BOLETÍN INFORMATIVO 10-16NOV2023

CONCIBER

Comité Nacional de Seguridad Cibernética

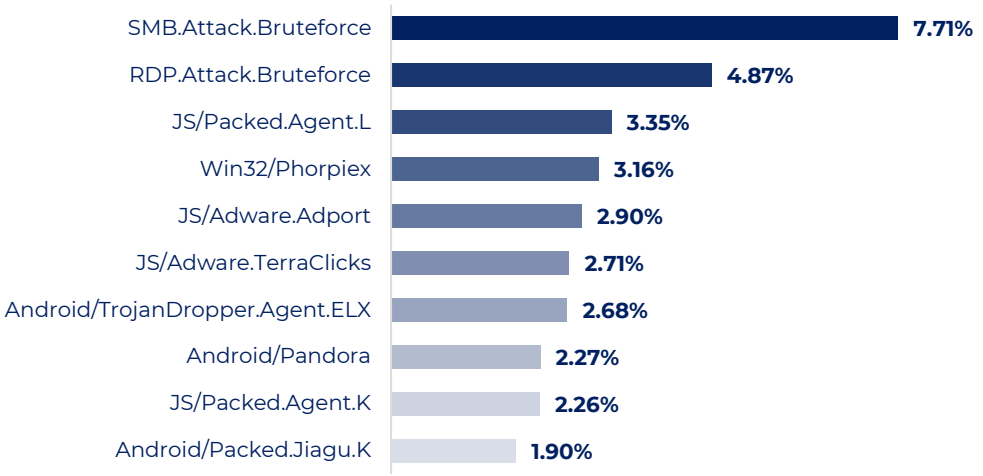
Boletín de Ciberseguridad

Amenazas cibernéticas en Guatemala

IMPORTANTE

10-16NOV2023 Según el reporte semanal de Virus Radar de ESET sobre las ciberamenazas más utilizadas por ciberdelincuentes en Guatemala, prevalece la amenaza SMB.Attack.Bruteforce (7.71 %) con mayor incidencia; seguida de RDP.Attack.Bruteforce (4.87 %).

Principales amenazas cibernéticas en Guatemala



Fuente: Virus Radar
https://virusradar.com/en/statistics/10

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

10-16NOV2023 El mapa de tiempo real que da seguimiento a las ciberamenazas de KASPERSKY, mostró que en Guatemala el software malicioso con mayor incidencia durante la semana fue Trojan-Ransom.Win32.Convagent.gen (42.11 %); seguido de Trojan-Ransom.Win32.Blocker.gen (15.79 %).

Principales troyanos de tipo ransomware en Guatemala

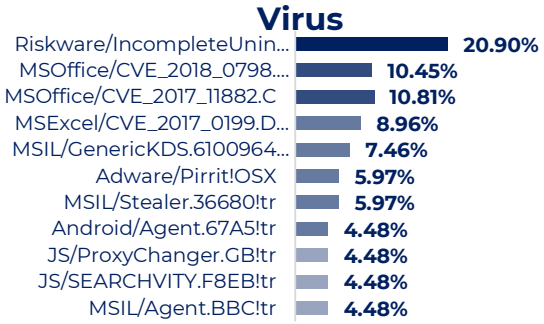
Ransomware	Frecuencia
Trojan-Ransom.Win32.Convagent.gen	42.11%
Trojan-Ransom.Win32.Blocker.gen	15.79%
Trojan-Ransom.BAT.Winlock.a	10.53%
Trojan-Ransom.MSIL.Blocker.gen	10.53%
Trojan-Ransom.JS.Alien.gen	5.26%
Trojan-Ransom.Win32.Blocker.pef	5.26%
Trojan-Ransom.win32.Blocker.vho	5.26%
Trojan-Ransom.MSIL.Mallox.gen	5.26%

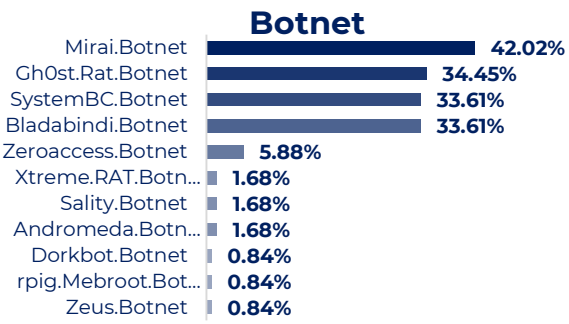
Fuente: CYBERMAP
https://cybermap.kaspersky.com/es/stats#country=38&type=RMW&period=w

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

10-16NOV2023 Principales amenazas cibernéticas en Guatemala, según reporte semanal de FORTIGUARD.

