BOLETÍN INFORMATIVO 19-25ENE2024

CONCIBER

Comité Nacional de Seguridad Cibernética

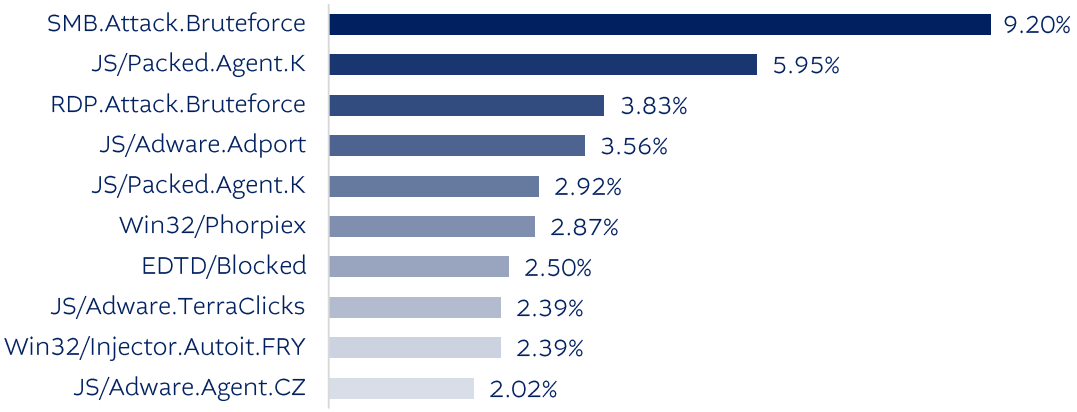
CONCIBER
Comité Nacional de Seguridad Cibernética

Boletín de Ciberseguridad

ESET	**Amenazas cibernéticas en Guatemala**	IMPORTANTE

19-25ENE2024 Según el reporte semanal de Virus Radar de ESET sobre las ciberamenazas más utilizadas por ciberdelincuentes en Guatemala, la amenaza SMB.Attack.Bruteforce (9.2 %) registró mayor incidencia; seguida de JS/Packed.Agent.L (5.95 %) y RPD.Attack.Bruteforce (3.83 %).

Principales amenazas cibernéticas en Guatemala



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

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

19-25ENE2024 El mapa en tiempo real de ciberamenazas de KASPERSKY mostró que en Guatemala únicamente se registraron cuatro softwares maliciosos durante la semana, el troyano trojan-ransom.win32.Polyransom.a (66.67 %); y el Trojan-Ransom.Win64.Covagent.gen (11.11 %).

Principales troyanos de tipo ransomware en Guatemala

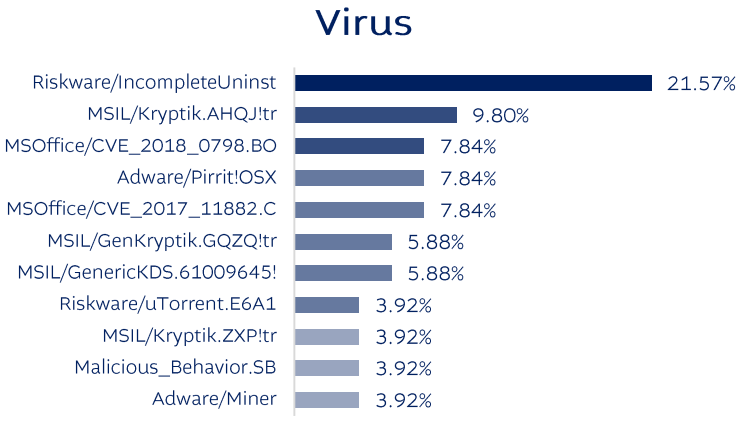
Ransomware	Frecuencia
trojan-ransom.win32.Polyransom.a	66.67%
Trojan-Ransom.Win64.Covagent.gen	11.11%
Trojan-Ransom.Win32.Crypmodng.gen	11.11%
Trojan-Ransom.Win32.PornoBlocker.ejtx	11.11%

