BOLETÍN INFORMATIVO 06OCT-12OCT2023

CONCIBER

Comité Nacional de Seguridad Cibernética

CONCIBER
Comité Nacional de Seguridad Cibernética

Boletín de Ciberseguridad

Amenazas cibernéticas en Guatemala

IMPORTANTE

06OCT-12OCT2023 Según el reporte semanal de Virus Radar de ESET sobre el progreso y descenso de amenazas cibernéticas más aprovechadas por ciberdelincuentes, la amenaza con mayor incidencia en Guatemala fue SMB.Attack.Bruteforce (8.83 %) seguida de RDP.Attack.Bruteforce (5.79 %).

Principales amenazas cibernéticas en Guatemala

	Threat Name	Change	Prevalence Level	
1	SMB.Attack.Bruteforce	▲	8.83 %	Map-Timeline
2	RDP.Attack.Bruteforce	▲	5.79 %	Map-Timeline
3	JS/Packed.Agent.K	▼	4.82 %	Map-Timeline
4	JS/Packed.Agent.L	▼	3.42 %	Map-Timeline
5	JS/Adware.Adport	▼	3.38 %	Map-Timeline
6	HTML/ScrInject	▼	3.33 %	Map-Timeline
7	Win32/Phorpiex	▼	2.99 %	Map-Timeline
8	JS/Adware.TerraClicks	▼	2.85 %	Map-Timeline
9	JS/RiskWare.Fingerprint	▼	2.75 %	Map-Timeline
10	JS/Packed.Agent.N	▼	2.7 %	Map-Timeline

Fuente: Virus Radar

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

kaspersky

Amenazas de tipo ransomware en Guatemala

IMPORTANTE

06OCT-12OCT2023 El mapa en tiempo real de ciberamenazas de KASPERSKY, evidenció que el software malicioso con mayor incidencia en Guatemala durante la semana fue el troyano Trojan-Ransom.MSIL.Blocker (25%) seguido de Trojan-Ranson.Win32.Crypmodng (21.43 %).

Principales troyanos de tipo ransomware en Guatemala (06OCT-12OCT2023)

1	Trojan-Ransom.MSIL.Blocker.gen	25%
2	Trojan-Ransom.Win32.Crypmodng.gen	21.43%
3	Trojan-Ransom.Win64.Magni.gen	14.29%
4	Trojan-Ransom.Win32.Crypren.afmu	7.14%
5	trojan-ransom.win32.Crypmod.gen	7.14%

Fuente: CYBERMAP

Ransomware a nivel global (06OCT-12OCT2023)

	MUNDO	
1	Guinea-Bisáu	8.86%
2	Turkmenistán	8.74%
3	Birmania	8.7%
4	Burundi	8.65%
5	Benín	8.64%
6	Afganistán	8.13%
7	Algeria	8.03%
8	Camerún	8.02%
9	Togo	7.99%
10	Kazajistán	7.93%
11	Ruanda	7.93%
12	Burkina Faso	7.68%
13	República del Congo	7.61%

Fuente: CYBERMAP

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

CONCIBER
Comité Nacional de Seguridad Cibernética

SPAMHAUS

Países con más incidencia de botnets

IMPORTANTE

06-12OCT2023 Según reporte semanal de SPAMHAUS, los países con más spam-bots a nivel mundial son: China, Estados Unidos e India. 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 (06OCT-12OCT2023)

1	China	Number of Bots: 671065
2	United States of America	Number of Bots: 547004
3	India	Number of Bots: 329375
4	Indonesia	Number of Bots: 174043
5	Venezuela (Bolivarian Republic of)	Number of Bots: 170004

Fuente: SPAMHAUS

Países con mayor índice de envió de spam en el mundo (06OCT-12OCT2023)

1	Porcelana	Número de problemas actuales de spam en vivo: 18778
2	Estados Unidos de América	Número de problemas actuales de spam en vivo: 6631
3	Arabia Saudita	Número de problemas actuales de spam en vivo: 830
4	México	Número de problemas actuales de spam en vivo: 815
5	Federación Rusa	Número de problemas actuales de spam en vivo: 767

Fuente: SPAMHAUS

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

.
.

