BOLETÍN INFORMATIVO 02-08FEB2024

CONCIBER

Comité Nacional de Seguridad Cibernética

CONCIBER
Comité Nacional de Seguridad Cibernética

Boletín de Ciberseguridad

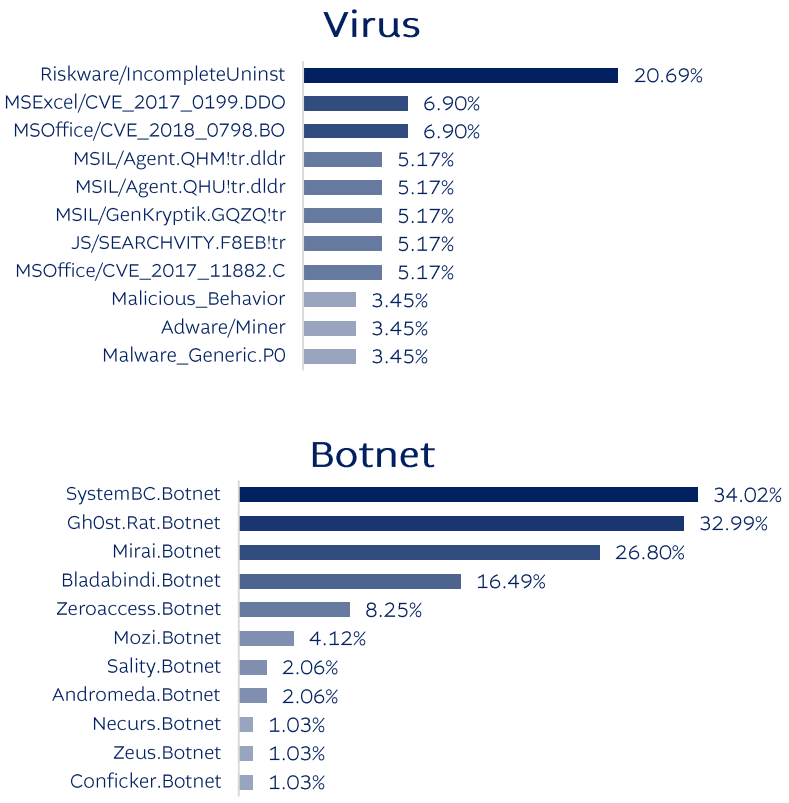
FORTINET

Reporte de amenazas cibernéticas en Guatemala

IMPORTANTE

02-08FEB2024 Principales amenazas cibernéticas en Guatemala, según reporte semanal de FORTIGUARD.

Principales amenazas



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

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

02-08FEB2024 El mapa en tiempo real de ciberamenazas de KASPERSKY, registró el flujo de detección de malware a través de aplicaciones de email durante la semana, siendo los más frecuentes el troyano Trojan.Win32.Badun.gen (27.95 %); el Trojan-PSW.MSIL.Agentla.wng (10.48 %) y Trojan-PSW.MSIL.Agensla.wpn (6.60 %).

Principales troyanos de tipo ransomware en Guatemala

Ransomware	Frecuencia
Trojan.Win32.Badun.gen	27.95%
Trojan-PSW.MSIL.Agentla.wng	10.48%
Trojan-PSW.MSIL.Agensla.wpn	6.60%
Trojan-PSW.MSIL.Agensla.gen	5.36%
DangerousObject.Multi.Generic	4.50%
Trojan-PSW.MSIL.Agensla.wpg	3.42%
Trojan.Msil.Taskun.gen	3.34%
Trojan-Spy.Win32.Stealer.fbsn	2.80%

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

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

02-08FEB2024 Según el reporte semanal del radar de CloudFlare, el mayor porcentaje de tráfico de bots se registró en Irán (95.39 %) seguido de Islas Vírgenes (83.04 %), Gibraltar (73.00 %) y Guinea (72.97 %).