Principales amenazas





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

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

10-16NOV2023 Según reporte semanal de SPAMHAUS, los países con más spam-bots a nivel mundial son: China, EE.UU., India, Indonesia y Argelia. 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

Posición	País	Número de Bots
1	China	577,610
2	EE.UU.	356,780
3	India	249,926
4	Indonesia	169,774
5	Argelia	134,827
6	Tailandia	107,311
7	Egipto	88,488
8	Brasil	79,388
9	Rusia	71,361
10	Pakistán	69,581

Fuente: SPAMHAUS

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

	**Grupo cibernético atacó a sectores tecnológicos en el Medio Oriente**	IMPORTANTE

10NOV2023 Grupo vinculado a Irán, Imperial Kitten, atacó a los sectores tecnológicos (transporte, logística y tecnología) en Medio Oriente en OCT2023. Estas cadenas de ataques, aprovechan los sitios web comprometidos para perfilar a los visitantes mediante JavaScript y así, poder perfilar la información hacia los dominios controlados por los atacantes.

https://thehackernews.com/2023/11/iran-linked-imperial-kitten-cyber-group.html

DP WORLD	**Operador portuario australiano sufrió ataque cibernético**	IMPORTANTE

13NOV2023 DP World Australia, responsable de gestionar alrededor del 40 % del comercio exterior del país, sufrió un ataque cibernético que puso en riesgo la información de la portuaria, además de paralizar las operaciones de sus diferentes puertos (Sídney, Melbourne, Brisbane y Fremantle). El ataque se llevó a cabo el 10NOV2023, sin embargo, aún no se ha retornado al desarrollo normal de las actividades portuarias debido a dicho incidente.

https://www.infobae.com/tecno/2023/11/13/cual-fue-el-ciberataque-que-paralizo-las-operaciones-portuarias-de-australia/?utm_medium=Social&utm_source=Twitter#Echobox=1699894524

Windows	**Nuevo malware «BiBi-Windows» apunta a sistemas Windows en ataques pro-Hamás**	IMPORTANTE

13NOV2023 Investigadores de ciberseguridad advirtieron sobre un malware de limpieza «BiBi-Windows Wiper», utilizado por un grupo de hackers pro Hamás, que surgieron a raíz de la reactivación de la guerra entre Israel y Hamás en OCT2023. Este malware, además de dañar los archivos del sistema, evita que las víctimas recuperen los mismos.

https://thehackernews.com/2023/11/new-bibi-windows-wiper-targets-windows.html

Google	**Estafadores de Vietnam utilizan imagen de Google para robar credenciales**	IMPORTANTE

14NOV2023 Un grupo de estafadores de Vietnam utilizó la imagen de Google en anuncios y páginas fraudulentas para instar a las personas a descargar una nueva versión de su chatbot «Bard». Sin embargo, la descarga de esta versión falsa resulta en la instalación de un software malicioso diseñado para robar las credenciales de los perfiles en redes sociales.

https://cybersecuritynews.es/google-toma-medidas-legales-contra-estafadores-que-distribuyen-version-fraudulenta-de-su-chatbot-bard/

National Cyber Security Centre	**Intel publicó correcciones sobre la vulnerabilidad de su CPU**	IMPORTANTE

14NOV2023 Centro Nacional de Seguridad Cibernética del Reino Unido (NCSC, por sus siglas en inglés), destacó en su informe la importancia del resguardo de infraestructuras críticas (agua potable, electricidad, comunicaciones, sus redes de transporte y financieras y conectividad a Internet). Lo anterior, debido a que se ha observado el surgimiento de ciberadversarios, alineados con el Estado de Rusia, quienes simpatizan con una mayor invasión rusa en Ucrania y están motivados de forma ideológica más que financieramente.

https://www.ncsc.gov.uk/files/Annual_Review_2023.pdf
https://www.ncsc.gov.uk/news/ncsc-warns-enduring-significant-threat-to-uks-critical-infrastructure

intel	**Intel publicó correcciones sobre la vulnerabilidad de su CPU**	**IMPORTANTE**

15NOV2023 Intel publicó correcciones para solucionar una falla clasificada de gravedad «Reptar» que afectaba las CPU, móviles y servidores. Esta vulnerabilidad podría conducir potencialmente la divulgación de información, además de permitir una escalada de privilegios y/o denegación de servicios a través del acceso local.

https://thehackernews.com/2023/11/reptar-new-intel-cpu-vulnerability.html

zimbra	**Grupos de ciberdelincuentes explotaron una vulnerabilidad de Zimbra**	**IMPORTANTE**

16NOV2023 Cuatro grupos diferentes de ciberdelincuentes explotaron una vulnerabilidad de día cero en el software de correo electrónico (Zimbra Collaboration) para robar datos de credenciales de usuario y tokens de autenticación. La explotación exitosa de la vulnerabilidad podría permitir la ejecución de scripts maliciosos en el navegador web de las víctimas simplemente engañándolos para que hagan clic en una URL especialmente diseñada.

https://thehackernews.com/2023/11/zero-day-flaw-in-zimbra-email-software.html