BOLETÍN INFORMATIVO 26OCT-02NOV2023

# CONCIBER

Comité Nacional de Seguridad Cibernética

CONCIBER
Comité Nacional de Seguridad Cibernética

# Boletín de Ciberseguridad

## Amenazas cibernéticas en Guatemala

IMPORTANTE

27OCT-02NOV2023 Según el reporte semanal de Virus Radar de ESET sobre las ciberamenazas más utilizadas por ciberdelincuentes en Guatemala, la amenaza con mayor incidencia fue SMB.Attack.Bruteforce (8.64 %); seguida de SMB.Attack.Bruteforce HTML/ScrInject (5.54 %).

### Principales amenazas cibernéticas en Guatemala

| | Threat Name | Change | Prevalence Level |
|---|---|---|---|
| 1 | SMB.Attack.Bruteforce | ▲ | 8.64 % |
| 2 | HTML/ScrInject | ▲ | 5.54 % |
| 3 | JS/Packed.Agent.K | ▲ | 4.46 % |
| 4 | JS/Packed.Agent.L | ▲ | 3.99 % |
| 5 | RDP.Attack.Bruteforce | ▲ | 3.79 % |
| 6 | JS/Adware.TerraClicks | ▲ | 3.24 % |
| 7 | JS/Adware.Adport | ▼ | 3.16 % |
| 8 | Win32/Phorpiex | ▼ | 3.04 % |
| 9 | Android/Packed.TencentProtect.D | ▼ | 2.06 % |
| 10 | Android/Pandora | ▲ | 2.02 % |

Fuente: Virus Radar

https://virusradar.com/en/statistics/10

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

27OCT-02NOV2023 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.Crypmodady.gen (87.34%); seguido de Trojan-Ransom.Win64.Convagent.gen (6.28%).

### Principales troyanos de tipo ransomware en Guatemala

| | | |
|---|---|---|
| 1 | trojan-ransom.win32.Crypmodadv.gen | 87.43% |
| 2 | Trojan-Ransom.Win64.Convagent.gen | 6.28% |
| 3 | Trojan-Ransom.Win32.Blocker.gen | 2.09% |
| 4 | trojan-ransom.win32.Crypren.gen | 1.05% |
| 5 | Trojan-Ransom.Win32.Blocker.pef | 1.05% |
| 6 | trojan-ransom.win32.Agent.vho | 1.05% |
| 7 | Trojan-Ransom.NSIS.MyxaH.gen | 0.52% |
| 8 | Trojan-Ransom.Win32.Cryptor.fsb | 0.52% |

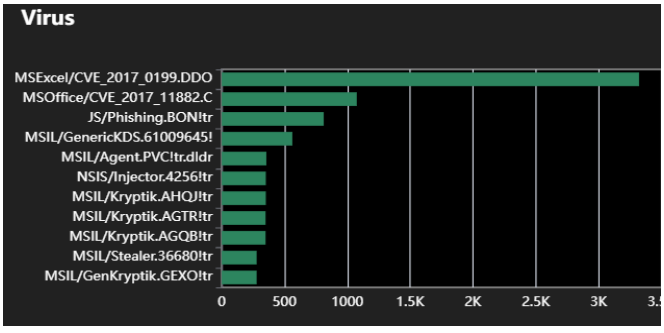
Fuente: CYBERMAP

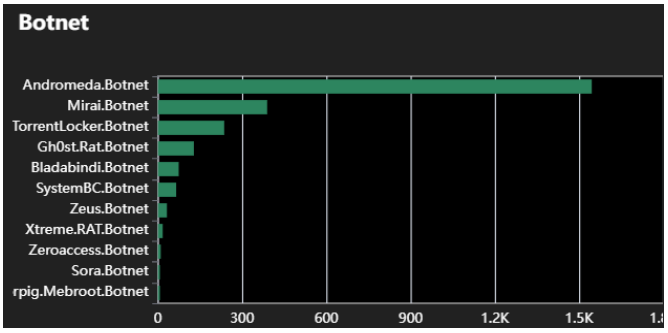
https://cybermap.kaspersky.com/es/stats#country=38&type=RMW&period=w

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

27OCT-02NOV2023 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 |
|---|---|---|

27OCT-02NOV2023 Según reporte semanal de SPAMHAUS, los países con más spam-bots a nivel mundial son: China, Estados Unidos, India, Egipto y Venezuela. 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**

| | | | | | |
|---|---|---|---|---|---|
| 1 | China | Number of Bots: 440001 | 6 | Indonesia | Number of Bots: 168716 |
| 2 | United States of America | Number of Bots: 378771 | 7 | Algeria | Number of Bots: 131783 |
| 3 | India | Number of Bots: 280595 | 8 | Brazil | Number of Bots: 106515 |
| 4 | Egypt | Number of Bots: 243979 | 9 | Thailand | Number of Bots: 102621 |
| 5 | Venezuela (Bolivarian Republic of) | Number of Bots: 172277 | 10 | United Kingdom of Great Britain and Northern Ireland | Number of Bots: 80302 |