Principales países con mayor porcentaje de tráfico de bots

Posición	País	Tráfico de bots
1	Irán	95.39%
2	Islas Vírgenes	83.04%
3	Gibraltar	73.00%
4	Guinea	72.97%
5	Singapur	69.47%

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

SPAMHAUS

ISPs con mayor número de spam-bots detectados

IMPORTANTE

02-08FEB2024 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	116,834
2	Chinanet-js	114,261
3	Microsoft.com	104,077
4	Chinanet-zj	77,212
5	Unicom-in	73,121
6	Tedata.net	61,681
7	chinanet-ah	59,045
8	Verizon.com	42,657
9	Chinanet-fj	34,169
10	Turkcell.com.tr	32,366

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

Panorama de amenazas cibernéticas y vulnerabilidades
AMENAZAS

IABC Asia/Pacific Region	**Agencias de empleo y empresas de la región APAC fueron atacadas por piratas informáticos**	IMPORTANTE

06FEB2024 Agencias de empleo y empresas minoristas ubicadas en la región de Asia Pacífico fueron atacadas por el actor de amenazas «ResumeLooters». El modus operandi implica el uso de la herramienta de código abierto sqlmap para llevar a cabo ataques de inyección SQL y soltar y ejecutar cargas útiles adicionales y código JavaScript fraudulento diseñado para recopilar datos confidenciales. y redirigir a los usuarios a páginas de recolección de credenciales.

https://thehackernews.com/2024/02/hackers-exploit-job-boards-in-apac.html

National Security Agency United States of America	**Agencia de Seguridad Nacional destacó ataques de China a infraestructura crítica de EE. UU.**	IMPORTANTE

07FEB2024 Agencia de Seguridad Nacional (NSA) en colaboración con otras agencias gubernamentales emitieron un aviso de ciberseguridad –CSA- con el objetivo de abordar ataques de la República Popular China hacia la infraestructura crítica de EE. UU. El CSA se centra en el grupo cibernético patrocinado por el Gobierno chino, «Volt Typhoon», que comprometió redes de TI en sectores clave. El informe destacó que la actividad de dicho actor de amenazas no se limita al ciberespionaje tradicional, sino que también tiene el potencial de interrumpir las funciones de OT en múltiples entidades de infraestructura crítica.

https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3669141/nsa-and-partners-spotlight-peoples-republic-of-china-targeting-of-us-critical-i/

Viamedis HEALTH DATA MANAGEMENT almerys Healthcare delivery management	**Filtraciones de datos a proveedores franceses afectaron a 33 millones de personas**	IMPORTANTE

08FEB2024 Proveedores franceses de servicios de pago de atención médica, Viamedis y Almerys, sufrieron filtraciones de datos afectando a más de 33 millones de personas en Francia. La exposición incluía información como nombres, fechas de nacimiento, detalles de la aseguradora y números de seguro social. Aunque no se expusieron datos bancarios ni de contacto, la violación comprometió información sensible necesaria para reembolsos y otros procesos. La autoridad de protección de datos de Francia confirmó ambos incidentes, calificándolos como uno de los ciberataques más significativos en la historia reciente del país.

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

VULNERABILIDADES

	**Múltiples vulnerabilidades de ejecución remota de Microsoft Edge**	**ALTO (Puntuación CVSS: 8.8)**

05FEB2024 Múltiples vulnerabilidades en Microsoft Edge identificados como CVE-2024-1059, CVE-2024-1060, CVE-2024-1077 y CVE-2024-21399. Podrían afectar a las versiones Microsoft Edge (estable) anterior a 121.0.2277.98 y Microsoft Edge (estable extendido) anterior a 120.0.2210.167. Un atacante remoto podría aprovechar algunas de estas fallas para desencadenar la ejecución remota de código en el sistema objetivo.

https://www.hkcert.org/security-bulletin/microsoft-edge-remote-code-execution-vulnerabilities_20240205
https://learn.microsoft.com/en-us/deployedge/microsoft-edge-relnotes-security#february-1-2024

