BOLETÍN INFORMATIVO 15-21DIC2023

CONCIBER

Comité Nacional de Seguridad Cibernética

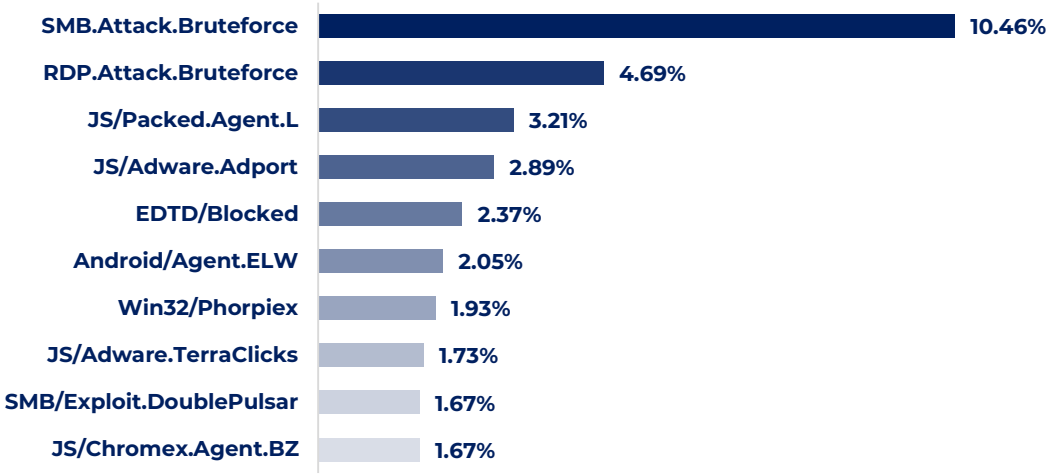
Boletín de Ciberseguridad

Amenazas cibernéticas en Guatemala

IMPORTANTE

15-21DIC2023 Según el reporte semanal de Virus Radar de ESET sobre las ciberamenazas más utilizadas por ciberdelincuentes en Guatemala, la amenaza SMB.Attack.Bruteforce (10.46 %) registró mayor incidencia; seguida de RPD/Attack.Bruteforce (4.69 %) y JS/Packed.Agent.L (3.21 %).

Principales amenazas cibernéticas en Guatemala



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

kaspersky	Amenazas de tipo ransomware en Guatemala	IMPORTANTE

15-21DIC2023 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.Crypmodadv.gen (95.24 %); seguido de Trojan-Ransom.Win32.Wanna.zbu (1.06 %).

Principales troyanos de tipo ransomware en Guatemala

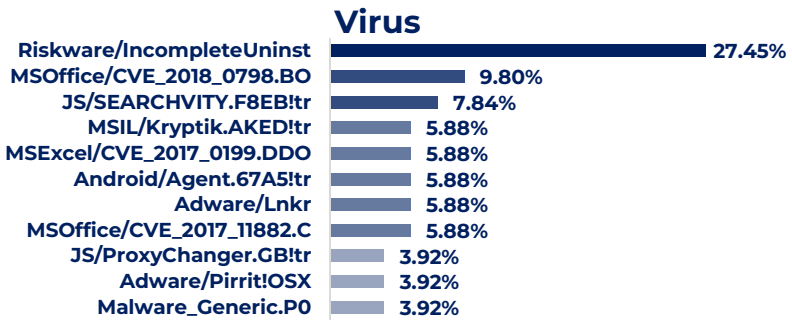
Ransomware	Frecuencia
trojan-ransom.win32.Crypmodadv.gen	95.24%
Trojan-Ransom.Win32.Wanna.zbu	1.06%
Trojan-Ransom.Win32.Phobos.vho	1.06%
trojan-ransom.win32.Crypren.gen	1.06%
Trojan-Ransom.Win32.PornoBlocker.ejtx	0.53%
Trojan-Ransom.Win32.Convagent.gen	0.53%
Trojan-Ransom.MSIL.Blocker.gen	0.53%

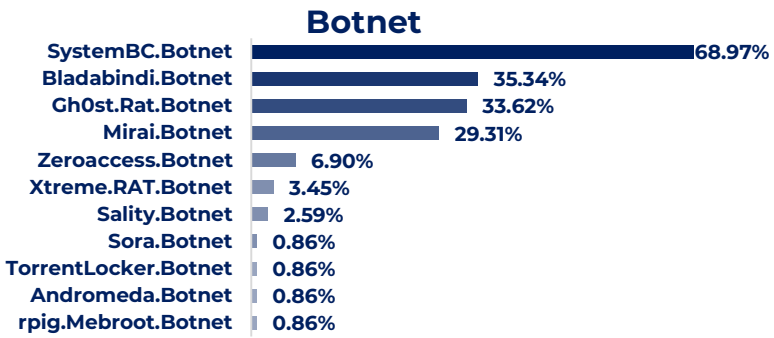
Fuente: CYBERMAP
https://cybermap.kaspersky.com/es/stats#country=38&type=RMW&period=w

FORTINET	Reporte de amenazas cibernéticas en Guatemala	IMPORTANTE

15-21DIC2023 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

15-21DIC2023 Según reporte semanal de SPAMHAUS, los países con más spam-bots a nivel mundial son: China, EE.UU., India, Indonesia y Algeria. 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	797,383
2	EE.UU.	344,057
3	India	306,425
4	Indonesia	174,701
5	Algeria	147,038
6	Tailandia	106,851
7	Brasil	93,275
8	Vietnam	78,394
9	Pakistán	72,032
10	Egipto	68,947

