BOLETÍN INFORMATIVO 26ENE-01FEB2024

CONCIBER

Comité Nacional de Seguridad Cibernética

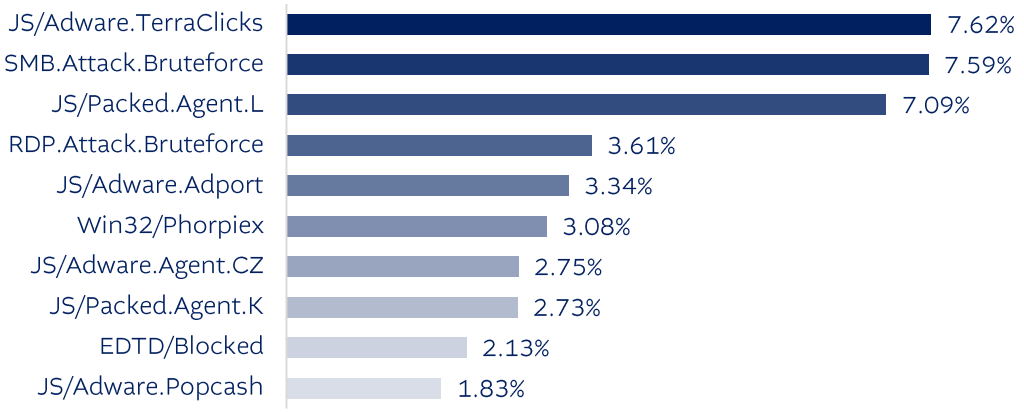
CONCIBER
Comité Nacional de Seguridad Cibernética

Boletín de Ciberseguridad

ESET	**Amenazas cibernéticas en Guatemala**	IMPORTANTE

26ENE-01FEB2024 Según el reporte semanal de Virus Radar de ESET sobre las ciberamenazas más utilizadas en Guatemala, la amenaza JS/Adware.TerraClicks (7.62 %) registró mayor incidencia; seguida de SMB.Attack.Bruteforce (7.59 %) y JS/Packed.Agent.L (7.09 %).

Principales amenazas cibernéticas en Guatemala



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

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

26ENE-01FEB2024 El mapa en tiempo real de ciberamenazas de KASPERSKY mostró que en Guatemala únicamente se registraron tres softwares maliciosos durante la semana, el troyano trojan-ransom.win32.Polyransom.a (75.0 %); el Trojan-Ransom.Win32.PornoBlocker.ejtx (12.5 %) y Trojan-Ransom.Win64.Convagent.gen (12.5 %).

Principales troyanos de tipo ransomware en Guatemala

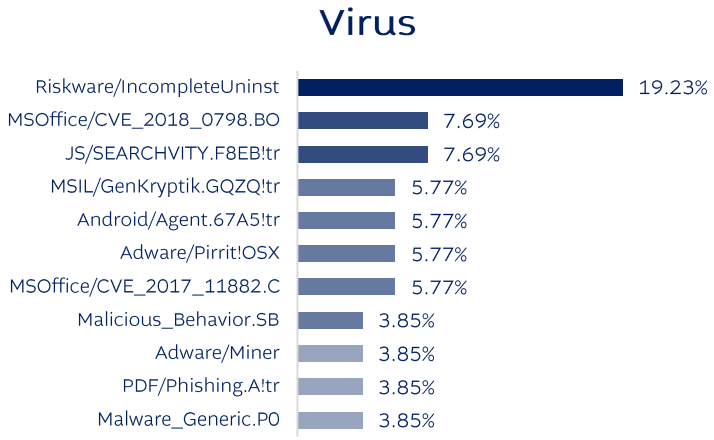
Ransomware	Frecuencia
trojan-ransom.win32.Polyransom.a	75.0%
Trojan-Ransom.Win32.PornoBlocker.ejtx	12.5%
Trojan-Ransom.Win64.Convagent.gen	12.5%

