BOLETÍN INFORMATIVO 16-22FEB2024

CONCIBER

Comité Nacional de Seguridad Cibernética

Boletín de Ciberseguridad

CONCIBER
Comité Nacional de Seguridad Cibernética

FORTINET

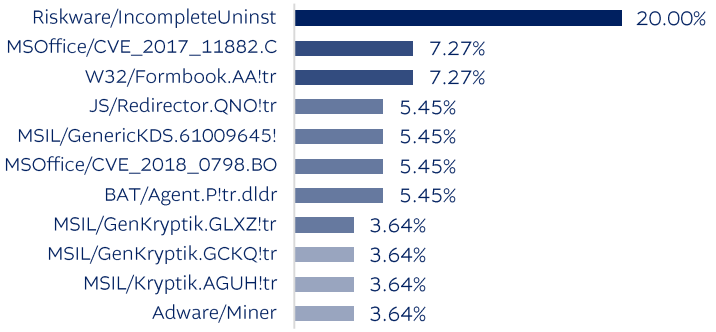
Reporte de amenazas cibernéticas en Guatemala

IMPORTANTE

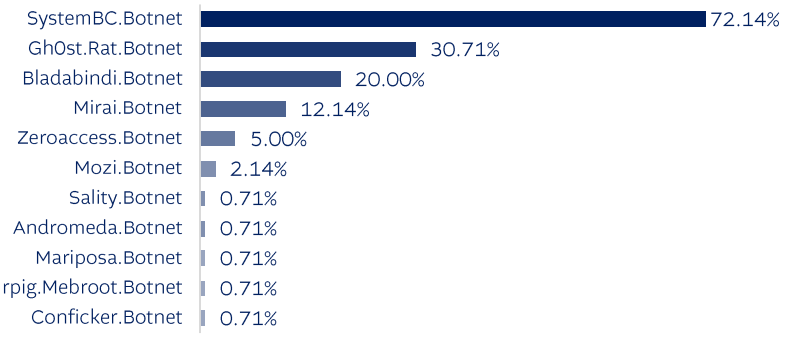
16-22FEB2024 Principales amenazas cibernéticas en Guatemala, según reporte semanal de FORTIGUARD.

Principales amenazas

Virus



Botnet



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

kaspersky	**Amenazas de tipo ransomware**	IMPORTANTE

16-22FEB2024 El mapa en tiempo real de ciberamenazas de KASPERSKY, registró el flujo de detección de malware mediante «On-Acces Scan», un escaneo activo y continuo para proteger el sistema contra posibles amenazas en tiempo real mientras se llevan a cabo diferentes operaciones, específicamente cuando los archivos o programas son abiertos, copiados, ejecutados o guardados en el sistema.

Principales troyanos escaneados en tiempo real a nivel mundial

Troyanos	Frecuencia
Trojan.Win32.Astaroth.gen	15.71%
DangerousObject.Multi.Generic	8.21%
Virus.Win32.Pioneer.cz	5.00%
Trojan.Win32.Agent.ifdx	4.29%
Virus.Win32.Renamer.j	3.93%
Email-Worm.Win32.Brontok.q	3.93%
Trojan.Win32.Khalesi.gen	3.57%

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

CLOUDFLARE	**Porcentaje de tráfico de bots a nivel mundial**	IMPORTANTE

16-22FEB2024 Según el reporte semanal del radar de CloudFlare, el mayor porcentaje de tráfico de bots se registró en Irán (95.56 %) seguido de Guinea (74.36 %), Singapur (67.15 %) y Seychelles (66.58 %).

Principales países con mayor porcentaje de tráfico de bots

Posición	País	Tráfico de bots
1	Irán	95.56%
2	Guinea	74.36%
3	Singapur	67.15%
4	Seychelles	66.58%
5	Islas Vírgenes	66.50%

Fuente: CloudFlare.
https://radar.cloudflare.com/traffic

CONCIBER
Comité Nacional de Seguridad Cibernética

SPAMHAUS

ISPs con mayor número de spam-bots detectados

IMPORTANTE

16-22FEB2024 Según reporte semanal de SPAMHAUS, los proveedores de servicios de internet –ISP- que poseen el mayor número de spam-bots son; charter.com, chinanet-js, Microsoft.com y chinanet-zj. La mayoría de los bots se pueden utilizar para spam, phishing, fraude de clics, DDoS y otras actividades maliciosas.

ISP más vulnerables a spam-bots a nivel mundial

Posición	País	Número de Bots
1	charter.com	184,727
2	Microsoft.com	149,760
3	Chinanet-js	107,343
4	Verizon.com	64,436
5	Chinanet-zj	64,178
6	Unicom-ln	62,558
7	Chinanet-ah	55,879
8	Virginmedia.com	47,560
9	Airtel.in	46,795
10	Bt.com	43,660

Fuente: SPAMHAUS.
https://www.spamhaus.com/threat-map/

Panorama de amenazas cibernéticas y vulnerabilidades
AMENAZAS

Schneider Electric	**Ransomware «Cactus» afirmó robar 1.5 TB de datos de Schneider Electric**	IMPORTANTE

19FEB2024 Grupo de ransomware «Cactus» afirmó robar 1.5 TB de datos de Schneider Electric después de infiltrar su red en ENE2024. Además, se filtraron 25 MB de datos como prueba en un sitio de la web oscura (incluyendo pasaportes y documentos de acuerdos de confidencialidad). «Cactus ransomware», una operación relativamente nueva, utiliza diversos métodos para infiltrarse en redes corporativas y robar datos confidenciales que luego utilizan en las negociaciones de rescate.

https://www.bleepingcomputer.com/news/security/cactus-ransomware-claim-to-steal-15tb-of-schneider-electric-data/