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

FORTINET	**Nuevo «KV-Botnet» dirigido a dispositivos Cisco, DrayTek y Fortinet en ataques sigilosos**	**IMPORTANTE**

15DIC2023 Un nuevo botnet «KV-Botnet» que consta de firewalls y enrutadores de Cisco, DrayTek, Fortinet y NETGEAR se está utilizando como una red encubierta de transferencia de datos para actores de amenazas persistentes avanzadas (APT). Este utiliza un malware que se propaga a través de vulnerabilidades en los dispositivos de red, el cual podría causar un impacto significativo en las organizaciones que son víctimas de los ataques de los APT (robo de datos confidenciales, interrupción de servicios o tomar el control de las redes).

https://thehackernews.com/2023/12/new-kv-botnet-targeting-cisco-draytek.html

pfsense	**Nuevas vulnerabilidades de seguridad descubiertas en software pfSense Firewall**	**ALTO (Puntuación CVSS: 8.8)**

15DIC2023 Vulnerabilidades de seguridad identificadas como CVE-2023-42325, CVE-2023-42327 y CVE-2023-42326 fueron descubiertas en solución de firewall, el cual un atacante podría encadenar para la ejecución de comandos arbitrarios de dispositivos susceptibles (espiar tráfico de red, atacar los servicios dentro de la red local y tomar el control de esta).

https://thehackernews.com/2023/12/iranian-hackers-using-muddyc2go-in-new.html

	Microsoft Edge identificó múltiples vulnerabilidades	**ALTO (Puntuación CVSS: 8.8)**

18DIC2023 Microsoft Edge identificó múltiples vulnerabilidades identificadas como CVE-2023-6702, CVE-2023-6703, CVE-2023-6704, CVE-2023-6705, CVE-2023-6706, CVE-2023-6707 y CVE-2023-36878. Un atacante podría aprovechar algunas de estas vulnerabilidades para desencadenar una condición de denegación de servicio, ejecución remota de código y elusión de restricciones de seguridad en el sistema objetivo.

https://www.hkcert.org/security-bulletin/microsoft-edge-multiple-vulnerabilities_20231218
https://msrc.microsoft.com/update-guide/vulnerability/

zimbra A SYNACOR PRODUCT	**Múltiples vulnerabilidades de Zimbra**	**IMPORTANTE**

19DIC2023 Zimbra identificó múltiples vulnerabilidades identificadas como CVE-2022-21449, CVE-2022-21476, CVE-2023-21930, CVE-2023-48432 y CVE-2023-50808, las cuales afectó a las tecnologías; Joule de colaboración de Zimbra antes del parche 8.8.15 45 GA, Colaboración Zimbra Kepler antes del parche 9.0.0 38 GA, Narciso de colaboración de Zimbra antes de 10.0.6. Un atacante podría aprovechar estas vulnerabilidades para activar secuencias de comandos entre sitios, eludir restricciones de seguridad, manipulación de datos y divulgación de información confidencial en el sistema objetivo.

https://www.hkcert.org/security-bulletin/zimbra-multiple-vulnerabilities_20231219
https://wiki.zimbra.com/wiki/Main_Page

	**Hackers iraníes realizaron ataques de espionaje de telecomunicaciones en África**	**IMPORTANTE**

19DIC2023 Grupo de ciberespionaje iraní, MuddyWater, utilizó un nuevo marco de comando y control (C2) «MuddyC2Go». MuddyC2Go es un ejecutable que viene equipado con un script PowerShell que se conecta automáticamente al servidor C2 de Seedworm, brindando así a los atacantes acceso remoto a un sistema víctima y obviando la necesidad de ejecución manual por parte de un operador.

https://thehackernews.com/2023/12/iranian-hackers-using-muddyc2go-in-new.html

	**Nuevo ataque de phishing roba códigos de respaldo de Instagram para evitar 2FA**	**IMPORTANTE**

20DIC2023 Nueva campaña de phishing pretende ser un correo electrónico de «infracción de derechos de autor» para el robo de códigos de seguridad de usuarios de Instagram. Si un atacante hurta los códigos de seguridad de un usuario, puede secuestrar su cuenta de Instagram, incluso si la autenticación de dos factores (2FA) está configurada.

https://www.bleepingcomputer.com/news/security/new-phishing-attack-steals-your-instagram-backup-codes-to-bypass-2fa/

CONCIBER
Comité Nacional de Seguridad Cibernética

	Nueva vulnerabilidad de ejecución remota de código de Google Chrome	**CRÍTICO (Puntuación CVSS: 10)**

21DIC2023 Google implementó actualizaciones de seguridad al navegador web Chrome, para abordar una falla crítica identificada como CVE-2023-7024, la cual afectó a las tecnologías; Google Chrome anterior a 120.0.6099.129 (Linux), Google Chrome anterior a 120.0.6099.129 (Mac) y Google Chrome anterior a 120.0.6099.129/130 (Windows). Un atacante podría aprovechar esta vulnerabilidad para desencadenar la ejecución remota de código en el sistema objetivo.

https://chromereleases.googleblog.com/2023/12/stable-channel-update-for-desktop_20.html
https://www.hkcert.org/security-bulletin/google-chrome-remote-code-execution-vulnerability_20231221