BOLETÍN INFORMATIVO 12-18ENE2024

CONCIBER

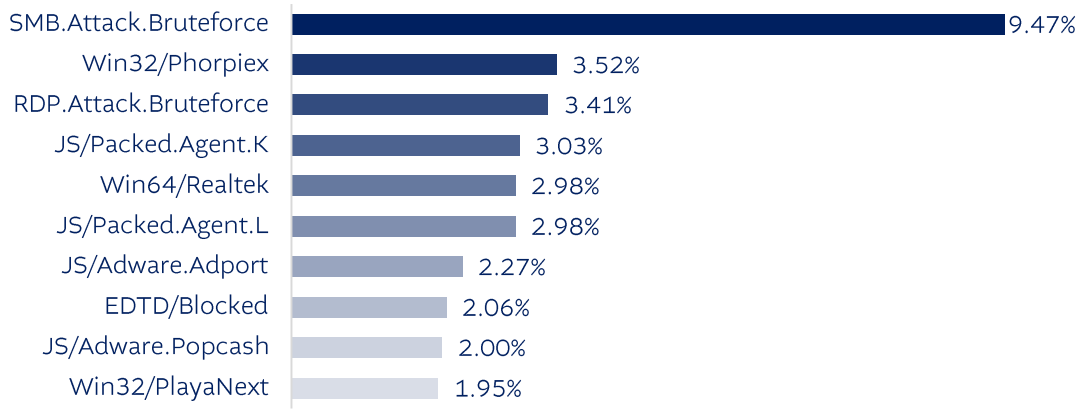
Comité Nacional de Seguridad Cibernética

Boletín de Ciberseguridad

ESET	**Amenazas cibernéticas en Guatemala**	IMPORTANTE

12-18ENE2024 Según el reporte semanal de Virus Radar de ESET sobre las ciberamenazas más utilizadas por ciberdelincuentes en Guatemala, la amenaza SMB.Attack.Bruteforce (9.47 %) registró mayor incidencia; seguida de Win32/Phorpiex (3.52 %) y RPD.Attack.Bruteforce (3.41 %).

Principales amenazas cibernéticas en Guatemala



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

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

12-18ENE2024 El mapa en tiempo real de ciberamenazas de KASPERSKY mostró que en Guatemala únicamente se registraron dos softwares maliciosos durante la semana, el troyano Trojan-Ransom.Win32.AutoIt.abdx (66.67 %); y el Trojan-Ransom.JS.Agent.cq (33.33 %).

Principales troyanos de tipo ransomware en Guatemala

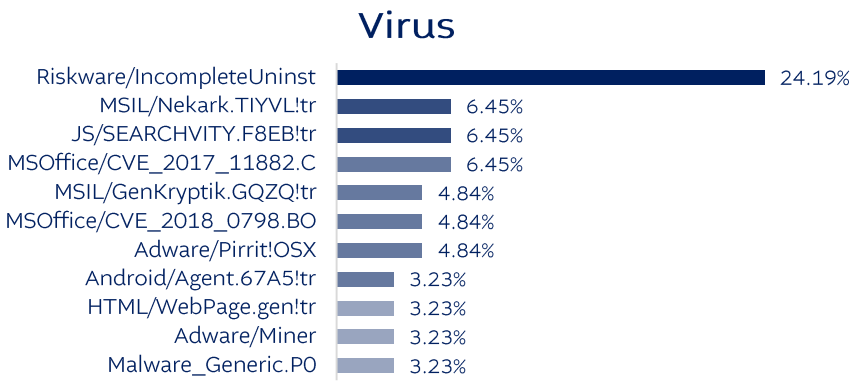
Ransomware	Frecuencia
Trojan-Ransom.Win32.AutoIt.abdx	66.67%
Trojan-Ransom.JS.Agent.cq	33.33%

