BOLETÍN INFORMATIVO 22-28DIC2023

CONCIBER

Comité Nacional de Seguridad Cibernética

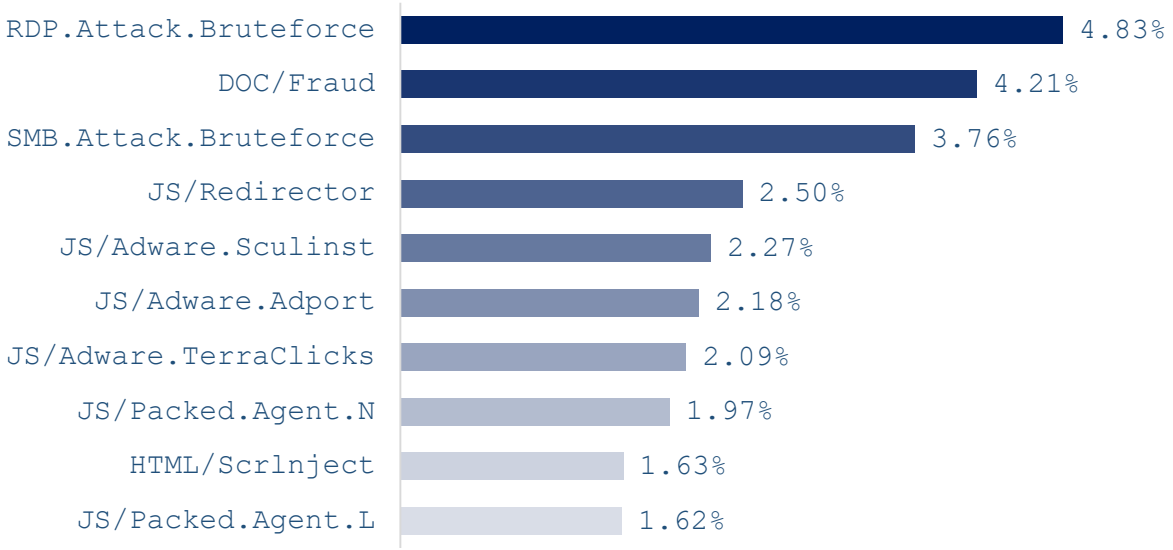
Boletín de Ciberseguridad

Amenazas cibernéticas en Guatemala

IMPORTANTE

22-28DIC2023 Según el reporte semanal de Virus Radar de ESET sobre las ciberamenazas más utilizadas por ciberdelincuentes en Guatemala, la amenaza RPD.Attack.Bruteforce registró mayor incidencia (4.83 %); seguida de DOC/Fraud (4.21 %).

Principales amenazas cibernéticas en Guatemala



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

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

22-28DIC2023 El mapa de 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.pef (25 %); seguido de Trojan-Ransom.MSIL.Blocker.gen (12.5 %).

Principales troyanos de tipo ransomware en Guatemala

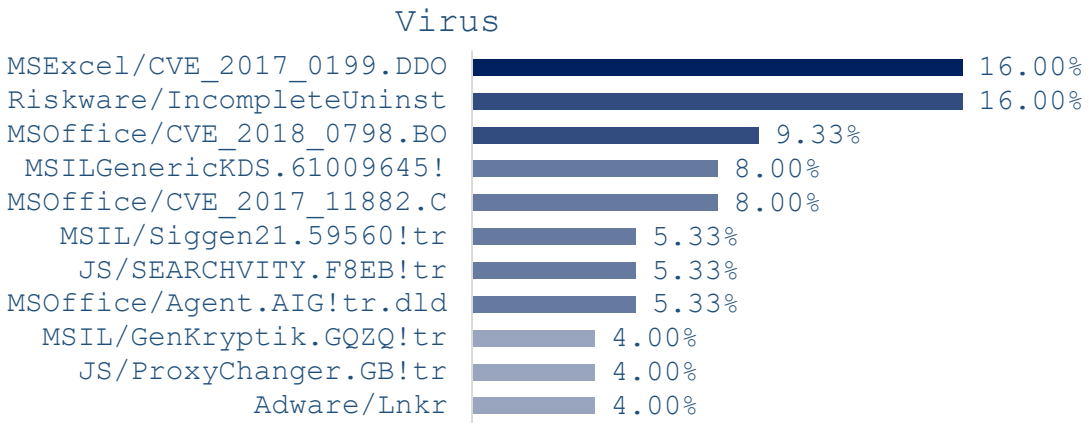
Ransomware	Frecuencia
Trojan-Ransom.Win32.Blocker.pef	25%
Trojan-Ransom.MSIL.Blocker.gen	12.5%
Trojan-Ransom.Win32.Blocker	12.5%
Trojan-Ransom.Win32.Stop.gen	12.5%
trojan-ransom.nsis.Onion.pef	12.5%
Trojan-Ransom.Win32.PornoBlocker.ejtx	12.5%
Trojan-Ransom.Win32.Locky.avt	12.5%

