BOLETÍN INFORMATIVO 23-29FEB2024

CONCIBER

Comité Nacional de Seguridad Cibernética

Boletín de Ciberseguridad

CONCIBER
Comité Nacional de Seguridad Cibernética

FORTINET

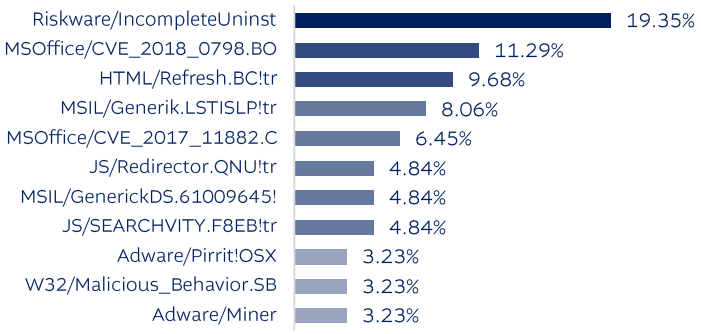
Reporte de amenazas cibernéticas en Guatemala

IMPORTANTE

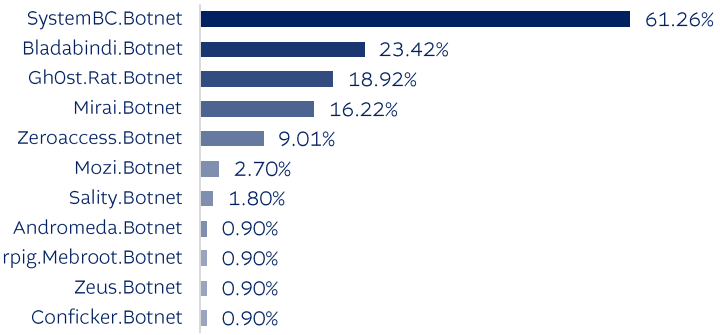
23-29FEB2024 Principales amenazas cibernéticas en Guatemala, según reporte semanal de FORTIGUARD.

Principales amenazas

Virus



Botnet



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

kaspersky	**Amenazas de tipo ransomware**	IMPORTANTE

23-29FEB2024 El mapa en tiempo real de ciberamenazas de KASPERSKY, registró el flujo de detección de malware mediante «On-Acces Scan», un escaneo activo y continuo para proteger el sistema contra posibles amenazas en tiempo real mientras se llevan a cabo diferentes operaciones, específicamente cuando los archivos o programas son abiertos, copiados, ejecutados o guardados en el sistema.

Principales troyanos escaneados en tiempo real a nivel mundial

Troyanos	Frecuencia
DangerousObject.Multi.Generic	9.45%
Trojan.WinLNK.Agent.gen	2.97%
Trojan.Win32.Shelm	2.33%
Trojan.Win32.Agentb.bqyr	2.26%
Worm.Python.Agent.gen	2.1%
Trojan.Win32.Agent.gen	1.87%
Trojan.Win32.Hosts2.gen	1.86%

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

CLOUDFLARE	**Porcentaje de tráfico de bots a nivel mundial**	IMPORTANTE

23-29FEB2024 Según el reporte semanal del radar de CloudFlare, el mayor porcentaje de tráfico de bots se registró en Irán (95.48 %) seguido de Turkmenistán (69.65 %), Isla de Man (67.33 %) y Singapur (66.17 %).

Principales países con mayor porcentaje de tráfico de bots

Posición	País	Tráfico de bots
1	Irán	95.48%
2	Turkmenistán	69.65%
3	Isla de Man	67.33%
4	Singapur	66.17%
5	Irlanda	63.49%

Fuente: CloudFlare.
https://radar.cloudflare.com/traffic

CONCIBER
Comité Nacional de Seguridad Cibernética

SPAMHAUS

ISPs con mayor número de spam-bots detectados

IMPORTANTE

23-29FEB2024 El reporte semanal de SPAMHAUS, los proveedores de servicios de internet -ISP- que poseen el mayor número de spam-bots son; charter.com, chinanet-js, Microsoft.com y chinanet-zj. La mayoría de los bots se pueden utilizar para spam, phishing, fraude de clics, DDoS y otras actividades maliciosas.

ISP más vulnerables a spam-bots a nivel mundial

Posición	País	Número de Bots
1	charter.com	199,098
2	Microsoft.com	156,351
3	Airtel.in	130,679
4	Chinanet-js	106,883
5	Djaweb.dz	75,754
6	Verizon.com	70,237
7	Unicom-ln	69,306
8	Chinanet-zj	63,183
9	Chinanet-ah	57,668
10	Virginmedia.com	57,302

Fuente: SPAMHAUS.
https://www.spamhaus.com/threat-map/

Panorama de amenazas cibernéticas y vulnerabilidades

AMENAZAS

OPTUM	**Filial de UnitedHealth Group, Optum, sufrió ciberataque de «estados-nación»**	IMPORTANTE

23FEB2024 UnitedHealth Group confirmó que su filial, Optum, sufrió un ciberataque por parte de presuntos piratas informáticos de «estados-nación» a la plataforma Change Healthcare, lo que llevó al cierre de sistemas de TI y servicios relacionados. La interrupción afecta a 119 servicios y plataformas de Change Healthcare y Optum, utilizadas ampliamente en el sistema de salud de EE. UU. Aunque no está confirmado, el incidente tiene signos de un posible ataque de ransomware. La investigación sobre el alcance del ciberataque está en curso.

https://www.bleepingcomputer.com/news/security/unitedhealth-confirms-optum-hack-behind-us-healthcare-billing-outage/

thyssenkrupp	**ThyssenKrupp sufrió ciberataque en su división automotriz**	IMPORTANTE