	**Actor de amenazas con sede en la Franja de Gaza, vinculado a una serie de ataques cibernéticos dirigidos a organizadores israelíes.**	IMPORTANTE

10OCT2023 La Instituciones públicas y privadas israelíes están siendo objeto de una campaña de ataque cibernético bajo el nombre «Storm-1133» según indicó Microsoft en su Informe anual de defensa digital. Los ciberataques están siendo dirigidos a organizaciones de energía, defensa y telecomunicaciones del sector privado.

https://thehackernews.com/2023/10/gaza-linked-cyber-threat-actor-targets.html

Symantec by Broadcom	**Campaña cibernética Grayling APT**	IMPORTANTE

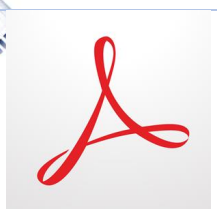
10OCT2023 Investigadores de ciberseguridad de Symantec Threat Hunter descubrieron la campaña de ataque cibernético bajo el nombre «Grayling APT» en diversas industrias. El grupo de APT está explotando cadenas de ataque que aprovechan la carga lateral de DLL a través de SbieDll_Hook para generar una variedad de cargas útiles, incluidas Cobalt Strike, NetSpy y el marco Havoc, junto con otras herramientas como Mimikatz

https://thehackernews.com/2023/10/researchers-uncover-grayling-apts.html

aws	**Vulnerabilidad Zero-Day en protocolo HTTP/2**	IMPORTANTE

10OCT2023 Vulnerabilidad CVE-2023-44487 de día cero (zero-day) en el protocolo HTTP/2 está siendo explotada para lanzar ataque distribuido de denegación de servicio - DDoS. Amazon Web Services (AWS), Cloudflare y Google Inc. están siendo objeto de ataques cibernéticos bajo el protocolo HTTP/2 que contiene una falla de día cero que puede explotarse para llevar a cabo ataques DDoS.

https://thehackernews.com/2023/10/http2-rapid-reset-zero-day.html

	**Agencia de Ciberseguridad de EE.UU. advirtió sobre vulnerabilidad activamente explotada en Adobe Acrobat Reader**	IMPORTANTE

11OCT2023 Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. –CISA- agregó una falla de gravedad en Adobe Acrobat Reader a su catálogo de vulnerabilidades explotadas conocidas (KEV), citando evidencia de explotación activa. Registrada como CVE-2023-21608 puntuación CVSS: 7.8, la vulnerabilidad se ha descrito como un error de uso después de la liberación que puede explotarse para lograr la ejecución remota de código (RCE) con los privilegios del usuario actual. Las versiones del software afectadas son: Acrobat DC: 22.003.20282 (Win), 22.003.20281 (Mac) y versiones anteriores; Acrobat Reader DC: 22.003.20282 (Win), 22.003.20281 (Mac) y versiones anteriores; Acrobat 2020 - 20.005.30418 y versiones anteriores; y Acrobat Reader 2020 - 20.005.30418 y versiones anteriores. Actualmente se desconocen los detalles sobre la naturaleza de la explotación y los actores de amenazas que pueden estar abusando de CVE-2023-21608.

https://thehackernews.com/2023/10/us-cybersecurity-agency-warns-of.html

	**Ataques dirigidos a gobiernos asiáticos y empresas de telecomunicaciones**	IMPORTANTE

12OCT2023 Entidades gubernamentales y de telecomunicaciones de alto perfil en Asia, han sido atacados como parte de una campaña en curso desde 2021 que está diseñada para implementar puertas traseras y entornos para la propagación de malware.

https://thehackernews.com/2023/10/researchers-uncover-ongoing.html