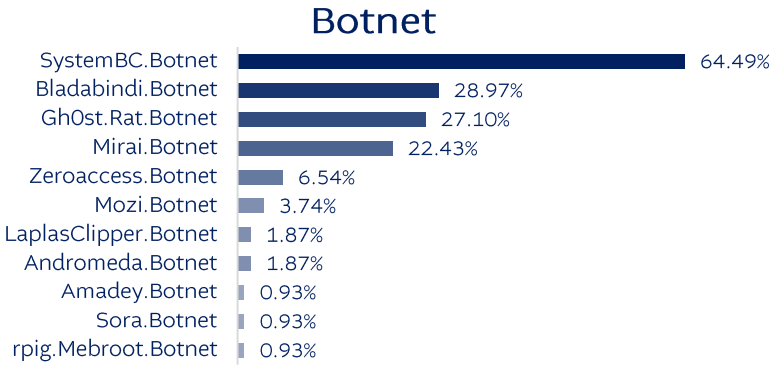
Fuente: CYBERMAP.
https://cybermap.kaspersky.com/es/stats#country=38&type=RMW&period=w

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

12-18ENE2024 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

12-18ENE2024 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	647,813
2	EE.UU.	433,799
3	India	240,443
4	Indonesia	140,719
5	Algeria	114,221
6	Brasil	91,403
7	Tailandia	89,029
8	Reino Unido	80,778
9	Vietnam	73,747
10	Egipto	61,619

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

Panorama de amenazas cibernéticas y vulnerabilidades

AMENAZAS

water for people EVERYONE • FOREVER	**Grupo de ransomware atacó a organización sin fines de lucro que proporciona agua potable**	IMPORTANTE

12ENE2024 Water for People, organización sin fines de lucro que mejora el acceso al agua potable en todo el mundo, fue víctima de un ataque de ransomware. El ataque fue llevado a cabo por la banda de ransomware «Medusa», que amenazó con publicar información robada exigiendo a la organización pagar un rescate de USD 300,000. Water for People indicó que los datos a los que se accedió eran anteriores a 2021 y no comprometieron sus sistemas financieros ni operaciones comerciales.

https://therecord.media/water-for-people-medusa-ransomware

SONICWALL	**Exposición de más de 178,000 firewalls de SonicWall a ataques DoS y RCE**	IMPORTANTE

15ENE2024 Investigadores de seguridad descubrieron que más de 178,000 firewalls de próxima generación (NGFW) de SonicWall con la interfaz de administración expuesta en línea son vulnerables a ataques de denegación de servicio (DoS) y posibles ataques de ejecución remota de código (RCE). Si los atacantes pueden explotar estas vulnerabilidades, podrían causar una serie de problemas, que incluyen una detención del servicio de firewalls y la ejecución de un código arbitrario en los dispositivos afectados para poder instalar malware o el robo de datos.

https://www.bleepingcomputer.com/news/security/over-178k-sonicwall-firewalls-vulnerable-to-dos-potential-rce-attacks/

AJUNTAMENT DE CALVIÀ MALLORCA	**Ciberataque registrado al ayuntamiento de Calviá, Mallorca**	IMPORTANTE

16ENE2024 El Ayuntamiento de Calviá, Mallorca, fue objeto de un ciberataque de ransomware que afectó a sus sistemas informáticos, lo que provocó la suspensión de los plazos administrativos y la interrupción de algunos servicios públicos. Los autores del ataque aún no han sido identificados, pero se estima que el rescate exigido es de 10 millones de euros.

https://www.bleepingcomputer.com/news/security/majorca-city-calvi-extorted-for-11m-in-ransomware-attack/

	**Piratas informáticos rusos del FSB implementan nuevo malware de puerta trasera Spica**	**IMPORTANTE**

18ENE2024 Grupo de piratería ColdRiver, proveniente de Rusia, utilizó un malware de puerta trasera previamente desconocido «Spica» para atacar a objetivos gubernamentales y de defensa. Los atacantes envían correos electrónicos de phishing que se hacen pasar por personas afiliadas a sus objetivos. Sin embargo, Microsoft frustró previamente los ataques de ColdRiver dirigidos a varias naciones europeas de la OTAN al deshabilitar las cuentas de Microsoft que los atacantes usaban para vigilancia y recolección de correos electrónicos.

