BOLETÍN INFORMATIVO 01-07MAR2024

CONCIBER

Comité Nacional de Seguridad Cibernética

Boletín de Ciberseguridad

CONCIBER
Comité Nacional de Seguridad Cibernética

FORTINET

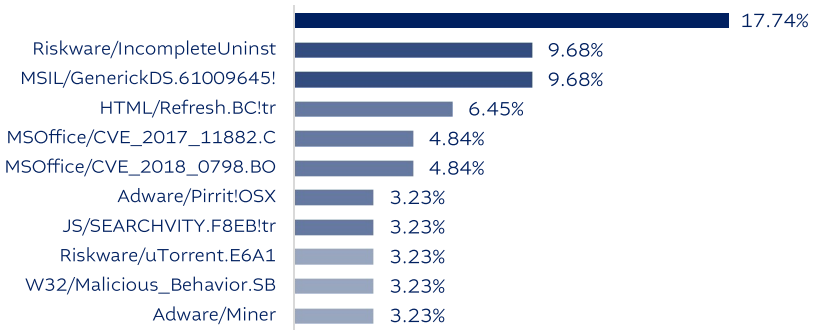
Reporte de amenazas cibernéticas en Guatemala

IMPORTANTE

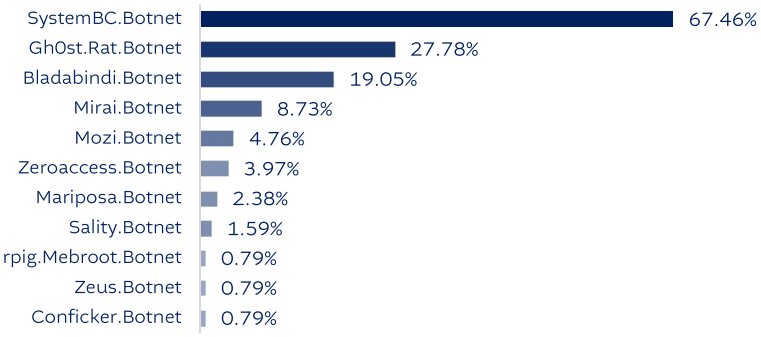
01-07MAR2024 Principales amenazas cibernéticas en Guatemala, según reporte semanal de FORTIGUARD.

Principales amenazas

Virus



Botnet



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

kaspersky	**Amenazas de tipo ransomware**	IMPORTANTE

01-07MAR2024 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	9.53%
Trojan.Script.Ext.gen	8.29%
Trojan.Script.Ext.gen	2.51%
Hoax.PDF.Phish.gen	2.37%
Trojan.WinLNK.Agent.gen	2.33%
Trojan.Win32.Agent.gen	2.22%
Worm.Python.Agent.gen	2.17%

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

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

01-07MAR2024 Según el reporte semanal del radar de CloudFlare, el mayor porcentaje de tráfico de bots se registró en Irán (94.99 %) seguido de Isla de Man (67.94 %), Turkmenistán (67.28 %) y Singapur (64.63 %).

Principales países con mayor porcentaje de tráfico de bots

Posición	País	Tráfico de bots
1	Irán	94.99%
2	Isla de Man	67.94%
3	Turkmenistán	67.28%
4	Singapur	64.63%
5	Irlanda	64.02%

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

SPAMHAUS

ISPs con mayor número de spam-bots detectados

IMPORTANTE

01-07MAR2024 El reporte semanal de SPAMHAUS, los proveedores de servicios de internet -ISP- que poseen el mayor número de spam-bots son; charter.com, airtel.in, Microsoft.com y djaweb.dz. 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	174,596
2	Airtel.in	173,692
3	Microsoft.com	137,663
4	Djaweb.dz	120,384
5	Chinanet-js	104,107
6	Telkom.co.id	72,551
7	Unicom-ln	67,374
8	Chinanet-zj	67,120
9	Verizon.com	61,967
10	Tedata.net	58,109

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

Panorama de amenazas cibernéticas y vulnerabilidades

AMENAZAS

	**EE. UU. acusa a Irán de hackear organizaciones de defensa**	IMPORTANTE

01MAR2024 El Departamento de Justicia de EE. UU. acusó a Alireza Shafie Nasab, ciudadano iraní de 39 años, por su participación en una campaña de ciberespionaje dirigida al gobierno y a entidades de defensa de EE. UU. Esta campaña operó en el periodo de 2016 hasta ABR2021, afectando a más de una docena de organizaciones estadounidenses, incluidos departamentos gubernamentales y empresas privadas. Las autoridades estadounidenses afirman que Nasab se enfrenta a cargos que incluyen conspiración para cometer fraude informático y electrónico, fraude electrónico y robo de identidad agravado.

https://www.bleepingcomputer.com/news/security/us-charges-iranian-for-hacks-on-defense-orgs-offers-10m-for-info/

	**Corea del Norte pirateó empresas de chips de Corea del Sur para robar datos**	IMPORTANTE

04MAR2024 El Servicio Nacional de Inteligencia –NIS- de Corea del Sur alertó sobre ataques cibernéticos norcoreanos dirigidos a fabricantes de semiconductores surcoreanos, comprometiendo servidores expuestos a Internet y robando datos confidenciales. Aunque no se mencionan las víctimas, las empresas de semiconductores «Samsung Electronics» y «SK Hynix» podrían ser objetivos. El NIS sugiere que Corea del Norte podría estar buscando desarrollar su propia tecnología de chips debido a las sanciones internacionales.

https://www.bleepingcomputer.com/news/security/north-korea-hacks-two-south-korean-chip-firms-to-steal-engineering-data/