Fuente: SPAMHAUS

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

| Microsoft | Actores de amenazas incrementaron actividad maliciosa | IMPORTANTE |
|---|---|---|

27OCT2023

- Microsoft emitió una advertencia sobre la actividad maliciosa realizada por el actor de amenazas bajo el alias «Scattered Spider», el cual ejecuta ataques a proveedores de servicios de telecomunicaciones con fines financieros.

  https://thehackernews.com/2023/10/microsoft-warns-as-scattered-spider.html

- Microsoft formuló un comunicado para informar sobre actores de amenazas que utilizan paquetes de aplicaciones MSIX de Windows para el software popular como Google Chrome, Microsoft Edge, Brave, Grammarly y Cisco Webex para distribuir un cargador de malware denominado «GHOSTPULSE».

  https://learn.microsoft.com/en-us/windows/msix/overview
  https://thehackernews.com/2023/10/hackers-using-msix-app-packages-to.html

| | | |
|---|---|---|
| kaspersky | **Actor de amenazas «Lazarus Group» incrementó su actividad maliciosa** | **IMPORTANTE** |

28OCT2023 kaspersy dio a conocer que un grupo de ciberdelincuentes aliado a Corea del Norte, está detrás de una nueva campaña de ciberataques mediante la explotación de fallas de seguridad conocidas.

https://thehackernews.com/2023/10/lazarus-group-targeting-defense-experts.html
https://securelist.com/apt-trends-report-q3-2023/110752/

| | | |
|---|---|---|
| CISCO | **Vulnerabilidad zero day en IOS XE CISCO** | **CRÍTICO (Puntuación CVSS de 10)** |

30OCT2023 Cisco presentó un comunicado para informar a sus consumidores sobre el incremento de actividad maliciosa por parte de actores de amenazas que se encuentran explotando activamente la vulnerabilidad zero day «CVE-2023-20198», que permite escalar privilegios en la función de interfaz de usuario web, permitiendo a un atacante remoto y no autenticado, crear una cuenta en un sistema afectado con acceso de nivel de privilegio.

https://thehackernews.com/2023/10/cisco-zero-day-exploited-to-implant.html
https://nvd.nist.gov/vuln/detail/CVE-2023-20198

| | | |
|---|---|---|
|  | **Canadá prohibió uso de aplicaciones WeChat y Kaspersky en dispositivos gubernamentales** | **IMPORTANTE** |

31OCT2023 Gobierno de Canadá emitió un comunicado para que se restringir el uso de WeChat y Kaspersky en dispositivos móviles de uso gubernamental, debido a que brindan un acceso considerable a la información almacenada en los dispositivos.

https://thehackernews.com/2023/10/canada-bans-wechat-and-kaspersky-apps.html

| | | |
|---|---|---|
| Google | **Campaña de phishing a través de la herramienta Google Ads** | **IMPORTANTE** |

31OCT2023 Actor de amenazas utiliza sitios web pirateados para distribuir versión troyanizada del software de desarrollo de aplicaciones PyCharm, a través de anuncios generados dinámicamente por la herramienta Google ADS.

https://www.malwarebytes.com/blog/threat-intelligence/2023/10/malvertising-via-dynamic-search-ads-delivers-malware-bonanza

| | | |
|---|---|---|
|  | **Grupo iraní de ciberespionaje apunta a sectores financieros y gubernamentales en Medio Oriente** | **IMPORTANTE** |

01NOV2023 Check Point, empresa israelí de ciberseguridad, emitió un comunicado para informar a sus clientes de medio oriente sobre la campaña de ciberespionaje realizada por el actor de amenazas «Scarred Manticore». Este actor es uno de los cuatro grupos iraníes vinculados a ataques destructivos en contra del Gobierno Albanés, realizados durante el 2022.

https://thehackernews.com/2023/11/hellokitty-ransomware-group-exploiting.html
https://www.rapid7.com/blog/post/2023/11/01/etr-suspected-exploitation-of-apache-activemq-cve-2023-46604/
https://nvd.nist.gov/vuln/detail/CVE-2023-46604

| | | |
|---|---|---|
| The Hacker News | **Actor de amenazas explota activamente la falla de seguridad crítica en el servicio de Apache ActiveMQ** | **IMPORTANTE** |

02NOV2023 Rapid7 informó que actor de amenazas se encuentra explotando la vulnerabilidad «CVE-2023-46604» que afecta al servicio de Apache ActiveMQ, lo que permite a un atacante la ejecución remota de código arbitrario. La falla faculta a un agresor remoto con acceso a la red ejecutar comandos shell arbitrarios manipulando tipos de clases en el protocolo OpenWire

https://thehackernews.com/2023/11/hellokitty-ransomware-group-exploiting.html
https://www.rapid7.com/blog/post/2023/11/01/etr-suspected-exploitation-of-apache-activemq-cve-2023-46604/
https://nvd.nist.gov/vuln/detail/CVE-2023-46604