BOLETÍN INFORMATIVO 09-15FEB2024

CONCIBER

Comité Nacional de Seguridad Cibernética

Boletín de Ciberseguridad

CONCIBER
Comité Nacional de Seguridad Cibernética

FORTINET

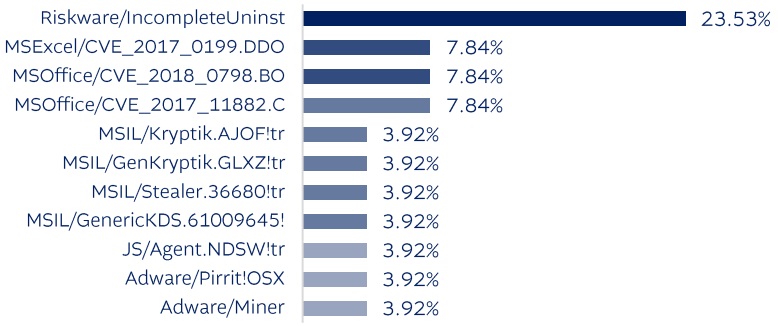
Reporte de amenazas cibernéticas en Guatemala

IMPORTANTE

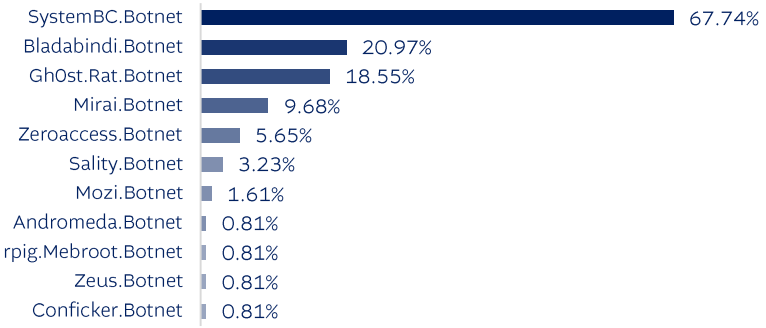
09-15FEB2024 Principales amenazas cibernéticas en Guatemala, según reporte semanal de FORTIGUARD.

Principales amenazas

Virus



Botnet



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

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

09-15FEB2024 El mapa en tiempo real de ciberamenazas de KASPERSKY, registró el flujo de detección de malware mediante On-Acces Scan, este realiza 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 en Guatemala

Troyanos	Frecuencia
Trojan.WinLNK.Agent.gen	11.57%
Trojan-Dropper.Script.Dorifel.gen	6.34%
DangerousObject.Multi.Generic	6.06%
Trojan.WinLNK.Agent.wu	5.23%
Trojan-Downloader.MSIL.Bitser.gen	4.41%
VHO:Trojan.Win32.Hesv.avwq	3.58%
Trojan-Banker.Win32.ClipBanker.gen	3.58%

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

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

09-15FEB2024 Según el reporte semanal del radar de CloudFlare, el mayor porcentaje de tráfico de bots se registró en Irán (95.96 %) seguido de Guinea (74.70 %), Singapur (69.13 %) e Irlanda (66.54 %).

Principales países con mayor porcentaje de tráfico de bots

Posición	País	Tráfico de bots
1	Irán	95.96%
2	Guinea	74.70%
3	Singapur	69.13%
4	Irlanda	66.54%
5	Islas Vírgenes	65.95%

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

CONCIBER
Comité Nacional de Seguridad Cibernética

SPAMHAUS

ISPs con mayor número de spam-bots detectados

IMPORTANTE

09-15FEB2024 Según 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	178,473
2	Microsoft.com	146,142
3	Verizon.com	62,162
4	Chinanet-js	55,258
5	Virginmedia.com	47,261
6	Bt.com	42,394
7	Sky.uk	32,502
8	Airtel.in	32,445
9	t-mobile.com	27,993
10	Vnpt.vn	27,434

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

Panorama de amenazas cibernéticas y vulnerabilidades
AMENAZAS

BANK OF AMERICA	**Bank of America advirtió a clientes sobre violación de datos**	IMPORTANTE

12FEB2024 Bank of America informó a sus clientes sobre una violación de datos que expuso información personal después de que uno de sus proveedores de servicios, Infosys McCamish Systems –IMS-, fuera hackeado en 2023. La información personal de los clientes incluye nombres, direcciones, números de seguro social, fechas de nacimiento y datos financieros (números de cuenta y tarjetas de crédito). Se estimó que alrededor de 57,028 personas se vieron directamente afectadas. El actor de amenazas «LockBit» se atribuyó la responsabilidad del ataque a IMS, cifrando más de 2,000 sistemas durante la infracción.

https://www.bleepingcomputer.com/news/security/bank-of-america-warns-customers-of-data-breach-after-vendor-hack/

INTEGRIS HEALTH	**Integris Health registró una violación de datos que afectó a 2.4 millones de pacientes**	IMPORTANTE

