BOLETÍN INFORMATIVO 03-09NOV2023

CONCIBER

Comité Nacional de Seguridad Cibernética

Boletín de Ciberseguridad

Amenazas cibernéticas en Guatemala

IMPORTANTE

03-09NOV2023 Según el reporte semanal de Virus Radar de ESET sobre las ciberamenazas más utilizadas por ciberdelincuentes en Guatemala, permanece la amenaza SMB.Attack.Bruteforce (8.13 %) con mayor incidencia; seguida de RDP.Attack.Bruteforce (4.47 %).

Principales amenazas cibernéticas en Guatemala

	Threat Name	Change	Prevalence Level	
1	SMB.Attack.Bruteforce	▼	8.13 %	Map-Timeline
2	RDP.Attack.Bruteforce	▲	4.47 %	Map-Timeline
3	JS/Packed.Agent.L	▼	3.46 %	Map-Timeline
4	JS/Adware.Adport	▼	3.18 %	Map-Timeline
5	Win32/Phorpiex	▼	2.96 %	Map-Timeline
6	JS/Adware.TerraClicks	▼	2.76 %	Map-Timeline
7	JS/Packed.Agent.K	▼	2.46 %	Map-Timeline
8	DOC/Fraud	▲	2.31 %	Map-Timeline
9	HTML/ScrInject	▲	2.31 %	Map-Timeline
10	Android/Pandora	▲	2.2 %	Map-Timeline

Fuente: Virus Radar

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

kaspersky	**Amenazas de tipo ransomware en Guatemala**	**IMPORTANTE**

03-09NOV2023 El mapa en tiempo real de ciberamenazas de KASPERSKY mostró que en Guatemala el software malicioso con mayor incidencia durante la semana fue el troyano Trojan-Ransom.Win32.Blocker.wol (15.38 %); seguido de Trojan-Ransom.Win32.Zerber.vho (15.38 %).

Principales troyanos de tipo ransomware en Guatemala (03-09NOV2023)

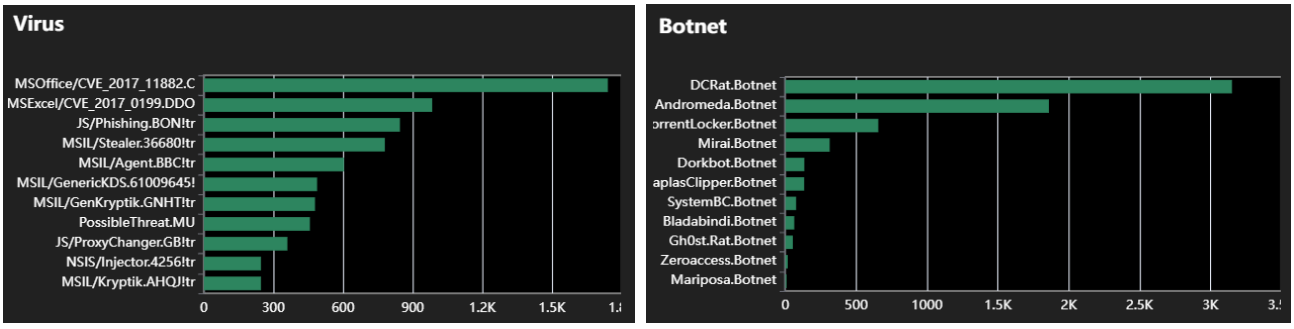
1	Trojan-Ransom.Win32.Blocker.wol	15.38%
2	Trojan-Ransom.Win32.Zerber.vho	15.38%
3	Trojan-Ransom.Win32.Blocker.gen	15.38%
4	Trojan-Ransom.Win32.Crypmodng_gen	15.38%
5	Trojan-Ransom.Win32.Blocker.pef	7.69%
6	Trojan-Ransom.MSIL.PolyRansom.gen	7.69%
7	Trojan-Ransom.Win64.Convagent.gen	7.69%
8	Trojan-Ransom.Win32.PornoBlocker.ejtx	7.69%
9	Trojan-Ransom.Win32.Blocker.zkcp	7.69%

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

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

03-09NOV2023 Principales amenazas cibernéticas en Guatemala, según reporte semanal de FORTIGUARD.