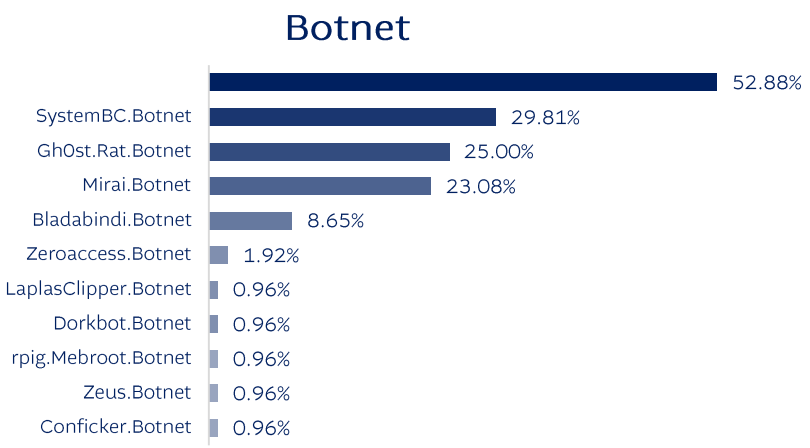
Fuente: CYBERMAP.
https://cybermap.kaspersky.com/es/stats#country=38&type=RMW&period=w

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

26ENE-01FEB2024 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

26ENE-01FEB2024 Según reporte semanal de SPAMHAUS, los países con más spam-bots a nivel mundial son: China, EE.UU., Egipto, Brasil e India. 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	528,875
2	EE.UU.	269,489
3	Egipto	67,462
4	Brasil	63,626
5	India	62,457
6	Reino Unido	58,725
7	Rusia	54,613
8	Vietnam	42,441
9	Turquía	36,324
10	Australia	24,793

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

Panorama de amenazas cibernéticas y vulnerabilidades
AMENAZAS

Microsoft	**Microsoft advirtió a organizaciones sobre ataques del grupo ATP29**	**IMPORTANTE**

26ENE2024 Microsoft notificó a varias organizaciones que fueron blanco de ataques por parte del grupo de piratas informáticos «APT29», patrocinado por el Estado ruso. El actor de amenazas es el mismo que atacó a Microsoft a finales de NOV2023. El objetivo principal de APT29 es recopilar información sensible de interés estratégico para Rusia, utilizando métodos para obtener acceso a las redes de organizaciones, incluyendo el uso de credenciales robadas, ataques a la cadena de suministro y la explotación de vulnerabilidades.

https://thehackernews.com/2024/01/microsoft-warns-of-widening-apt29.html

Schneider Electric	**Schneider Electric sufrió ataque de ransomware que afectó sus operaciones**	**IMPORTANTE**

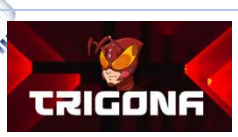
29ENE2024 Empresa de automatización y gestión de energía, Schneider Electric, sufrió ataque de ransomware «Cactus» que afectó a su división de negocios de sostenibilidad. Los ciberdelincuentes accedieron a gran cantidad de datos corporativos y amenazan con filtrarlos si no se paga un rescate. Los datos robados podrían ser confidenciales e incluir información sobre el uso de energía de los clientes, sistemas de automatización y control industrial, y cumplimiento de regulaciones ambientales y energéticas.

https://www.bleepingcomputer.com/news/security/energy-giant-schneider-electric-hit-by-cactus-ransomware-attack/

Johnson Controls	**Johnson Controls confirmó que ataque de ransomware le costó USD 27 millones**	**IMPORTANTE**

31ENE2024 Empresa multinacional de sistemas de control industrial y seguridad, Johnson Controls, confirmó que un ataque de ransomware en SEP2023 le costó aproximadamente USD 27 millones, además de provocar una filtración de datos. El ataque, llevado a cabo por «Dark Angels», afectó a las oficinas de Asia y se extendió por la red, obligando a la empresa a cerrar gran parte de su infraestructura de TI. Los piratas informáticos robaron más de 27 TB de datos confidenciales.

https://www.bleepingcomputer.com/news/security/johnson-controls-says-ransomware-attack-cost-27-million-data-stolen/

	**Ransomware «Trigona» desencadena alarmas de ciberseguridad en Centroamérica**	**IMPORTANTE**

31ENE2024 Ransomware «Trigona» desencadenó una serie de ataques en la región, dejando a empresas de todos los tamaños en estado de emergencia. Este virus cifra archivos esenciales, cambiando sus nombres y añadiendo la extensión "._locked". El malware se propaga rápidamente a través de correos electrónicos infectados.

https://devel.group/blog/ransomware-trigona-desencadena-alarmas-de-ciberseguridad-en-la-region/

