BOLETÍN INFORMATIVO 20-26OCT2023

CONCIBER

Comité Nacional de Seguridad Cibernética

Boletín de Ciberseguridad

ESET	**Amenazas cibernéticas en Guatemala**	**IMPORTANTE**

20-26OCT2023 Según el reporte semanal de Virus Radar de ESET sobre el incremento y descenso de ciberamenazas más aprovechadas por ciberdelincuentes en Guatemala, la amenaza con mayor incidencia fue HTML/Scrinject (10.31 %) seguida de SMB.Attack.Bruteforce (7.82 %).

Principales amenazas cibernéticas en Guatemala

	Threat Name	Change	Prevalence Level
1	HTML/ScrInject	▲	10.31 %
2	SMB.Attack.Bruteforce	▲	7.82 %
3	RDP.Attack.Bruteforce	▲	4.27 %
4	JS/Packed.Agent.K	▲	3.33 %
5	JS/Adware.Adport	▼	3.26 %
6	JS/Packed.Agent.L	▲	3.21 %
7	Win32/Phorpiex	▼	2.84 %
8	JS/Adware.TerraClicks	▲	2.18 %
9	Android/Packed.TencentProtect.D	▼	2.15 %
10	Android/Pandora	▲	2.01 %

Fuente: Virus Radar

https://virusradar.com/en/statistics/10

kaspersky	Amenazas de tipo ransomware en Guatemala	IMPORTANTE

20-26OCT2023 El mapa en tiempo real de ciberamenazas de KASPERSKY evidenció que en Guatemala el software malicioso con mayor incidencia durante la semana fue el troyano Trojan-Ransom.Win32.Crypmodady.gen (88.192%) seguido de Trojan-Ransom.win32.Blocker-a (2.75 %) .

Principales troyanos de tipo ransomware en Guatemala

1	trojan-ransom.win32.Crypmodadv.gen	88.19%
2	Trojan-Ransom.Win32.Blocker.a	2.75%
3	Trojan-Ransom.Win32.Autoit.b	2.2%
4	trojan-ransom.win32.Blocker.dap	2.2%
5	Trojan-Ransom.Win32.Crypmodng.gen	1.92%
6	Trojan-Ransom.MSIL.PolyRansom.gen	1.1%
7	trojan-ransom.win32.Crypmod.gen	0.55%
8	Trojan-Ransom.Win32.Blocker.gen	0.55%
9	Trojan-Ransom.Win64.Convagent.gen	0.27%
10	Trojan-Ransom.Win32.Stop.gen	0.27%

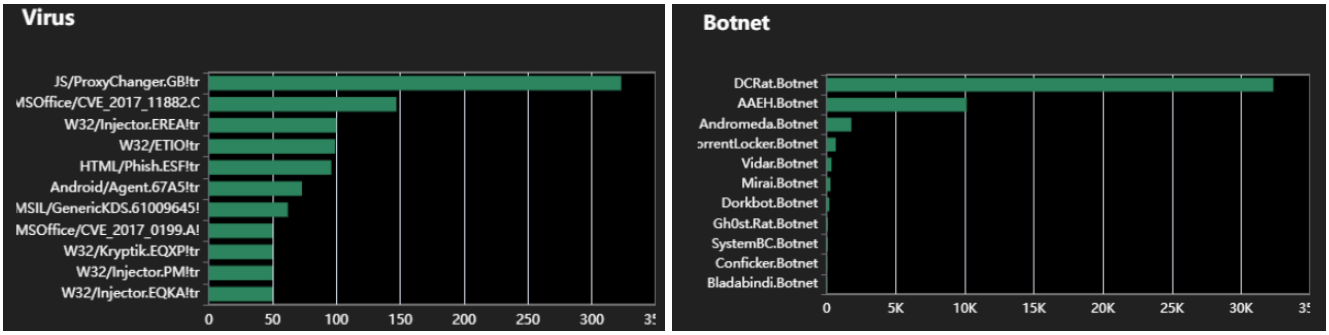
Fuente: CYBERMAP

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

FORTINET	Reporte de amenazas cibernéticas en Guatemala	IMPORTANTE

20-26OCT2023 Principales amenazas cibernéticas en Guatemala, según reporte semanal de FORTIGUARD

Principales amenazas



Fuente: FORTIGUARD

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

SPAMHAUS	**Países con más incidencia de botnets**	IMPORTANTE

20-26OCT2023 Según reporte semanal de SPAMHAUS, los países con más spam-bots a nivel mundial son: China, Estados Unido, India, Venezuela e Indonesia. La mayoría de los bots detectados son utilizados como vectores de ataque de spam, phishing, fraude de clics, DDoS y otras actividades maliciosas.