https://www.bleepingcomputer.com/news/security/google-russian-fsb-hackers-deploy-new-spica-backdoor-malware/

VULNERABILIDADES

	**Múltiples vulnerabilidades de Microsoft Edge**	**MEDIO (Puntuación CVSS: 6.3)**

15ENE2024 Microsoft Edge identificó multiples vulnerabilidades; CVE-2024-0333, CVE-2024-20675, CVE-2024-20709, CVE-2024-20721, CVE-2024-21337 que podrían afectar a los sistemas de Microsoft Edge (estable) anteriores a 120.0.2210.133. Un atacante remoto podría aprovechar algunas de estas vulnerabilidades para desencadenar una condición de denegación de servicio, elevación de privilegios, ejecución remota de código y elusión de restricciones de seguridad en el sistema objetivo.

https://www.hkcert.org/security-bulletin/microsoft-edge-multiple-vulnerabilities_20240115
https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#january-11-2024

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

17ENE2024 Múltiples vulnerabilidades en productos Oracle identificadas como; CVE-2022-21432, CVE-2022-41409, CVE-2022-46337, CVE-2023-2976, CVE-2023-38545, CVE-2023-40167, CVE-2023-4043, CVE-2023-46589, CVE-2023-47248 y CVE-2024-20903. Dichas fallas afectan a los sistemas oráculo MySQL, JavaSE, servidor de base de datos Oracle y el servidor WebLogic. Un atacante remoto podría utilizarlas para desencadenar una condición de denegación de servicio, elevación de privilegios, ejecución remota de código, divulgación de información confidencial, manipulación de datos y elusión de restricciones de seguridad en el sistema objetivo.

https://www.hkcert.org/security-bulletin/oracle-products-multiple-vulnerabilities_20240117
https://www.oracle.com/security-alerts/cpujan2024verbose.html

 	**Múltiples vulnerabilidades de Google Chrome y Microsoft Edge**	**CRÍTICO (Puntuación CVSS: 9.0)**

17ENE2024 Google Chrome identificó múltiples vulnerabilidades; CVE-2024-0517, CVE-2024-0518, CVE-2024-0519 las cuales podrían afectar a los sistemas de Google Chrome anteriores a 120.0.6099.224 (Linux), Google Chrome anterior a 120.0.6099.234 (Mac), Google Chrome anterior a 120.0.6099.224/225 (Windows). Un atacante remoto podría aprovechar algunas de estas fallas 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/google-chrome-multiple-vulnerabilities_20240117
https://chromereleases.googleblog.com/
https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#january-17-2024

CITRIX®	**Múltiples vulnerabilidades en productos de Citrix**	**MEDIO (Puntuación CVSS: 5.5)**

18ENE2024 Citrix identificó múltiples vulnerabilidades en sus productos las cuales se identifican como CVE-2023-6548, CVE-2023-6549, CVE-2023-6184 en donde un atacante remoto podría aprovechar algunas de estas vulnerabilidades para desencadenar una condición de denegación de servicio y la ejecución remota de código en el sistema objetivo. Estas vulnerabilidades afectan a las tecnologías NetScaler ADC y NetScaler Gateway 14.1 anteriores a 14.1-12.35, NetScaler ADC y NetScaler Gateway 13.1 anteriores a 13.1-51.15, Citrix Virtual Apps and Desktops antes del 2311, Citrix Virtual Apps and Desktops 1912 LTSR antes de la revisión CU8 19.12.8100.4 y Citrix Virtual Apps and Desktops 2203 LTSR antes de CU4.

https://www.hkcert.org/security-bulletin/citrix-products-multiple-vulnerabilities_20240117
https://support.citrix.com/article/CTX584986/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20236548-and-cve20236549