BOLETÍN INFORMATIVO 03-09MAY2024

CONCIBER

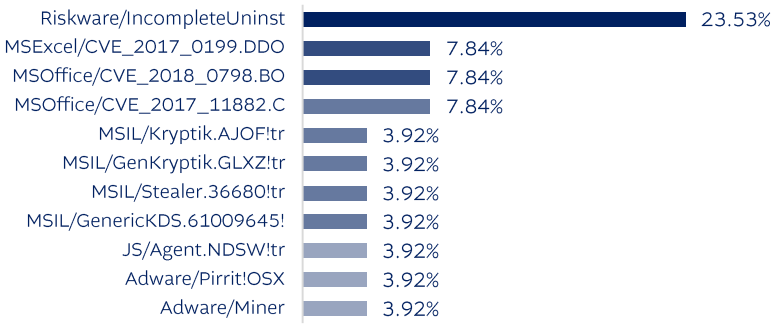
Comité Nacional de Seguridad Cibernética

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

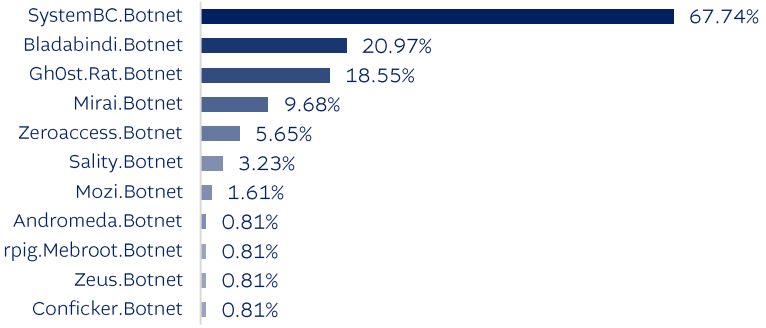
03-09MAY2024 Principales amenazas cibernéticas en Guatemala, según reporte semanal de FORTIGUARD.

Principales amenazas

Virus



Botnet



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

kaspersky

Amenazas de tipo ransomware en Guatemala

IMPORTANTE

03-09MAY2024 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

03-09MAY2024 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/

CONCIBER
Comité Nacional de Seguridad Cibernética

Panorama de amenazas cibernéticas y vulnerabilidades

AMENAZAS

	La NSA FBI alertan sobre actividad cibernética de piratas informáticos norcoreanos	IMPORTANTE

03MAY2024 El gobierno de Estados Unidos publicó recientemente un nuevo aviso de seguridad cibernética advirtiendo sobre los intentos de los actores de amenazas norcoreanos de enviar correos electrónicos falsificados con la apariencia de ser legítimos y confiables.

https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3762915/nsa-highlights-mitigations-against-north-korean-actor-email-policy-exploitation/

Microsoft Graph	**Piratas informáticos abusan de la API Microsoft Graph**	IMPORTANTE

03MAY2024 Actores de amenazas utilizan de forma maliciosa la API «Microsoft Graph» como arma para evadir la detección, con el fin de obtener acceso privilegiado.

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/graph-api-threats

	APT28 aprovecha fallo de seguridad en Microsoft Outlook	IMPORTANTE

04MAY2024 Republica Checa y Alemania revelaron que fueron el objetivo de una campaña de ciberespionaje a largo plazo, llevada a cabo por el «actor-Estado-nación» vinculado a Rusia conocido como APT28.

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

	Instituciones polacas se ven afectadas tras ciberataques	IMPORTANTE

09MAY2024 Actor de amenazas denominado «APT28» vinculado a la república de Rusia perpetuaron un ciberataque de tipo ransomware a gran escala que afecto a distintas instituciones del gobierno de Polonia.

https://cert.pl/en/posts/2024/05/apt28-campaign/

CONCIBER
Comité Nacional de Seguridad Cibernética

VULNERABILIDADES

HPE aruba networking	**Vulnerabilidades críticas en dispositivos HPE Networks**	**CRÍTICO (Puntuación CVSS: 9.3)**

03MAY2024 HPE Aruba Networking ha lanzado actualizaciones de seguridad para abordar fallas críticas que afectan a ArubaOS y que podrían resultar en la ejecución remota de código (RCE) en los sistemas afectados.

https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2024-004.txt

	**Piratas informáticos aprovechan fallo en el servicio LiteSpeed Web Server**	**CRÍTICO (Puntuación CVSS: 8.3)**

09FEB2024 Actores de amenazas están explotando activamente una falla de alta gravedad que afecta al complemento LiteSpeed Cache para WordPress para crear cuentas de administrador fraudulentas en sitios web susceptibles.

https://nvd.nist.gov/vuln/detail/CVE-2023-40000