BOLETÍN INFORMATIVO 22-28SEP2023

CONCIBER

Comité Nacional de Seguridad Cibernética

Boletín de Ciberseguridad

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

22-28SEP2023 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 JS/Agent.RAN (11.28 %) seguida de SMB.Attack.Bruteforce (8.29 %).

Principales amenazas cibernéticas en Guatemala

	Threat Name	Change	Prevalence Level	
1	JS/Agent.RAN	▼	11.28 %	Map-Timeline
2	SMB.Attack.Bruteforce	▼	8.29 %	Map-Timeline
3	RDP.Attack.Bruteforce	▼	4.77 %	Map-Timeline
4	JS/Adware.Adport	▼	4.77 %	Map-Timeline
5	HTML/ScrInject	▲	4.57 %	Map-Timeline
6	JS/Packed.Agent.L	▼	3.91 %	Map-Timeline
7	JS/Packed.Agent.K	▼	3.66 %	Map-Timeline
8	Win32/Phorpiex	▼	3.27 %	Map-Timeline
9	JS/Adware.TerraClicks	▼	2.7 %	Map-Timeline
10	Android/Packed.Jiagu.K	▼	2.08 %	Map-Timeline

Fuente: Virus Radar

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

kaspersky	Amenazas de tipo ransomware en Guatemala	IMPORTANTE

22-28SEP2023 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.Blocker (44.12%) seguido de SMB.Attack.Bruteforce (8.29 %).

Principales troyanos de tipo ransomware en Guatemala

1	Trojan-Ransom.Win32.Blocker.gen	44.12%
2	Trojan-Ransom.MSIL.Blocker.gen	35.29%
3	Trojan-Ransom.Win32.Zerber.vho	8.82%
4	Trojan-Ransom.Win32.Crypmodng.gen	4.41%
5	trojan-ransom.win32.Crypren.gen	2.94%
6	Trojan-Ransom.NSIS.MyxaH	1.47%
7	trojan-ransom.win32.Crypmod.gen	1.47%
8	Trojan-Ransom.Win32.PornoBlocker.ejtx	1.47%

Fuente: CYBERMAP

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

SPAMHAUS	Países con más incidencia de botnets	IMPORTANTE

22-28SEP2023 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

1	China	Number of Bots: 759665
2	United States of America	Number of Bots: 614375
3	India	Number of Bots: 241227
4	Venezuela (Bolivarian Republic of)	Number of Bots: 177430
5	Indonesia	Number of Bots: 108503

Fuente: SPAMHAUS

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

	**Servicios de Instituciones gubernamentales de Colombia afectados tras incidente de seguridad en IFX Networks S.A.S**	**IMPORTANTE**

22SEP2023 IFX Networks S.A.S., proveedor de servicios tecnológicos del Gobierno de Colombia, fue afectado tras un incidente de seguridad por infección del ransomware «MarioLocker» impactando en la disponibilidad, confidencialidad e integridad de los servicios de más de 50 instituciones públicas y privadas.

23SEP2023 Equipo de respuesta a Incidentes de seguridad de la información del Gobierno, emitió el informe correspondiente sobre el comportamiento y perpetración del ataque, concluyendo que el software malicioso polimórfico tiene unas variables de ejecución estrictas para asegurar su funcionamiento en hypervisores ESXI de VMWare.

https://www.colcert.gov.co/800/articles-280622_Documento_1.pdf

	**Evolución de botnet P2PInfect con variantes de malware más sigilosas**	**IMPORTANTE**

25SEP2023 Evolución de actividad del botnet P2PInfect conocido como un malware peer-to-peer (punto a punto) que viola instancias de Redis utilizando una falla de ejecución remota de código en sistemas Windows y Linux. Este gusano ha generado actividad a nivel global, afectando a sistemas en países como China, EE. UU., Alemania, Singapur, Hong Kong, Reino Unido y Japón.

https://www.bleepingcomputer.com/news/security/p2pinfect-botnet-activity-surges-600x-with-stealthier-malware-variants/

	**Falso exploit de prueba de concepto (PoC) en WinRAR**	**IMPORTANTE**

26SEP2023 Actor de amenazas difundió un falso exploit de prueba de concepto (PoC) para una vulnerabilidad en el software de compresión de datos WinRAR recientemente corregida en GitHub, 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.bleepingcomputer.com/news/security/fake-winrar-proof-of-concept-exploit-drops-venomrat-malware/

CONCIBER
Comité Nacional de Seguridad Cibernética

The Hacker News

Paquetes npm maliciosos amenazan las configuraciones de Kubernetes y claves SSH

IMPORTANTE

27SEP2023 Nuevo lote de códigos maliciosos en el registro de paquetes npm diseñados para filtrar configuraciones de Kubernetes y claves SSH de máquinas comprometidas a un servidor remoto, intentan hacerse pasar por bibliotecas y componentes de JavaScript, como los complementos de ESLint y las herramientas TypeScript SDK. Junto con la configuración de Kubernetes y las claves SSH, los módulos son capaces de recopilar metadatos del sistema, como nombre de usuario, dirección IP y nombre de host, los cuales se transmiten a un dominio llamado app.threatest[.]com.

https://thehackernews.com/2023/09/fresh-wave-of-malicious-npm-packages.html