Lo anterior, evidenció la expansión del alcance de objetivos por parte del grupo chino. Se estima que la entidad se vio comprometida durante un período de cinco días (10-15AGO2023).

https://thehackernews.com/2023/11/mustang-panda-hackers-targets.html

Malware «Atomic Stealer» distribuido a usuarios de Mac a través de actualizaciones falsas del navegador

IMPORTANTE

21NOV2023 El malware «Atomic Stealer» (también conocido como AMOS), el cual se caracteriza por robar credenciales, archivos y otros datos confidenciales de las víctimas, se distribuyó a usuarios de Mac a través de una cadena de actualización de navegador falsa llamada ClearFake. Dicha cadena se transmite a través de sitios web comprometidos que simulan ser páginas de descarga de software legítimo.

https://www.malwarebytes.com/blog/threat-intelligence/2023/11/atomic-stealer-distributed-to-mac-users-via-fake-browser-updates

APACHE ACTIVEMQ	**Kinsing explotó falla de seguridad crítica en servidores Apache ActiveMQ**	**CRÍTICO (Puntuación CVSS de 10)**

21NOV2023 Grupo de amenazas Kinsing explotó activamente una falla de seguridad crítica en servidores Apache ActiveMQ vulnerables para infectar sistemas Linux con rootkits y mineros de criptomonedas. «CVE-2023-46604» permite la ejecución remota de código, permitiendo acceder al adversario para descargar e instalar el malware Kinsing. Una vez que los atacantes tienen control del servidor, pueden instalar un rootkit que brinda acceso completo al sistema.

https://thehackernews.com/2023/11/kinsing-hackers-exploit-apache-activemq.html
https://nvd.nist.gov/vuln/detail/CVE-2023-46604

Citrix NetScaler	**Lockbit aprovechó vulnerabilidad de Citrix para ingresar a su sistema**	**CRÍTICO (Puntuación CVSS de 9.4)**

22NOV2023 Afiliados del ransomware «Lockbit», explotaron una vulnerabilidad crítica «CVE-2023-4966» de control de entrega de aplicaciones (ADC) Citrix NetScaler y dispositivos Gateway. Esta vulnerabilidad permite a los atacantes eludir los requisitos de contraseña y la autenticación multifactor, permitiendo secuestrar sesiones de usuarios legítimos. Citrix lanzó un parche para la vulnerabilidad en AGO2023, sin embargo, los atacantes ya la estaban explotando antes de la publicación.

https://thehackernews.com/2023/11/lockbit-ransomware-exploiting-critical.html
https://nvd.nist.gov/vuln/detail/CVE-2023-4966

Red Hat	Múltiples vulnerabilidades en Kernel de Linux de RedHat	**CRÍTICO (Puntuación CVSS de 10)**

22NOV2023 Múltiples vulnerabilidades han sido identificadas en productos RedHat Linux Kernel. Atacante remoto podría aprovechar alguna de estas vulnerabilidades para desencadenar una condición de denegación de servicio, ejecución remota de código y divulgación de información confidencial.

https://www.hkcert.org/security-bulletin/redhat-linux-kernel-multiple-vulnerabilities_20231123

	Mozilla Firefox presentó múltiples vulnerabilidades	**CRÍTICO (Puntuación CVSS de 8.8)**

23NOV2023 Múltiples vulnerabilidades han sido identificadas en productos Mozilla Firefox. Atacantes remotos aprovecharon algunas de estas fallas para la manipulación de datos, divulgación de información confidencial, elevación de privilegios, denegación del servicio, la elusión de restricciones de seguridad y la ejecución remota de código en el sistema objetivo.

https://www.hkcert.org/security-bulletin/mozilla-products-multiple-vulnerabilities_20231122

	Mozilla Firefox presentó múltiples vulnerabilidades en Kernel de Linux de RedHat	**CRÍTICO (Puntuación CVSS de 9.1)**

23NOV2023 Múltiples vulnerabilidades han sido identificadas en la distribución GNU/Linux Ubuntu, basada en Debian GNU/Linux. El desarrollo de atacante remoto, podría aprovechar algunas de estas vulnerabilidades para desencadenar condiciones de denegación de servicio, ejecución remota de código, elevación de privilegios y divulgación de información confidencial en el sistema objetivo.

https://www.hkcert.org/security-bulletin/ubuntu-linux-kernel-multiple-vulnerabilities_20231102