VULNERABILIDADES

	**Múltiples vulnerabilidades de productos Cisco**	**MEDIO (Puntuación CVSS: 6.8)**

26ENE2024 Múltiples vulnerabilidades en productos de Cisco identificados como CVE-2024-20305, CVE-2024-20253 y CVE-2024-20263, podrían afectar a Interruptores inteligentes serie 250, Switches administrados serie 350, Switches administrados apilables serie 350X y 550X, conmutadores inteligentes empresariales serie 250, Switches administrados Business serie 350 y la conexión de unidad de Cisco. Un atacante remoto podría aprovechar estas vulnerabilidades para activar la ejecución remota de código, eludir las restricciones de seguridad y ejecutar secuencias de comandos entre sitios en el sistema objetivo.

https://www.hkcert.org/security-bulletin/cisco-products-multiple-vulnerabilities_20240126
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuc-xss-9TFuu5MS

	**Múltiples vulnerabilidades de Microsoft Edge**	**CRÍTICO (Puntuación CVSS: 9.6)**

29ENE2024 Microsoft Edge identificó múltiples vulnerabilidades en sus sistemas; CVE-2024-21326, CVE-2024-21336, CVE-2024-21382, CVE-2024-21383, CVE-2024-21385, CVE-2024-21387 y CVE-2024-21388 que afectan a los sistemas Microsoft Edge (estable) anterior a 121.0.2277.83 y Microsoft Edge (estable extendido) anterior a 120.0.2210.160. Un atacante remoto podría aprovechar algunas de estas vulnerabilidades para activar la elevación de privilegios, la divulgación de información confidencial y la suplantación de identidad en el sistema objetivo.

https://www.hkcert.org/security-bulletin/microsoft-edge-multiple-vulnerabilities_20240129
https://msrc.microsoft.com/update-guide/vulnerability/

Jenkins	**Múltiples vulnerabilidades de Jenkins**	**ALTO (Puntuación CVSS: 7.5)**

30ENE2024 Jenkins identificó múltiples vulnerabilidades; CVE-2023-6147, CVE-2023-6148, CVE-2024-23897 (afecta a las versiones semanales de Jenkins hasta la 2.441 inclusive, y a las versiones LTS de Jenkins hasta la 2.426.2 inclusive), CVE-2024-23898, CVE-2024-23899, CVE-2024-23900, CVE-2024-23901, CVE-2024-23902, CVE-2024-23903, CVE-2024-23904 y CVE-2024-23905. Un atacante remoto podría aprovechar estas vulnerabilidades para desencadenar la ejecución remota de código, la divulgación de información confidencial, secuencias de comandos entre sitios y eludir las restricciones de seguridad en el sistema objetivo.

https://www.hkcert.org/security-bulletin/jenkins-multiple-vulnerabilities_20240130
https://www.jenkins.io/security/advisory/2024-01-24/

	Múltiples vulnerabilidades de ejecución remota de Google Chrome	**MEDIO (Puntuación CVSS: 6.5)**

31ENE2024 Google Chrome identificó tres vulnerabilidades las cuales se identifican como CVE-2024-1059, CVE-2024-1060 y CVE-2024-1077 que afectan a los sistemas Google Chrome anterior a 121.0.6167.139 (Linux), anterior a 121.0.6167.139 (Mac) y anterior a 121.0.6167.139/140 (Windows). Un atacante remoto podría aprovechar algunas de estas vulnerabilidades para desencadenar la ejecución remota de código en el sistema objetivo.

https://www.hkcert.org/security-bulletin/google-chrome-multiple-vulnerabilities_20240131
https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_30.html

GitLab	**GitLab identificó múltiples vulnerabilidades**	**ALTO (Puntuación CVSS: 8.1)**

31ENE2024 GitLab identificó múltiples vulnerabilidades las cuales se identifican como CVE-2023-5612, CVE-2023-5933, CVE-2023-6159, CVE-2023-41056, CVE-2023-45322, CVE-2024-0402, CVE-2024-0456 que afectan a las versiones de GitLab Community Edition (CE) anteriores a 16.8.1, 16.7.4, 16.6.6 y 16.5.8 y Versiones de GitLab Enterprise Edition (EE) anteriores a 16.8.1, 16.7.4, 16.6.6 y 16.5.8. Un atacante remoto podría aprovechar algunas de estas vulnerabilidades para provocar denegación de servicio, elevación de privilegios, ejecución remota de código, divulgación de información confidencial y manipulación de datos en el sistema objetivo.

https://www.hkcert.org/security-bulletin/gitlab-multiple-vulnerabilities_20240131
https://about.gitlab.com/releases/2024/01/25/critical-security-release-gitlab-16-8-1-released/