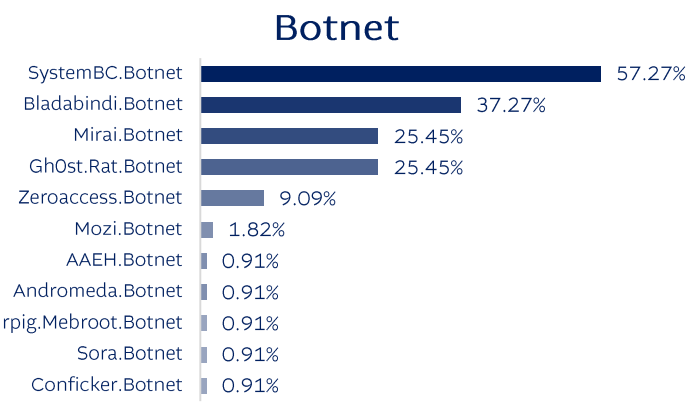
Fuente: CYBERMAP.
https://cybermap.kaspersky.com/es/stats#country=38&type=RMW&period=w

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

19-25ENE2024 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

19-25ENE2024 Según reporte semanal de SPAMHAUS, los países con más spam-bots a nivel mundial son: China, EE.UU., Brasil, India y Reino Unido. 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	561,914
2	EE.UU.	403,455
3	Brasil	133,637
4	India	131,668
5	Reino Unido	78,151
6	Indonesia	75,658
7	Egipto	61,459
8	Vietnam	60,415
9	Rusia	50,241
10	Argelia	47,902

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

Panorama de amenazas cibernéticas y vulnerabilidades
AMENAZAS

EQUILEND	**EquiLend sufrió ciberataque que afectó sus operaciones**	IMPORTANTE

22ENE2024 La firma global de tecnología financiera, EquiLend, sufrió un ciberataque que provocó que algunos sistemas de la empresa quedaran fuera de línea y que se produjera un acceso no autorizado a su red. La empresa confirmó el incidente y dijo que está trabajando con expertos externos para investigar la violación de seguridad y ayudar a restaurar los servicios afectados. Sin embargo, no reveló si algún dato de la empresa o del cliente quedó expuesto o fue robado durante el incidente.

https://www.bleepingcomputer.com/news/security/global-fintech-firm-equilend-offline-after-recent-cyberattack/

	lendDepot confirmó robo de información en un ataque de ransomware	IMPORTANTE

22ENE2024 Prestamista hipotecario «lendDepot» confirmó que la información personal de aproximadamente 16.6 millones de personas fue robada en un ataque de ransomware que la empresa sufrió el 06ENE2024. La información personal a la que se cree que se accedió y robó incluye nombres, direcciones, números de teléfono, números de Seguro Social, números de cuentas bancarias y otra información financiera. Además, está ofreciendo servicios gratuitos de monitoreo de crédito y protección de identidad a las personas afectadas.

https://www.bleepingcomputer.com/news/security/loandepot-cyberattack-causes-data-breach-for-166-million-people/

VEOLIA	**Veolia North America sufrió ataque de ransomware**	IMPORTANTE

23ENE2024 Veolia North America, empresa de servicios de distribución de agua, reveló un ataque de ransomware que afectó los sistemas que forman parte de su división de agua municipal e interrumpió sus sistemas de pago de facturas. El ataque no interrumpió las operaciones de tratamiento de agua ni servicios de aguas residuales de Veolia. Sin embargo, provocó retrasos en los pagos de clientes y la posible exposición de información personal de un número limitado de personas.

https://www.bleepingcomputer.com/news/security/water-services-giant-veolia-north-america-hit-by-ransomware-attack/

Hewlett Packard Enterprise	**HPE confirmó que fue víctima de ataque cibernético por piratas informáticos rusos**	**IMPORTANTE**

24ENE2024 Hewlett Packard Enterprise –HPE- reveló que fue víctima de un ataque cibernético por parte del grupo patrocinado por el estado ruso «APT29». El ataque permitió a los piratas informáticos acceder y extraer datos de los buzones de correo de un pequeño porcentaje de empleados de HPE. El ataque podría haber permitido a los ciberdelincuentes obtener información confidencial sobre sus clientes, empleados y operaciones. Además de ser utilizado para lanzar ataques contra otras organizaciones.