Países con mayor índice de botnets en el mundo

1	China	Number of Bots: 588366
2	United States of America	Number of Bots: 390559
3	India	Number of Bots: 320598
4	Venezuela (Bolivarian Republic of)	Number of Bots: 180035
5	Indonesia	Number of Bots: 168284

6	Algeria	Number of Bots: 129772
7	Brazil	Number of Bots: 117511
8	Egypt	Number of Bots: 106998
9	Thailand	Number of Bots: 97336
10	United Kingdom of Great Britain and Northern Ireland	Number of Bots: 89203

Fuente: SPAMHAUS

https://www.spamhaus.org/statistics/botnet-cc/

	Campaña de publicidad maliciosa	IMPORTANTE

20OCT2023 Google informó sobre una campaña de publicidad maliciosa que aprovecha Google Ads para atraer a sus víctimas a sitios infectados, con el fin de distribuir software malicioso (malware, ransomware).

https://www.malwarebytes.com/blog/threat-intelligence/2023/10/the-forgotten-malvertising-campaign

	Instituciones públicas y privadas de Guatemala bajo Ciberataques	IMPORTANTE

21OCT2023 Instituciones públicas y privadas de Guatemala continúan bajo ciberataques bajo la Operación #OpDemocracia promovida por el actor de amenazas «Anonymous Guatemala».

https://twitter.com/hashtag/OpDemocracia?src=hashtag_click

CISCO	**Vulnerabilidad zero day en IOS XE CISCO**	**CRÍTICO (Puntuación CVSS de 10)**

22OCT2023 Vulnerabilidad zero day «CVE-2023-20198» presentó falla de escalada de privilegios en la función de interfaz de usuario web, permitiendo a un atacante remoto y no autenticado crear una cuenta en un sistema afectado con acceso de nivel de privilegio 15,

https://thehackernews.com/2023/10/cisco-zero-day-exploited-to-implant.html
https://nvd.nist.gov/vuln/detail/CVE-2023-20198

	**Ciberataque afectó a cinco hospitales en Canadá**	**IMPORTANTE**

23OCT2023 Proveedor canadiense de servicios de salud «TransForm» emitió un comunicado para informar sobre incidente de ciberseguridad que provocó la interrupción de los sistemas informáticos, incluido el correo electrónico de los hospitales miembros de la organización.

https://www.malwarebytes.com/blog/news/2023/10/cyberattack-on-service-provider-impacts-operations-in-5-hospitals
https://www.transformsso.ca/2023/10/23/immediate-release-systems-outage-update/

	**Hong Kong es objeto de campañas de publicidad maliciosa para WhatsApp y Telegram**	**IMPORTANTE**

24OCT2023 Actor de amenazas utiliza páginas web maliciosas suplantando la identidad de herramientas de mensajería instantánea. Esta campaña es impulsada a través de anuncios maliciosos de Google en los que los usuarios son redirigidos a una página similar a la versión web de «WhatsApp» y «Telegram» con el objetivo de vincular dispositivos del actor de amenazas a través del escaneo de un código QR engañoso. Los ataques han tenido como blanco exclusivo a pobladores de Hong Kong y se estima que en SEP2023 causaron pérdidas de alrededor de USD 300 mil.

https://www.malwarebytes.com/blog/threat-intelligence/2023/10/hong-kong-residents-targeted-in-malvertising-campaigns-for-whatsapp-telegram

The Hacker News	**Backdoor implantada en dispositivos alterados de CISCO**	**IMPORTANTE**

24OCT2023 Actor de amenazas implantó puerta trasera en dispositivos CISCO con el fin de realizar ataques que implican crear un usuario de acceso inicial (CVE-2023-20198) e inyectar comandos en la interfaz de usuario web de Cisco IOS XE (CVE-2023-20273) para elevar el privilegio a nivel de «súper usuario (*root)*» y escribir en el sistema de archivos para obtener acceso a los dispositivos.

https://thehackernews.com/2023/10/backdoor-implant-on-hacked-cisco.html

vmware®	**VMWare corrigió una vulnerabilidad crítica**	**IMPORTANTE**

25OCT2023 VMWare publicó una actualización para corregir la vulnerabilidad CVE-2023-34048 (puntuación 9.8) que afecta a las versiones Mware vCenter Server versions 7.0, 8.0, VMware Cloud Foundation versions 5.x y 4.x.
Esta vulnerabilidad permite a un atacante ejecutar código arbitrario y obtener acceso remoto.

https://www.malwarebytes.com/blog/news/2023/10/update-vcenter-server-now-vmware-fixes-critical-vulnerability
https://www.vmware.com/security/advisories/VMSA-2023-0023.html

	**Empresas importantes de Noruega se vieron afectadas tras un incidente informático**	**IMPORTANTE**

26OCT2023 Jefe de Seguridad Nacional de Noruega (NSM) emitió una advertencia sobre el abuso de explotación de dos vulnerabilidades identificadas como CVE-2023-20198 y CVE-2023-20273 por actores de amenazas que han afectado a empresas importantes de la región.

https://www.dn.no/teknologi/nsm/cybersikkerhet/sofie-nystrom/nsm-sjefen-bekrefter-handterer-nytt-avansert-cyberangrep-mot-norge/2-1-1538140
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z