PSI	**PSI Software SE confirmó ataque de ransomware en su infraestructura interna**	IMPORTANTE

20FEB2024 Desarrollador de software alemán especializado en soluciones para proveedores de energía, PSI Software SE, sufrió un ataque de ransomware que afectó su infraestructura interna. La empresa, con una plantilla global de más de 2,000 personas, anunció que desconectó varios sistemas informáticos. Aunque aún no se ha determinado el vector exacto de intrusión, la empresa afirmó que no hay evidencia de que los sistemas de los clientes hayan sido comprometidos. Sin embargo, PSI Software está colaborando con las autoridades y recibiendo asistencia de expertos en seguridad desde el 16FEB2024 para responder y remediar el incidente.

https://www.bleepingcomputer.com/news/security/critical-infrastructure-software-maker-confirms-ransomware-attack/

LOCKBIT 3.0	**«LockBit» interrumpido por operación policial global**	IMPORTANTE

20FEB2024 La Agencia Nacional contra el Crimen del Reino Unido –NCA- logró obtener el código fuente de LockBit y una considerable cantidad de información de inteligencia relacionada con sus actividades como parte de la Operación Cronos. La NCA también anunció el arresto de dos individuos asociados con LockBit en Polonia y Ucrania, junto con el congelamiento de más de 200 cuentas de criptomonedas relacionadas con el grupo.

https://thehackernews.com/2024/02/lockbit-ransomware-operation-shut-down.html

Google Cloud Run	**Advertencia sobre el abuso de Google Cloud Run para distribuir malware bancario**	IMPORTANTE

21FEB2024 Investigadores de seguridad detectaron un aumento significativo en el abuso del servicio Google Cloud Run para la distribución masiva de troyanos bancarios «Astaroth, Mekotio y Ousaban». Google Cloud Run, que permite la implementación de servicios y aplicaciones sin la necesidad de administrar infraestructuras, es explotado por ciberdelincuentes brasileños desde SEP2023. Los ataques comienzan con correos electrónicos de phishing en español o italiano, diseñados para parecer legítimos y dirigidos a víctimas potenciales principalmente en América Latina.

https://www.bleepingcomputer.com/news/security/200-000-facebook-marketplace-user-records-leaked-on-hacking-forum/

VULNERABILIDADES

Exchange	**Exploit de alto riesgo afectó a Microsoft Exchange Server**	CRÍTICO (Puntuación CVSS: 9.8)

16FEB2024 Se detectó el exploit «CVE-2024-21410» que afecta a Microsoft Exchange Server el cual podría explotarse enviando una solicitud diseñada para robar el hash NTLM del usuario, causando una ejecución remota de código, denegación de servicios, omisiones de restricción de seguridad y suplantación de identidad.

https://www.hkcert.org/security-bulletin/microsoft-monthly-security-update-february-2024

chrome OS	**ChromeOS identificó múltiples vulnerabilidades**	ALTO (Puntuación CVSS: 7.8)

19FEB2024 ChromeOS identificó múltiples vulnerabilidades; CVE-2023-6817, CVE-2023-6931, CVE-2023-6932, CVE-2023-46813, CVE-2023-51042, CVE-2024-0807 y CVE-2024-0808 que podría afectar la versión anterior a 114.0.5735.351 (Versión de plataforma: 15437.91.0). Un atacante remoto podría aprovechar algunas de estas para desencadenar una condición de denegación de servicio y la ejecución remota de código.

https://chromereleases.googleblog.com/2024/02/long-term-support-channel-update-for_16.html
https://www.hkcert.org/security-bulletin/chromeos-multiple-vulnerabilities_20240219

Google	**Múltiples vulnerabilidades de Google Chrome**	**ALTO (Puntuación CVSS: 8.8)**

21FEB2024 Google Chrome identificó múltiples vulnerabilidades en sus sistemas las cuales se registraron como CVE-2024-1669, CVE-2024-1670, CVE-2024-1671, CVE-2024-1672, CVE-2024-1673, CVE-2024-1674, CVE-2024-1675 y CVE-2024-1676 las cuales podrían afectar a las versiones Google Chrome anterior a 122.0.6261.57 (Linux), anterior a 122.0.6261.57 (Mac) y anterior a 122.0.6261.57/.58 (Windows). Un atacante remoto podría aprovechar algunas de estas para desencadenar la divulgación de información, la elusión de restricciones de seguridad, la ejecución remota de código y la condición de denegación de servicio en el sistema objetivo.

https://www.hkcert.org/security-bulletin/google-chrome-multiple-vulnerabilities_20240221
https://chromereleases.googleblog.com/2024/02/stable-channel-update-for-desktop_20.html

	**Múltiples vulnerabilidades en productos Mozilla**	**MEDIO (Puntuación CVSS: 5.8)**

22FEB2024 Se identificaron múltiples vulnerabilidades en productos Mozilla, las cuales se identifican como; CVE-2024-1546, CVE-2024-1547, CVE-2024-1548, CVE-2024-1549, CVE-2024-1550, CVE-2024-1551, CVE-2024-1552, CVE-2024-1553, CVE-2024-1554, CVE-2024-1555, CVE-2024-1556 y CVE-2024-1557. Dichas fallas afectan las versiones FirefoxESR 115.8, Firefox 123 y Pájaro del trueno 115.8. Un atacante remoto puede aprovechar algunas de estas para desencadenar una condición de denegación de servicio, suplantación de identidad, ejecución remota de código, elevación de privilegios y elusión de restricciones de seguridad.

https://www.hkcert.org/security-bulletin/mozilla-products-multiple-vulnerabilities_20240222