13FEB2024 La red de atención médica sin fines de lucro más grande de Oklahoma, Integris Health, reportó a las autoridades estadounidenses que una filtración de datos en NOV2023 expuso información personal de aproximadamente 2.4 millones de personas. Los datos filtrados incluyen nombres, fechas de nacimiento, información de contacto, números de seguro social y otros datos demográficos. Sin embargo, el ataque no provocó ninguna interrupción de la red y permitió a Integris Health seguir brindando sus servicios a los pacientes.

https://www.bleepingcomputer.com/news/security/integris-health-says-data-breach-impacts-24-million-patients/

Facebook Marketplace	**Facebook Marketplace sufrió una filtración de datos por medio de un foro de piratería**	IMPORTANTE

13FEB2024 El actor de amenazas «IntelBroker» filtró 200,000 registros en un foro de piratas informáticos, afirmando que contienen números de teléfono móvil, direcciones de correo electrónico y otra información personal de usuarios de Facebook Marketplace. Los actores de amenazas podrían utilizar esta información para llevar a cabo ataques de phishing y ataques de intercambio de SIM, entre otros. Además, en ABR2021, se filtraron datos vinculados a más de 533 millones de cuentas de Facebook, recibiendo una multa de alrededor USD 276 millones por no proteger la información personal de usuarios de Facebook.

https://www.bleepingcomputer.com/news/security/200-000-facebook-marketplace-user-records-leaked-on-hacking-forum/

	Hackers chinos realizan ataques avanzados de malware a la banca móvil en región APAC	IMPORTANTE

15FEB2024 Grupo de amenazas chino, GoldFactory, se identificó como el responsable del desarrollo de un troyano bancario para iOS y Android «GoldPickaxe» el cual puede recopilar documentos de identidad, datos de reconocimiento facial e interceptar SMS. Sus ataques se dirigen principalmente a la región de Asia y el Pacífico y se llevan a cabo a través de ingeniería social para dirigir a las víctimas a aplicaciones de mensajería instantánea. Además, tanto las versiones para Android como para iOS pueden recopilar datos sensibles de las víctimas y facilitar transferencias de fondos no autorizadas.

https://thehackernews.com/2024/02/chinese-hackers-using-deepfakes-in.html

VULNERABILIDADES

	Microsoft Edge identificó múltiples vulnerabilidades	CRÍTICO (Puntuación CVSS: 9.8)

09FEB2024 Se identificaron dos vulnerabilidades en Microsoft Edge; CVE-2024-1283 y CVE-2024-1284. Podrían afectar a las versiones Microsoft Edge (estable) anterior a 121.0.2277.113 y Microsoft Edge (estable extendido) anterior a 120.0.2210.175. Un atacante remoto podría aprovechar algunas de estas fallas para desencadenar la divulgación de información, la ejecución remota de código y una condición de denegación de servicio en el sistema.

https://learn.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#february-8-2024

FORTINET	**Múltiples vulnerabilidades de productos Fortinet**	CRÍTICO (Puntuación CVSS: 9.8)

09FEB2024 Fortinet identificó múltiples vulnerabilidades en sus productos; CVE-2023-26206, CVE-2023-44487, CVE-2023-45581, CVE-2023-47537, CVE-2024-21762 y CVE-2024-23113. Un atacante remoto podría aprovechar algunas de estas para desencadenar una condición de denegación de servicio, ejecución remota de código, divulgación de información confidencial y secuencias de comandos entre sitios.

https://fortiguard.fortinet.com/psirt/FG-IR-23-063
https://www.hkcert.org/security-bulletin/fortinet-products-multiple-vulnerabilities_20240209

zoom	**Múltiples vulnerabilidades en productos de Zoom**	**CRÍTICO (Puntuación CVSS: 7.2)**

14FEB2024 Se identificaron múltiples vulnerabilidades en productos de Zoom las cuales se registraron como CVE-2024-24690, CVE-2024-24691, CVE-2024-24695, CVE-2024-24696, CVE-2024-24697, CVE-2024-24698 y CVE-2024-24699. Un atacante remoto podría aprovechar algunas de estas para desencadenar una condición de denegación de servicio, elevación de privilegios y divulgación de información confidencial.

https://www.hkcert.org/security-bulletin/zoom-products-multiple-vulnerabilities_20240214
https://www.zoom.com/en/trust/security-bulletin/ZSB-24002/

node JS	**Múltiples vulnerabilidades de Node.js**	**ALTO (Puntuación CVSS: 7.0)**

15FEB2024 Node.js identificó las vulnerabilidades CVE-2023-46809, CVE-2024-21890, CVE-2024-21891, CVE-2024-21892, CVE-2024-21896, CVE-2024-22017, CVE-2024-22019, CVE-2024-22025. Dichas fallas afectan las versiones Versiones de Node.js anteriores a 18.19.1 (LTS), 20.11.1 (LTS) y 21.6.2 (Actual). Un atacante remoto puede aprovechar estas para provocar denegación de servicio, elusión de restricciones de seguridad, elevación de privilegios y divulgación de información confidencial.

https://www.hkcert.org/security-bulletin/android-multiple-vulnerabilities_20240207
https://source.android.com/docs/security/bulletin/2024-02-01?hl=es