BOLETÍN INFORMATIVO 24-30NOV2023

CONCIBER

Comité Nacional de Seguridad Cibernética

CONCIBER
Comité Nacional de Seguridad Cibernética

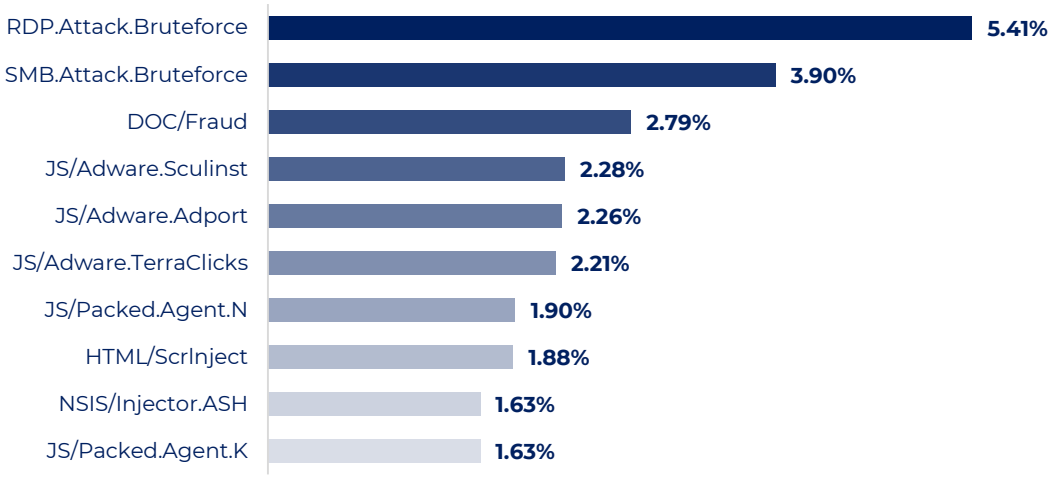
Boletín de Ciberseguridad

Amenazas cibernéticas en Guatemala

IMPORTANTE

24-30NOV2023 Según el reporte semanal de Virus Radar de ESET sobre las ciberamenazas más utilizadas por ciberdelincuentes en Guatemala, la amenaza RPD.Attack.Bruteforce (5.41 %) registró mayor incidencia; seguida de SMB.Attack.Bruteforce (3.90 %).

Principales amenazas cibernéticas en Guatemala



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

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

24-30NOV2023 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.Zerber.vho (31.25 %); seguido de Trojan-Ransom.Win32.Generic (6.25 %).

Principales troyanos de tipo ransomware en Guatemala

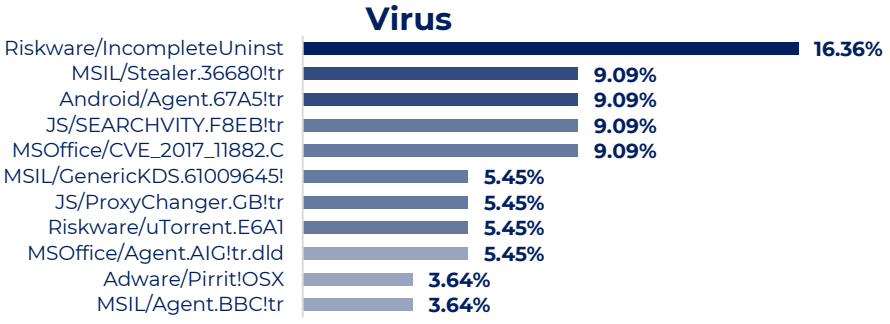
Ransomware	Frecuencia
Trojan-Ransom.Win32.Zerber.vho	31.25%
Trojan-Ransom.Win32.Generic	6.25%
Trojan-Ransom.Win32.Blocker.pef	6.25%
Trojan-Ransom.Win32.Phobos.vho	6.25%
Trojan-Ransom.Win32.Makop.vho	6.25%
Trojan-Ransom.Win32.Makop.a	6.25%
Trojan-Ransom.Win32.Crypmodng.gen	6.25%
Trojan-Ransom.MSIL.Blocker.gen	6.25%
Trojan-Ransom.Win32.PornoBlocker.ekqd	6.25%
Trojan-Ransom.Win32.Blocker.gen	6.25%

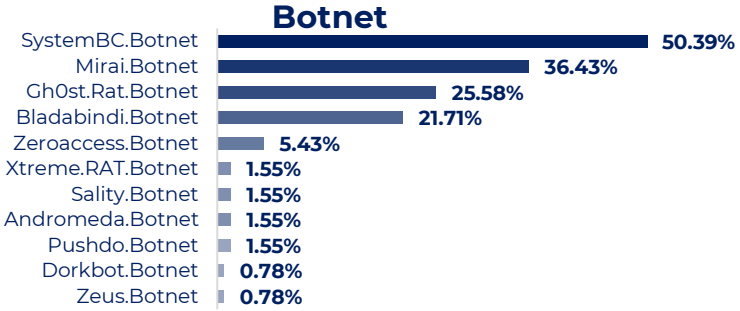
Fuente: CYBERMAP
https://cybermap.kaspersky.com/es/stats#country=38&type=RMW&period=w

