CIBER E-DEA

Boletín de Seguridad

X (Twitter) golpeado por un ciberataque masivo

Ragnar Loader: La Herramienta de Acceso Persistente en Operaciones de Ransomware

CPU RISC-V de Alibaba y la autosuficiencia de china tecnológicamente.

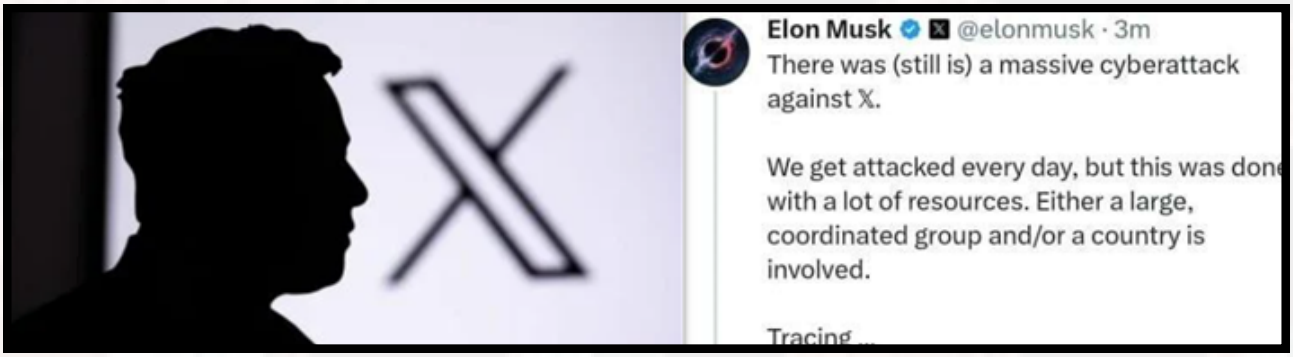
Cinco formas en que los profesionales contribuyen a una gestión eficaz de las amenazas

CVE-2025-24813 en Apache Tomcat expone servidores de RCE

Ciber Incidentes en colombia y en el mundo

e-dea NETWORKS | CYBER SECURITY

X (Twitter) golpeado por un ciberataque masivo



- Elon Musk ha informado que X (antes conocido como Twitter) sufrió de un "gran ataque cibernético", lo que ha provocado interrupciones significativas y ha impedido que los usuarios accedan a la plataforma el 10 de marzo de 2025.
- El ciberataque a X comenzó alrededor de las 5:30 AM del 10 de marzo de 2025, causando interrupciones intermitentes durante todo el día.

CRONOGRAMA E IMPACTO DEL ATAQUE

A pesar de breves períodos de servicio restaurado entre las interrupciones, la plataforma experimentó al menos cinco períodos de caída durante el día.

- 5:30 AM: Comenzaron los primeros informes de interrupciones.
- 9:42 AM: Más de 40,000 informes de interrupciones registrados en Downdetector.
- 3:00 PM: Primer pico importante de interrupciones con casi 2,200 informes de usuarios.
- 7:30 PM: Segundo aumento de informes de interrupciones.
- 9:00 PM: Tercera ola de problemas de acceso reportados.

DECLARACIÓN DE ELON MUSK

La afirmación de Elon Musk de que el ciberataque a X fue llevado a cabo "con muchos recursos" ha llevado a especulaciones sobre una posible implicación estatal en el incidente. En su declaración en la plataforma, Musk sugirió que "O bien un grupo grande y coordinado y/o un país está involucrado" en el ataque.

Esta afirmación ha generado preocupaciones sobre la escala y sofisticación de la amenaza cibernética que enfrenta X.

La Falla CVE-2025-24813 en Apache Tomcat expone los servidores a RCE

Se ha descubierto la vulnerabilidad CVE-2025-24813 , en Apache Tomcat que podría permitir a atacantes ejecutar código remoto, divulgar información confidencial o corromper datos.
Apache Tomcat, un servidor web y contenedor de servlets de código abierto ampliamente utilizado, es vulnerable a esta falla debido a una debilidad en su gestión de solicitudes PUT parciales. Según el aviso, la implementación original de PUT parcial "utilizaba un archivo temporal basado en el nombre y la ruta de archivo proporcionados por el usuario, con el separador de ruta reemplazado por '.'". Este detalle, aparentemente insignificante, crea una vulnerabilidad de seguridad significativa en ciertas circunstancias.

Divulgación de información y Corrupción

Si las escrituras están habilitadas para el servlet predeterminado (deshabilitadas de manera predeterminada), el soporte PUT parcial está activo (habilitado de manera predeterminada), una URL de destino para cargas confidenciales es un subdirectorio de una URL de carga pública y un atacante conoce los nombres de archivos confidenciales que se cargan a través de PUT parcial, puede "ver archivos confidenciales de seguridad y/o inyectar contenido en esos archivos".

Ejecución remota de código (RCE)

Si las escrituras están habilitadas para el servlet predeterminado, el PUT parcial está activo, la aplicación usa la persistencia de sesión basada en archivos de Tomcat con el almacenamiento predeterminado y la aplicación incluye una biblioteca vulnerable a ataques de deserialización, "un usuario malintencionado puede realizar una ejecución de código remota".