	**Ucrania pirateó servidores del Ministerio de Defensa ruso**	IMPORTANTE

04MAR2024 El Ministerio de Defensa de Ucrania, a través de su Dirección Principal de Inteligencia –GUR-, anunció la realización de un ciberataque a servidores del Ministerio de Defensa ruso, el cual se obtuvieron documentos confidenciales (software de cifrado, documentos secretos del servicio de inteligencia ruso y detalles sobre la estructura del sistema ministerio ruso). Además, el análisis de los datos obtenidos ayudó a identificar a generales y otros altos directivos de las divisiones estructurales del Ministerio de Defensa ruso, los cuales utilizaban el software para la gestión de documentos electrónicos.

https://www.bleepingcomputer.com/news/security/ukraine-claims-it-hacked-russian-ministry-of-defense-servers/

Google	**Ingeniero de Google robó secretos tecnológicos de inteligencia artificial**	**IMPORTANTE**

07MAR2024 El Departamento de Justicia de EE. UU. acusó a Linwei Ding, un ex ingeniero de software de Google, de robar secretos comerciales de inteligencia artificial de la empresa para empresas chinas. Ding presuntamente robó información sobre tecnologías clave de inteligencia artificial de Google y la transfirió a dos empresas chinas, donde trabajaba en secreto. Los cargos alegan que Ding copió información patentada sobre arquitectura de chips, sistemas de procesamiento de gráficos y software utilizado en centros de datos de supercomputación de Google.

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

VULNERABILIDADES

	Microsoft Edge identificó múltiples vulnerabilidades	**MEDIO (Puntuación CVSS: 5.8)**

01MAR2024 Microsoft Edge identificó dos vulnerabilidades; CVE-2024-1938 y CVE-2024-1939, las cuales podrían afectar la versión Microsoft Edge (estable) anterior a 122.0.2365.63. Un atacante remoto podría aprovechar algunas de estas para desencadenar la ejecución remota de código en el sistema objetivo.

https://www.hkcert.org/security-bulletin/microsoft-edge-remote-code-execution-vulnerability_20240301

IBM MQ	**IBM MQ identificó múltiples vulnerabilidades**	**CRÍTICO (Puntuación CVSS: 9.8)**

04MAR2024 IBM MQ identificó múltiples vulnerabilidades en sus sistemas; CVE-2023-4218, CVE-2023-26159, CVE-2023-39976, CVE-2023-44487, CVE-2023-47745 y CVE-2024-25016. Las cuales tendrían la capacidad de afectar las versiones IBM MQ 9.0 LTS, IBM MQ 9.1LTS, IBM MQ 9.2LTS, IBM MQ 9.3LTS y CD de IBM MQ 9.3. Un atacante remoto podría aprovechar alguna de estas para desencadenar una condición de denegación de servicio, divulgación de información confidencial y ejecución remota de código en el sistema objetivo.

https://www.hkcert.org/security-bulletin/ibm-mq-multiple-vulnerabilities_20240304
https://www.auscert.org.au/bulletins/ESB-2024.1326/

SAMSUNG	**Múltiples vulnerabilidades en productos Samsung**	**CRÍTICO (Puntuación CVSS: 9.3)**

06MAR2024 Se identificaron múltiples vulnerabilidades en productos Samsung, las cuales se identifican como; CVE-2023-5091, CVE-2023-5249, CVE-2023-5643, CVE-2023-21135, CVE-2023-21234, CVE-2023-32841, CVE-2023-32842, CVE-2023-32843, CVE-2023-33046, CVE-2023-33049, CVE-2023-33057, CVE-2023-33058, CVE-2023-33060, CVE-2023-33072 y CVE-2023-33076. Dichas fallas afectan la tecnología Androide 11, 12, 13, 14. Un atacante remoto podría aprovechar algunas de estas vulnerabilidades 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/samsung-products-multiple-vulnerabilities_20240306
https://security.samsungmobile.com/securityUpdate.smsb

	Múltiples vulnerabilidades en productos de Apple	**ALTO (Puntuación CVSS: 7.8)**

06MAR2024 Se identificaron cuatro vulnerabilidades en productos Apple, las cuales se identifican como; CVE-2024-23225, CVE-2024-23243, CVE-2024-23256 y CVE-2024-23296. Dichas fallas afectan las versiones iOS 16.7.6 y iPadOS 16.7.6, iOS 17.4 y iPadOS 17.4. Un atacante con capacidad arbitraria de lectura y escritura del kernel puede eludir las protecciones de la memoria del kernel. Apple tiene conocimiento de un informe que indica que este problema puede haber sido aprovechado. Para explotar estas vulnerabilidades, los atacantes necesitan capacidad arbitraria de lectura y escritura del kernel. Por lo tanto, el nivel de riesgo se califica como Riesgo Medio.

https://www.hkcert.org/security-bulletin/apple-products-multiple-vulnerabilities_20240306
https://support.apple.com/en-us/HT214082

	Vulnerabilidades de ejecución remota de código de Google Chrome	**MEDIO (Puntuación CVSS: 6.5)**

06MAR2024 Se identificaron tres vulnerabilidades en Google Chrome, las cuales se identifican como; CVE-2024-2173, CVE-2024-2174 y CVE-2024-2176. Dichas fallas afectan las versiones Google Chrome anterior a 122.0.6261.111 (Linux), Google Chrome anterior a 122.0.6261.111/.112 (Mac), Google Chrome anterior a 122.0.6261.111/.112 (Windows). Por lo que un atacante remoto podría aprovechar algunas de estas vulnerabilidades para desencadenar la ejecución remota de código en los sistemas.

https://www.hkcert.org/security-bulletin/google-chrome-remote-code-execution-vulnerabilities_20240307
https://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop.html