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

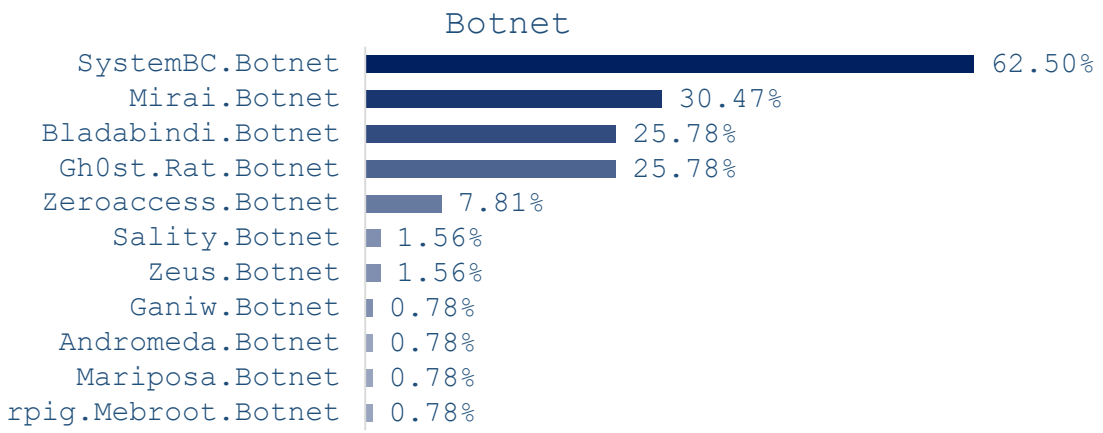
FORTINET	**Reporte de amenazas cibernéticas en Guatemala**	IMPORTANTE

22-28DIC2023 A continuación, se listan las principales amenazas cibernéticas en Guatemala, según reporte semanal de FORTIGUARD.

Principales amenazas



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



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

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

22-28DIC2023 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	741,172
2	EE.UU.	327,650
3	India	281,530
4	Indonesia	180,957
5	Argelia	154,877
6	Tailandia	108,745
7	Brasil	99,091
8	Egipto	73,287
9	Pakistán	72,112
10	Vietnam	71,216

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

	Vulnerabilidad afecta protocolo SSH	**CRÍTICO (Puntuación CVSS de 9.2)**

22DIC2023 OpenSSH emitió una alerta sobre la vulnerabilidad identificada como CVE-2023-48795, la cual afecta al protocolo de transporte SSH con ciertas extensiones en la versión anterior a la 9.6. Esta vulnerabilidad permite a un atacante remoto eludir las comprobaciones de integridad de modo que algunos paquetes se omiten y, en consecuencia, un cliente y un servidor pueden terminar con una conexión para la cual algunas características de seguridad han sido degradadas o deshabilitadas. Esto ocurre porque el protocolo de paquetes binarios (BPP) SSH implementado por estas extensiones, maneja mal la fase de protocolo de enlace y el uso de números de secuencia.