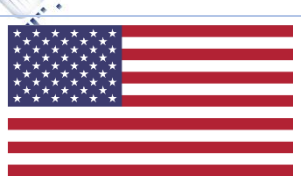
26FEB2024 Compañía siderúrgica, ThyssenKrupp, confirmó que sus sistemas de división automotriz fueron comprometidos por piratas informáticos, lo que llevó al cierre temporal de los sistemas de TI como medida de respuesta y contención. El ciberataque se limitó a su división de producción de carrocerías de automóviles. Aunque se tomaron medidas de seguridad para contener la amenaza, la situación está bajo control y la empresa está trabajando para restablecer gradualmente sus operaciones normales. ThyssenKrupp asegura que el suministro a los clientes no se ha visto afectado. Aún se desconoce el tipo de violación y ningún grupo importante ha asumido la responsabilidad del incidente hasta el momento.

https://www.bleepingcomputer.com/news/security/steel-giant-thyssenkrupp-confirms-cyberattack-on-automotive-division/

cencora	**Farmacéutica Cencora sufrió ciberataque que afectó sus sistemas de TI**	IMPORTANTE

27FEB2024 La empresa farmacéutica estadounidense Cencora, sufrió un ciberataque en el que los actores de amenazas robaron datos de sus sistemas de TI corporativos los cuales podrían tener información personal de sus clientes y empleados. La compañía tomó medidas de contención y está colaborando con autoridades, expertos en ciberseguridad para investigar el incidente. Además, no se ha identificado al grupo responsable del ataque, sin embargo, un grupo de ransomware «Lorenz» afirmó haber violado la ciberseguridad de la compañía.

https://www.bleepingcomputer.com/news/security/pharmaceutical-giant-cencora-says-data-was-stolen-in-a-cyberattack/



Joe Biden bloqueó la transferencia masiva de datos personales a países de alto riesgo

IMPORTANTE

29FEB2024 El presidente de EE. UU., Joe Biden, firmó una Orden Ejecutiva para prohibir la transferencia masiva de datos personales de ciudadanos a países de interés, con el fin de salvaguardar información confidencial como datos genómicos, biométricos, de salud, financieros y de identificación personal. Esta medida busca proteger la privacidad de los ciudadanos y prevenir posibles abusos por parte de actores de amenazas extranjeros (vigilancia intrusiva, chantaje y otras violaciones de la seguridad nacional). Además, exige a las agencias federales establecer regulaciones para limitar el acceso a estos datos y garantizar que los fondos federales no se utilicen indebidamente para facilitar el acceso a información confidencial.

https://thehackernews.com/2024/02/president-biden-blocks-mass-transfer-of.html

VULNERABILIDADES

chrome OS

ChromeOS identificó múltiples vulnerabilidades

CRÍTICO
(Puntuación CVSS: 9.8)

23FEB2024 ChromeOS identificó múltiples vulnerabilidades; CVE-2024-0611, CVE-2024-0646, CVE-2024-1283, CVE-2024-1284 y CVE-2024-6817, las cuales podrían afectar la versión anterior a 120.0.6099.294 (Versión de plataforma: 15662.94.0). Un atacante remoto podría aprovechar algunas de estas para desencadenar una condición de denegación de servicio, ejecución remota de código y divulgación de información confidencial en el sistema.

https://www.hkcert.org/security-bulletin/chromeos-multiple-vulnerabilities_20240223
https://chromereleases.googleblog.com/2024/02/long-term-support-channel-update-for_21.html

NetApp®

NetApp identificó una vulnerabilidad de denegación de servicio

ALTO
(Puntuación CVSS: 7.4)

26FEB2024 NetApp identificó una vulnerabilidad en sus sistemas (CVE-2024-0565), la cual tendría la capacidad de afectar las Herramientas ONTAP para VMware vSphere 9, con la cual el atacante remoto podría aprovechar para desencadenar la divulgación de información, manipulación de datos y denegación de servicio.

https://www.hkcert.org/security-bulletin/netapp-denial-of-service-vulnerability_20240226
https://security.netapp.com/advisory/ntap-20240223-0002/

	**Múltiples vulnerabilidades de Microsoft Edge**	**ALTO (Puntuación CVSS: 8.2)**

26FEB2024 Se identificaron múltiples vulnerabilidades en Microsoft Edge, las cuales se identifican como; CVE-2024-1669, CVE-2024-1670, CVE-2024-1671, CVE-2024-1672, CVE-2024-1673, CVE-2024-1674, CVE-2024-1675, CVE-2024-1676, CVE-2024-26192. Dichas fallas afectan la versión de Microsoft Edge (estable) anterior a 122.0.2365.52. Un atacante remoto podría aprovechar algunas de estas vulnerabilidades para desencadenar la divulgación de información, la ejecución remota de código, la elusión de restricciones de seguridad y la condición de denegación de servicio en el sistema objetivo.

https://www.hkcert.org/security-bulletin/mozilla-products-multiple-vulnerabilities_20240222

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

29FEB2024 Se identificaron dos vulnerabilidades en Google Chrome, las cuales se identifican como; CVE-2024-1938 y CVE-2024-1939. Dichas fallas afectan la versión Google Chrome anterior a 122.0.6261.94 (Linux), Google Chrome anterior a 122.0.6261.94 (Mac) y Google Chrome anterior a 122.0.6261.94/.95 (Windows). Un atacante remoto podría aprovechar algunas de estas para desencadenar una condición de denegación de servicio y la ejecución remota de código en el sistema objetivo.

https://www.hkcert.org/security-bulletin/google-chrome-multiple-vulnerabilities_20240229
https://chromereleases.googleblog.com/2024/02/stable-channel-update-for-desktop_27.html