BOLETÍN INFORMATIVO 13-19OCT2023

CONCIBER

Comité Nacional de Seguridad Cibernética

Boletín de Ciberseguridad

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

13-19OCT2023 Según el reporte semanal de Virus Radar de ESET sobre el progreso y descenso de amenazas cibernéticas más aprovechadas por ciberdelincuentes en Guatemala, la amenaza con mayor incidencia fue HTML/Scrinject (8.38 %) seguida de SMB.Attack.Bruteforce (7.79 %).

Principales amenazas cibernéticas en Guatemala

	Threat Name	Change	Prevalence Level		
1	HTML/ScrInject	▲		8.38 %	Map-Timeline
2	SMB.Attack.Bruteforce	▲		7.79 %	Map-Timeline
3	RDP.Attack.Bruteforce	▲		3.94 %	Map-Timeline
4	JS/Packed.Agent.L	▲		3.77 %	Map-Timeline
5	JS/Packed.Agent.K	▲		3.34 %	Map-Timeline
6	JS/Adware.Adport	▼		3.21 %	Map-Timeline
7	Win32/Phorpiex	▲		2.81 %	Map-Timeline
8	JS/Adware.TerraClicks	▲		2.58 %	Map-Timeline
9	JS/Agent.RAW	▼		2.13 %	Map-Timeline
10	Android/Packed.TencentProtect.D	▼		2.08 %	Map-Timeline

Fuente: Virus Radar

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

kaspersky	Amenazas de tipo ransomware en Guatemala	IMPORTANTE

13-19OCT2023 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 (89.2%) seguido de Trojan-MSIL.PolyRansom.gen (3.76 %).

Principales troyanos de tipo ransomware en Guatemala

1	trojan-ransom.win32.Crypmodadv.gen	89.2%
2	Trojan-Ransom.MSIL.PolyRansom.gen	3.76%
3	Trojan-Ransom.Win64.Magni.gen	1.88%
4	trojan-ransom.win32.Crypren.gen	1.41%
5	trojan-ransom.win32.Blocker.vho	0.94%
6	Trojan-Ransom.Win32.Crypmodng.gen	0.94%
7	Trojan-Ransom.Win32.Stop.gen	0.47%
8	Trojan-Ransom.NSIS.MyxaH.gen	0.47%
9	Trojan-Ransom.Win32.PornoBlocker.ejtx	0.47%
10	Trojan-Ransom.Win32.Zerber.vho	0.47%

Fuente: CYBERMAP

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

SPAMHAUS	Países con más incidencia de botnets	IMPORTANTE

13-19OCT2023 Según reporte semanal de SPAMHAUS, los países con más spam-bots a nivel mundial son: China, Estados Unidos, 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

Fuente: SPAMHAUS

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

Instituciones públicas y privadas de Guatemala bajo Ciberataques

IMPORTANTE

14-18OCT2023 Instituciones públicas y privadas de Guatemala están siendo víctimas de ciberataques bajo la Operación #OpDemocracia promovida por el actor de amenazas «Anonymous Guatemala»,

https://devel.group/blog/continuan-los-ataques-hacia-sitios-publicos-y-gubernamentales-guatemaltecos/
https://twitter.com/hashtag/OpDemocracia?src=hashtag_click
https://twitter.com/AnonGTReloaded
https://twitter.com/YourAnonTl3x

Proveedores de telecomunicaciones ucranianos afectados por ciberataques

IMPORTANTE

16OCT2023 Equipo de Respuesta a Emergencias Informáticas de Ucrania (CERT-UA) informó que actores de amenazas interfirieron con al menos once (11) proveedores de servicios de telecomunicaciones en el país, bajo un reconocimiento y explotación de servicios vulnerables.

https://cert.gov.ua/article/6123309

Falso exploit de prueba de concepto (PoC) en WinRAR

IMPORTANTE

16OCT2023 Actor de amenazas difundió un falso exploit de prueba de concepto (PoC) para una vulnerabilidad en el software de compresión de datos WinRAR, con el objetivo de infectar a los usuarios con el malware VenomRAT. La PoC falsa es para la vulnerabilidad de ejecución de código arbitrario CVE-2023-40477, que puede desencadenarse cuando se abren archivos RAR especialmente diseñados en WinRAR antes de la versión 6.23.

https://www.theverge.com/2023/10/18/23922075/winrar-security-vulnerability-exploit-patch-update/
https://blog.google/threat-analysis-group/government-backed-actors-exploiting-winrar-vulnerability/
https://thehackernews.com/2023/10/pro-russian-hackers-exploiting-recent.html

The Hacker News	**Grupo de hackers pro-rusos aprovechó vulnerabilidad en WinRAR para desencadenar ciberataques**	**IMPORTANTE**

17OCT2023 Grupo de hackers pro-rusos explotó una vulnerabilidad de seguridad recientemente revelada en archivos WinRAR, como parte de una campaña de phishing diseñada para recolectar credenciales de sistemas comprometidos. El ataque implica el uso de archivos maliciosos que explotan la vulnerabilidad de forma remota.

https://thehackernews.com/2023/10/pro-russian-hackers-exploiting-recent.html

Microsoft	**Grupo de hackers norcoreanos aprovechó vulnerabilidad crítica en JetBrains TeamCity**	**IMPORTANTE**

18OCT2023 Microsoft informó que actores de amenazas norcoreanos están explotando activamente una falla de seguridad crítica en JetBrains TeamCity para violar servidores vulnerables. Los ataques, que implican la explotación de CVE-2023-42793 (puntuación CVSS: 9,8), se atribuyeron al actor de amenazas Diamond Sleet (Labyrinth Chollima) y Onyx Sleet (Andariel o Silent Chollima).

https://www.state.gov/digital-press-briefing-with-anne-neuberger-deputy-national-security-advisor-for-cyber-and-emerging-technologies/
https://thehackernews.com/2023/10/microsoft-warns-of-north-korean-attacks.html

CISCO	**Vulnerabilidad día cero en IOS XE CISCO**	**CRÍTICO (Puntuación CVSS de 10,09)**

18OCT2023 Vulnerabilidad día cero CVE-2023-20198 provoca fallas 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/warning-unpatched-cisco-zero-day.html
https://nvd.nist.gov/vuln/detail/CVE-2023-20198

CONCIBER
Comité Nacional de Seguridad Cibernética

Actores de amenazas de Rusia y China explotaron falla de seguridad en herramienta de archivo WinRAR para Windows

IMPORTANTE

19OCT2023 Google informó que varios actores de amenazas estatales de Rusia y China están explotando una falla de seguridad reciente en la herramienta de archivo WinRAR para Windows como parte de sus operaciones. La explotación exitosa de esta falla permite a los atacantes ejecutar código arbitrario cuando un usuario intenta ver un archivo benigno dentro de un archivo ZIP. Los ataques que implican la explotación de CVE-2023-42793 (puntuación CVSS: 9,8), se han atribuido al actor de amenazas Diamond Sleet (Labyrinth Chollima) y Onyx Sleet (Andariel o Silent Chollima).

https://thehackernews.com/2023/10/google-tag-detects-state-backed-threat.html
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/exploring-winrar-vulnerability-cve-2023-38831/