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-48795
https://www.hkcert.org/security-bulletin/openssh-security-restriction-bypass-vulnerability_20231219

	Vulnerabilidad afecta a los navegadores Microsoft Edge y Google Chrome	**ALTO (Puntuación CVSS: 8.3)**

22DIC2023 Microsoft Edge y Google Chrome, emitieron una alerta sobre la vulnerabilidad identificada como CVE-2023-7024, la cual provoca el desbordamiento de búfer en la función WebRTC. Esta vulnerabilidad permite a un atacante remoto explotar potencialmente la corrupción de dicha función a través de una página web HTML, diseñada para su efecto. Lo anterior puede desencadenar una condición de denegación de servicio, la ejecución remota de código y elusión de restricciones de seguridad en el sistema objetivo.

https://www.hkcert.org/security-bulletin/microsoft-edge-remote-code-execution-vulnerability_20231222
https://msrc.microsoft.com/update-guide/vulnerability/
https://nvd.nist.gov/vuln/detail/CVE-2023-7024

	Vulnerabilidad afecta a productos Apple	**CRÍTICO (Puntuación CVSS de 9.1)**

23DIC2023 Vulnerabilidad identificada como CVE-2023-42940, afecta a productos Apple. La falla identificada, provoca que un usuario que comparte su pantalla, puede compartir sin querer el contenido incorrecto, pudiendo aprovechar esta vulnerabilidad para desencadenar la divulgación y desinformación en el sistema objetivo.

https://www.hkcert.org/security-bulletin/apple-product-information-disclosure-vulnerability_20231221
https://support.apple.com/en-us/HT214048

	**Operación «RusticWeb»**	IMPORTANTE

23DIC023 Entidades gubernamentales y del sector de defensa de la república de la India, han sido objeto de una campaña de phishing, para distribuir malware desarrollado bajo el lenguaje de programación «Rust». A través de una nueva técnica, se han utilizado cargas útiles y comandos cifrados de PowerShell para filtrar documentos confidenciales en un motor de servicios web.

Recientemente, se han descubierto superposiciones tácticas entre el grupo y aquellos ampliamente rastreados bajo los apodos «Transparent Tribe y SideCopy», los cuales se considera que están vinculados a la República de Pakistán.

https://thehackernews.com/2023/12/operation-rusticweb-rust-based-malware.html
https://socradar.io/why-ransomware-groups-switch-to-rust-programming-language/#:~:text=Ransomware%20written%20in%20Rust%2C%20which,strains%20from%20Golang%20to%20Rust.

	**Vulnerabilidad en el plugin «Rogue» de Wordpress permite exponer sitios web de comercio electrónico**	IMPORTANTE

23DIC023 Wordpress emitió una alerta sobre una campaña dirigida a sitios web de comercio electrónico por actores de amenazas que están distribuyendo el plugin denominado «Rogue», el cual contiene código malicioso capaz de crear usuarios de tipo administrador falsos e inyectar código JavaScript malicioso para robar información de tarjetas de crédito.

https://thehackernews.com/2023/12/rogue-wordpress-plugin-exposes-e.html

	**Vulnerabilidad afecta a productos de ciberseguridad de ESET**	CRÍTICO (Puntuación CVSS de 9.2

27DIC2023 ESET fue informado sobre una vulnerabilidad identificada como CVE-2023-5594 que afecta a la función de escaneo del protocolo SSL/TLS, que se encuentra disponible en los productos de ESET. Esta vulnerabilidad hace que un navegador confíe en un sitio con un certificado firmado con un algoritmo obsoleto. La validación incorrecta de la cadena de certificados del servidor en la función de escaneo de tráfico seguro consideró que, el certificado intermedio firmado utilizando el algoritmo MD5 o SHA1 era confiable.

https://support.eset.com/en/ca8562-eset-customer-advisory-improper-following-of-a-certificates-chain-of-trust-in-eset-security-products-fixed
https://www.hkcert.org/security-bulletin/eset-products-security-restriction-bypass-execution-vulnerability_20231227