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

24-30NOV2023 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

24-30NOV2023 Según reporte semanal de SPAMHAUS, los países con más spam-bots a nivel mundial son: China, EE.UU., India, Brasil e Indonesia. 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	666,668
2	EE.UU.	354,146
3	India	269,261
4	Brasil	188,449
5	Indonesia	169,782
6	Algeria	142,227
7	Tailandia	107,051
8	Rusia	82,363
9	Egipto	78,281
10	Pakistán	71,163

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

Nuevo shell web «HrServ» detectado en un ataque ATP hacia gobierno afgano

IMPORTANTE

25NOV2023 Entidad gubernamental de Afganistán fue atacada por el shell web «HrServ». Se cree que el ataque fue realizado por una amenaza persistente avanzada (APT). Hrserv.dll que exhibe características sofisticadas como métodos de codificación personalizados para la comunicación con el cliente y la ejecución en memoria. La intrusión permitió a los atacantes robar datos, monitorear el servidor y avanzar lateralmente dentro de la red.

https://thehackernews.com/2023/11/new-hrservdll-web-shell-detected-in-apt.html

OwnCloud advirtió sobre vulnerabilidades críticas que podrían revelar información confidencial y modificar archivos

CRÍTICO (Puntuación CVSS de 10)

25NOV2023 Los responsables del software de intercambio de archivos de código abierto ownCloud advirtieron sobre tres vulnerabilidades críticas (CVE-2023-49103, CVE-2023-49104 y CVE-2023-49105) que podrían explotarse para revelar información confidencial y modificar archivos. Las fallas podrían permitir a los atacantes robar información confidencial, como contraseñas y claves de licencia, modificar o eliminar archivos.
https://thehackernews.com/2023/11/warning-3-critical-vulnerabilities.html

Vulnerabilidad en la delegación de dominio de Google Workspace podría permitir a los atacantes escalar privilegios

IMPORTANTE

28NOV2023 Investigadores de ciberseguridad descubrieron una vulnerabilidad en la función de delegación de dominio (DWD) de Google Workspace la cual podría ser explotada por actores de amenazas para escalar privilegios y obtener acceso no autorizado a las API de Workspace. Dicha explotación podría resultar en el robo de correos electrónicos de Gmail, la filtración de datos de Google Drive u otras acciones no autorizadas.

https://hackernoon.com/es/el-equipo-de-cazadores-axon-descubre-un-defecto-de-diseno-que-podria-dejar-el-espacio-de-trabajo-de-google-vulnerable-para-la-adquisicion

Municipal Water Authority of Aliquippa	**CISA advirtió de un ataque cibernético a instalaciones de agua en EE.UU.**	**IMPORTANTE**

29NOV2023 Agencia de Seguridad de Infraestructura y Ciberseguridad de EE.UU. advirtió de un ciberataque que implicó la explotación de controladores lógicos programables (PLC) de Unitronics para atacar la Autoridad Municipal del Agua de Aliquippa, Pensilvania. El ataque se atribuyó a un colectivo hacktivista respaldado por Irán «Cyber Av3ngers». La autoridad desconectó el sistema y cambió a operaciones manuales en respuesta al ataque.

https://thehackernews.com/2023/11/iranian-hackers-exploit-plcs-in-attack.html

Google	**Google lanzó parches de seguridad para siete vulnerabilidades en Chrome**	**CRÍTICO (Puntuación CVSS de 9.6)**

29NOV2023 Google lanzó actualizaciones de seguridad para solucionar siete vulnerabilidades en su navegador Chrome, incluido un día cero que ha sido objeto de explotación activa. La vulnerabilidad «CVE-2023-6345» es un error de desbordamiento de enteros en Skia, una biblioteca de gráficos 2D de código abierto, permitiendo a los atacantes adquirir información confidencial, instalar malware y tomar control de los sistemas de usuarios.

https://thehackernews.com/2023/11/zero-day-alert-google-chrome-under.html

APACHE ACTIVEMQ	**GoTitan explotó reciente vulnerabilidad de Apache ActiveMQ**	**CRÍTICO (Puntuación CVSS de 10)**

29NOV2023 La vulnerabilidad de ejecución remota de código CVE-2023-46604 está siendo explotada activamente por Botnet GoTitan para distribuir una variedad de malware (botnets, cryptojackers y troyanos de acceso remoto). Los ataques implican la explotación de la falla para inyectar código malicioso en un servidor Apache ActiveMQ vulnerable. Una vez que el código malicioso se ha inyectado, los atacantes pueden ejecutar comandos arbitrarios en el sistema afectado.

https://thehackernews.com/2023/11/gotitan-botnet-spotted-exploiting.html