Principales amenazas cibernéticas en Guatemala (03-09NOV2023)



Fuente: FORTIGUARD

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

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

03-09NOV2023 Según reporte semanal de SPAMHAUS, los países con más spam-bots a nivel mundial son: China, EE.UU., India, Egipto y Venezuela. La mayoría de los bots detectados, fueron 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 (03-09NOV2023)

1	China	Number of Bots: 521484	6	Algeria	Number of Bots: 132335
2	United States of America	Number of Bots: 305530	7	Thailand	Number of Bots: 105972
3	India	Number of Bots: 294620	8	Brazil	Number of Bots: 92413
4	Egypt	Number of Bots: 236170	9	Pakistan	Number of Bots: 75162
5	Indonesia	Number of Bots: 170132	10	Viet Nam	Number of Bots: 66634

Fuente: SPAMHAUS

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

mac OS	**Nuevo malware para MacOS vinculado a hackers norcoreanos**	IMPORTANTE

03NOV2023 Grupo de hackers norcoreanos «Lazarus» utilizó nuevo malware (KandyKorn) para macOS y Windows para realizar sus ataques hacia una comunidad de blockchain. Según Elastic Security, KandyKorn es un implante avanzado con una variedad de capacidades para monitorear, interactuar y evitar la detección de los usuarios.

https://www.securityweek.com/north-korean-hackers-use-new-kandykorn-macos-malware-in-attacks/

QNAP®	**QNAP lanzó parche para abordar fallas críticas de su sistema operativo**	IMPORTANTE

06NOV2023 Empresa taiwanesa QNAP lanzó un parche de seguridad para abordar dos fallas críticas (CVE-2023-23368 y CVE-2023-23369) que afectaron su sistema operativo. Esto se produjo tras la eliminación de un servidor malicioso dirigido especialmente a dispositivos conectados a la red NAS expuestos a Internet.

https://thehackernews.com/2023/11/qnap-releases-patch-for-2-critical.html

Grupo cibernéticos atacaron a sectores tecnológicos en el Medio Oriente

IMPORTANTE

06NOV2023 Hackers iraníes «Agonizing Serpens» lanzaron ciberataques contra los sectores de tecnología y educación de Israel. Los ataques se caracterizan por el robo de datos confidenciales (identificación del personal y la propiedad intelectual) para posteriormente desplegar malware de limpieza para cubrir los registros de los atacantes e inutilizar los puntos infectados.

https://thehackernews.com/2023/11/iranian-hackers-launches-destructive.html

SideCopy aprovechó la vulnerabilidad de WinRAR para atacar entidades gubernamentales indias

IMPORTANTE

07NOV2023 El actor de amenazas SideCopy, vinculado a Pakistán, aprovechó la vulnerabilidad de seguridad de WinRAR para atacar a entidades gubernamentales de la India para enviar troyanos de acceso remoto (AllaKore RAT, Ares RAT y DRat). Además, los ataques también fueron diseñados para infiltrarse en sistemas Linux con una versión compatible de Ares RAT.

https://thehackernews.com/2023/11/sidecopy-exploiting-winrar-flaw-in.html

MARINA BAY Sands SINGAPORE

Marina Bay Sands reveló violación de datos de sus clientes

IMPORTANTE

08NOV2023 Marina Bay Sands, Singapur, reveló que alrededor de 665,000 de sus clientes se vieron afectados por una violación de datos, obteniendo acceso a información sensible (nombre, correo electrónico, número de teléfono, país y residencia). Además, si bien las contraseñas e información financiera no parecen haber sido comprometidas, el tipo de datos que quedaron expuestos en este incidente pueden ser útiles para ataques futuros de phishing dirigidos.

https://www.securityweek.com/marina-bay-sands-discloses-data-breach-impacting-665k-customers/

CISA CYBER+INFRASTRUCTURE	**Vulnerabilidad SLP de alta gravedad agregada por CISA**	**IMPORTANTE**

09NOV2023 La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE.UU., agregó una falla de alta gravedad en el Protocolo de ubicación de servicios SLP. Este problema se relaciona con una vulnerabilidad de denegación de servicio la cual se utilizaría como arma de ataques masivos de amplificación (DoS).

https://thehackernews.com/2023/11/cisa-alerts-high-severity-slp.html

gtd	**Ataque de ransomware al grupo GTD afectó organismos públicos y empresas de Chile y Perú**	**IMPORTANTE**

09NOV2023 Empresa de servicios tecnológicos GTD sufrió un ataque ransomware que afectó a la plataforma de Infraestructura como Servicio –IaaS-, por lo que se comprometieron los servicios de data center, telefonía, VPN y conexión a internet de más de 3,000 clientes en Chile y Perú. Sin embargo, la empresa decidió bajar sus IaaS para revisarlas de forma exhaustiva y evitar que se propague el software malicioso.
https://www.welivesecurity.com/es/ransomware/ransomware-afecta-grup-gtd-organismos-chile-peru/