QNAP	**Múltiples vulnerabilidades del NAS de QNAP**	**ALTO (Puntuación CVSS: 7.2)**

05FEB2024 QNAP NAS identificó múltiples vulnerabilidades en sus sistemas; CVE-2023-32967, CVE-2023-39297, CVE-2023-39302, CVE-2023-39303, CVE-2023-41273, CVE-2023-41274, CVE-2023-41275, CVE-2023-41276, CVE-2023-41277, CVE-2023-41278, CVE-2023-41279, CVE-2023-41280, CVE-2023-41281, CVE-2023-41282, CVE-2023-41283, CVE-2023-41292, CVE-2023-45036, CVE-2023-45037, CVE-2023-47566, CVE-2023-47567, CVE-2023-47568 y CVE-2023-50359. Un atacante remoto podría aprovechar algunas de estas fallas para desencadenar una condición de denegación de servicio, ejecución remota de código, divulgación de información confidencial y elusión de restricciones de seguridad en el sistema objetivo.

https://www.hkcert.org/security-bulletin/qnap-nas-multiple-vulnerabilities_20240205
https://www.qnap.com/en/security-advisory/qsa-23-30

SUSE	**Múltiples vulnerabilidades del kernel de SUSE Linux**	**CRÍTICO (Puntuación CVSS: 9.8)**

07FEB2024 Se identificaron tres vulnerabilidades en SUSE Linux Kernel las cuales se registraron como CVE-2023-5178, CVE-2023-6176 y CVE-2023-6932. Estas fallas podrían afectar a las versiones SUSE Linux Enterprise Micro 5.1, 5.2, 5.3, 5.4 y 5.5. Un atacante remoto podría explotar estas vulnerabilidades para desencadenar una condición de denegación de servicio, elevación de privilegios y ejecución remota de código.

https://www.hkcert.org/security-bulletin/suse-linux-kernel-multiple-vulnerabilities_20240207
https://www.suse.com/support/update/announcement/2024/suse-su-20240348-1/

android	**Android identificó múltiples vulnerabilidades en sus sistemas**	**ALTO (Puntuación CVSS: 7.5)**

07FEB2024 Sistema operativo Android identificó las vulnerabilidades CVE-2023-40093, CVE-2023-40122, CVE-2024-0014, CVE-2024-0029, CVE-2024-0030, CVE-2024-0031, CVE-2024-0032, CVE-2024-0033, CVE-2024-0034, CVE-2024-0035, CVE-2024-0036, CVE-2024-0037, CVE-2024-0038, CVE-2024-0040 y CVE-2024-0041. Dichas fallas afectan el nivel de parche de seguridad de Android anterior al 2024-02-05. Un atacante remoto podría aprovechar algunas de estas para activar la elevación de privilegios, la ejecución remota de código y la 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

chromeOS	**ChromeOS identificó múltiples vulnerabilidades**	**ALTO (Puntuación CVSS: 8.8)**

08FEB2024 ChromeOS identificó las vulnerabilidades: CVE-2023-6817, CVE-2023-6932, CVE-2024-0806, CVE-2024-0807, CVE-2024-0808, CVE-2024-0809, CVE-2024-0811, CVE-2024-0813, CVE-2024-0814, CVE-2024-1280, CVE-2024-1281, CVE-2024-25556, CVE-2024-25557 y CVE-2024-25558. Dichas fallas podrían afectar a la versión anterior a 121.0.6167.159 (Versión de plataforma: 15699.58.0). Un atacante remoto podría aprovechar algunas de estas para desencadenar una condición de denegación de servicio, ejecución remota de código, elusión de restricciones de seguridad y manipulación de datos en el sistema objetivo.

https://www.hkcert.org/security-bulletin/chromeos-multiple-vulnerabilities_20240208
https://chromereleases.googleblog.com/2024/02/stable-channel-update-for-chromeos.html