BOLETÍN INFORMATIVO 29SEP-05OCT2023

CONCIBER

Comité Nacional de Seguridad Cibernética

Boletín de Ciberseguridad

Amenazas cibernéticas en Guatemala

IMPORTANTE

29SEP-05OCT2023 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 (8.94 %) seguida de JS/Adware.Adport (4.79 %).

Principales amenazas cibernéticas en Guatemala

	Threat Name	Change	Prevalence Level	
1	SMB.Attack.Bruteforce	▲	8.94 %	Map-Timeline
2	JS/Adware.Adport	▼	4.79 %	Map-Timeline
3	HTML/ScrInject	▲	4.77 %	Map-Timeline
4	JS/Packed.Agent.L	▼	4.26 %	Map-Timeline
5	JS/Packed.Agent.K	▲	3.72 %	Map-Timeline
6	RDP.Attack.Bruteforce	▼	3.71 %	Map-Timeline
7	Win32/Phorpiex	▼	3.6 %	Map-Timeline
8	JS/Adware.TerraClicks	▲	3.09 %	Map-Timeline
9	JS/Packed.Agent.N	▲	2.24 %	Map-Timeline
10	JS/RiskWare.Fingerprint	▼	1.98 %	Map-Timeline

Fuente: Virus Radar

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

kaspersky

Amenazas de tipo ransomware en Guatemala

IMPORTANTE

29SEP-05OCT2023 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.Win32.Blocker (44.12%) seguido de SMB.Attack.Bruteforce (8.29 %).

Principales troyanos de tipo ransomware en Guatemala (29SEP-05OCT2023)

1	Trojan-Ransom.Win32.Blocker.gen	41.27%
2	Trojan-Ransom.MSIL.Blocker.gen	19.05%
3	trojan-ransom.win32.Crypmod.gen	17.46%
4	Trojan-Ransom.AndroidOS.Agent.bw	9.52%
5	Trojan-Ransom.Win32.PornoBlocker.ejtx	3.17%

Fuente: CYBERMAP

Ransomware a nivel global (29SEP-05OCT2023)

	MUNDO	
1	Afganistán	0.51%
2	Turkmenistán	0.43%
3	Yemen	0.36%
4	Papúa Nueva Guinea	0.35%
5	Irán	0.33%
6	Pakistán	0.29%
7	Bangladés	0.28%
8	Etiopía	0.24%
9	Túnez	0.2%
10	Siria	0.14%
11	Uruguay	0.14%
12	Egipto	0.13%
13	Bielorrusia	0.13%
14	Territorios Palestinos	0.13%
15	Corea del Sur	0.12%
16	México	0.12%
17	Irak	0.12%
18	Tailandia	0.11%
19	Vietnam	0.11%
20	Suazilandia	0.11%

Fuente: CYBERMAP

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

SPAMHAUS

Países con más incidencia de botnets

IMPORTANTE

29SEP-5OCT2023 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 (29SEP-05OCT2023)

1	China	Number of Bots: 651048
2	United States of America	Number of Bots: 580282
3	India	Number of Bots: 324778
4	Venezuela (Bolivarian Republic of)	Number of Bots: 190334
5	Indonesia	Number of Bots: 167813

Fuente: SPAMHAUS

Países con mayor índice de envió de spam en el mundo (29SEP-05OCT2023)

1	Porcelana	Número de problemas actuales de spam en vivo: 18755
2	Estados Unidos de América	Número de problemas actuales de spam en vivo: 6582
3	Arabia Saudita	Número de problemas actuales de spam en vivo: 830
4	México	Número de problemas actuales de spam en vivo: 814
5	India	Número de problemas actuales de spam en vivo: 758

Fuente: SPAMHAUS

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

	FBI advirtió sobre nueva tendencia de ataques duales de ransomware	IMPORTANTE

02OCT2023 La Oficina Federal de Investigaciones –FBI- advirtió sobre una nueva tendencia de ataques duales de ransomware dirigidas a empresas. Durante los ataques, los actores de amenazas cibernéticas implementaron dos variantes diferentes a las siguientes: AvosLocker, Diamond, Hive, Karakurt, LockBit, Quantum y Royal.

https://www.ic3.gov/Media/News/2023/230928.pdf
https://thehackernews.com/2023/09/fbi-warns-of-rising-trend-of-dual.html

	Casa Real británica sufre un ciberataque Ddos	IMPORTANTE

03OCT2023 La Casa Real británica fue víctima de un ciberataque que dejó inaccesible el servicio web de la institución. El ataque cibernético de tipo DDos (ataque distribuido de denegación de servicio) realizado por ciberdelincuentes dejaron inaccesible la disponibilidad de servicios tecnológicos.

https://cybersecuritynews.es/la-web-de-la-casa-real-britanica-sufre-un-ciberataque-ddos/

	Entidad gubernamental de Guyana fue afectada por ataque de ciberespionaje	IMPORTANTE

04OCT2023 Entidad gubernamental de Guyana fue atacada como parte de una campaña de ciberespionaje denominada «Operación Jacana». La firma eslovaca de ciberseguridad ESET, dijo que la intrusión podría estar vinculada a un adversario con nexos con China, debido al uso de PlugX (también conocido como Korplug), un troyano de acceso remoto utilizado por los equipos de hackers chinos.

https://thehackernews.com/2023/10/guyana-governmental-entity-hit-by.html

	Explotación activa de las vulnerabilidades de JetBrains y Windows	**IMPORTANTE**

04OCT2023 Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. –CISA- agregó dos fallas de seguridad (CVE-2023-42793, CVE-2023-28229) a su catálogo de vulnerabilidades conocidas (KEV) debido a una explotación activa, mientras que eliminó cinco errores de la lista debido a la falta de evidencia.

https://thehackernews.com/2023/10/cisa-warns-of-active-exploitation-of.html

	Apple lanzó parches de seguridad para la falla de día cero de iOS explotada activamente	**IMPORTANTE**

04OCT2023 Apple lanzó parches de seguridad para abordar una nueva falla de día cero en sistemas iOS y iPadOS, que ha sido explotada activamente por actores de amenazas.

https://support.apple.com/en-us/HT201222

	Cisco lanzó un parche urgente para corregir fallas críticas	**CRÍTICO (Puntuación CVSS de 9,8)**

05OCT2023 CISCO lanzó parches de seguridad (CVE-2023-20101) para corregir fallas críticas en los sistemas de respuesta a emergencias, que podrían propiciar que un atacante explote dicha vulnerabilidad utilizando la cuenta para iniciar sesión en un sistema afectado.

https://thehackernews.com/2023/10/cisco-releases-urgent-patch-to-fix.html