https://thehackernews.com/2024/01/tech-giant-hp-enterprise-hacked-by.html
https://www.bleepingcomputer.com/news/security/hpe-russian-hackers-breached-its-security-teams-email-accounts/

VULNERABILIDADES

chromeOS	**Múltiples vulnerabilidades de ChromeOS**	**ALTO (Puntuación CVSS: 8.8)**

19ENE2024 ChromeOS identificó multiples vulnerabilidades; CVE-2023-4969, CVE-2023-6508, CVE-2023-6703, CVE-2023-6706 y CVE-2024-0519, las cuáles podrían afectar la versión anterior a 114.0.5735.347 (Versión de plataforma: 15437.87.0). 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/chromeos-multiple-vulnerabilities_20240119
https://chromereleases.googleblog.com/

vmware vCenter Server Standard	**Múltiples vulnerabilidades de VMware vCenter Server**	**CRÍTICO (Puntuación CVSS: 9.8)**

22ENE2024 VMware vCenter server identificó dos vulnerabilidades en sus sistemas; CVE-2023-34048 y CVE-2023-34056, las cuales podrían afectar sus sistemas VMware vCenter Server 7.0 y 8.0 y VMware Cloud Foundation 4.x y 5.x. Un atacante remoto podría aprovechar algunas de estas vulnerabilidades para desencadenar la divulgación de información confidencial y la ejecución remota de código en el sistema objetivo.

https://www.hkcert.org/security-bulletin/vmware-vcenter-server-multiple-vulnerabilities_20231026
https://www.vmware.com/

	Múltiples vulnerabilidades de los productos Apple	**ALTO (Puntuación CVSS: 7.5)**

23ENE2024 Apple identificó múltiples vulnerabilidades en sus productos; CVE-2023-38039, CVE-2023-38545, CVE-2023-38546, CVE-2023-40528, CVE-2023-42887, CVE-2023-42888, CVE-2023-42915, CVE-2023-42935, CVE-2023-42937, CVE-2024-23203, CVE-2024-23204, CVE-2024-23206, CVE-2024-23207, CVE-2024-23208, CVE-2024-23209, CVE-2024-23210, CVE-2024-23211, CVE-2024-23212, CVE-2024-23213, CVE-2024-23214, CVE-2024-23215, CVE-2024-23217, CVE-2024-23218, CVE-2024-23219, CVE-2024-23222, CVE-2024-23223 y CVE-2024-23224. Un atacante remoto podría aprovechar algunas de estas vulnerabilidades para activar la elevación de privilegios, la ejecución remota de código, la divulgación de información confidencial y la elusión de restricciones de seguridad en el sistema objetivo. Para CVE-2024-23222, el procesamiento de contenido web puede dar lugar a la ejecución de código arbitrario.

https://www.hkcert.org/security-bulletin/apple-products-multiple-vulnerabilities_20240123
https://support.apple.com/es-es/HT201222

	Múltiples vulnerabilidades de Google Chrome	**MEDIO (Puntuación CVSS: 6.0)**

25ENE2024 Google Chrome identificó múltiples vulnerabilidades las cuales se identifican como CVE-2024-0804, CVE-2024-0805, CVE-2024-0806, CVE-2024-0807, CVE-2024-0808, CVE-2024-0809, CVE-2024-0810, CVE-2024-0811, CVE-2024-0812, CVE-2024-0813 y CVE-2024-0814 que afectan a los sistemas Google Chrome anterior a 121.0.6167.85 (Linux), anterior a 121.0.6167.85 (Mac), anterior a 121.0.6167.85/.86 (Windows). Un atacante remoto podría aprovechar algunas de estas vulnerabilidades para activar la elusión de restricciones de seguridad, suplantación de identidad, divulgación de información, ejecución remota de código y condición de denegación de servicio en el sistema objetivo.

https://www.hkcert.org/security-bulletin/google-chrome-multiple-vulnerabilities_20240125
https://chromereleases.googleblog.com/