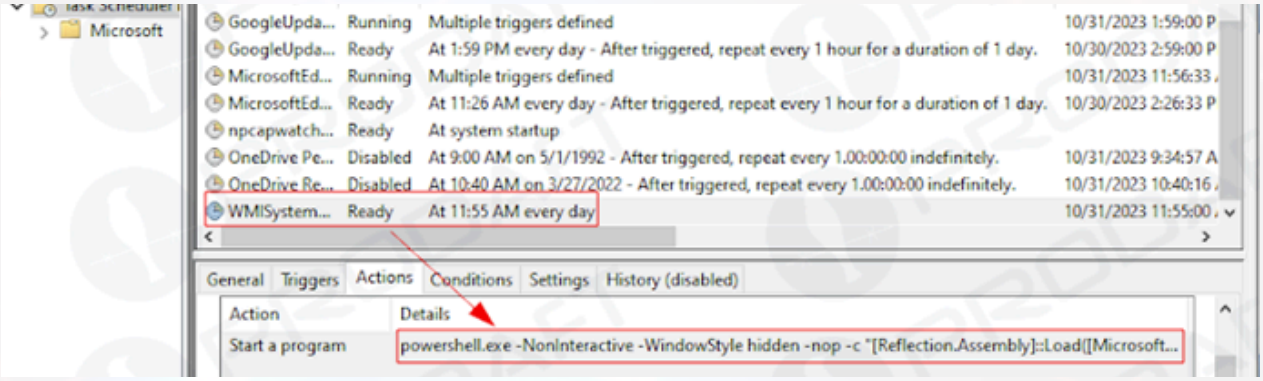
Afecta a las siguientes versiones de Apache Tomcat:
Apache Tomcat 11.0.0-M1 a 11.0.2
Apache Tomcat 10.1.0-M1 a 10.1.34

Se recomienda que los usuarios de estas versiones actualicen a Apache Tomcat 11.0.3 o posterior

Más información

Ragnar Loader: La Herramienta de Acceso Persistente en Operaciones de Ransomware

El malware Ragnar Loader, utilizado por grupos de cibercriminales como FIN7, FIN8, Ragnar Locker (Monstrous Mantis) y Ruthless Mantis (ex-REvil), ha evolucionado hasta convertirse en un kit de herramientas modular que facilita el acceso persistente y la ejecución de ransomware en sistemas comprometidos.
Este malware, documentado por primera vez en 2021 por Bitdefender, ha evolucionado con nuevas capacidades de evasión y persistencia. Investigaciones recientes de PRODAFT confirman que Ragnar Loader sigue en uso.



Características Claves de Ragnar Loader

Ejecución en PowerShell con cargas útiles cifradas en RC4 y Base64.
Evasión de detección mediante inyección de procesos y manipulación de tokens.
Persistencia y acceso remoto a través de un panel de control C2.
Movimiento lateral dentro de redes comprometidas.
Compatibilidad con Linux, incluyendo un módulo ELF llamado "bc", similar a BackConnect en QakBot e IcedID.

Contexto Actual y Relevancia

Este malware sigue siendo una herramienta clave en campañas de ransomware, con ataques recientes dirigidos a sectores empresariales y financieros.

Su continua evolución y el hecho de que pueda ser utilizado por múltiples actores lo convierten en una amenaza persistente para la ciberseguridad en 2024.

Medidas de Mitigación

- ✓ Monitorear actividad de PowerShell y tráfico cifrado.
- ✓ Implementar segmentación de red para limitar la propagación.
- ✓ Utilizar soluciones EDR/XDR basadas en comportamiento.
- ✓ Configurar alertas en SIEM para detectar patrones sospechosos.

Más información

CPU RISC-V de Alibaba y la autosuficiencia de china tecnológicamente.

RISC-V y la Apuesta de Alibaba

RISC-V es una arquitectura de conjunto de instrucciones abierta y libre de regalías, lo que la convierte en una alternativa a las tecnologías propietarias como x86 de Intel y ARM. Alibaba, a través de su filial T-Head, ha desarrollado procesadores RISC-V como el Xuantie C910, enfocados en aplicaciones de alto rendimiento y computación en la nube. Esta adopción responde tanto a razones técnicas como estratégicas, ya que las sanciones de EE. UU. han restringido el acceso de China a tecnologías avanzadas de semiconductores.

El Impacto Global de los Chips RISC-V de Alibaba

La apuesta de Alibaba por RISC-V fortalece la posición de China en el sector de semiconductores y podría disminuir la hegemonía de EE. UU. en la industria. Además, Alibaba promueve RISC-V como una alternativa a ARM y x86, lo que podría transformar el desarrollo de chips en un modelo más colaborativo y descentralizado.

Reacción de EE.UU. y sus Aliados

EE. UU. ha intensificado sus restricciones sobre la exportación de semiconductores a China, pero la naturaleza abierta de RISC-V dificulta su control. A pesar de las tensiones, empresas y universidades estadounidenses también han mostrado interés en esta arquitectura.

Impacto Económico en los Mercados Mundiales y Países Emergentes

La producción de chips RISC-V por parte de China podría generar competencia en los mercados globales, reduciendo costos y ofreciendo acceso a tecnología de alto rendimiento más asequible. Para los países emergentes.

Esto podría alterar las dinámicas comerciales, favoreciendo a mercados que buscan alternativas accesibles para su digitalización.

Más información

Cinco formas en que los profesionales contribuyen a una gestión eficaz de las amenazas

Los programas efectivos de gestión de amenazas se sustentan en cinco pilares clave: preparación, detección, evaluación, mitigación y control, respuesta y prevención. Los profesionales de inteligencia juegan un papel crucial en cada una de estas etapas, colaborando con equipos de seguridad física y tecnología de la información para garantizar una gestión integral de las amenazas.

1. Preparación:

Anticipan amenazas analizando escenarios futuros y evaluando riesgos, colaborando con otros equipos de seguridad para desarrollar estrategias de mitigación y respuesta.

2. Detección y evaluación:

Monitorean diversas fuentes, como redes sociales y datos abiertos, para identificar amenazas emergentes y priorizarlas según su gravedad, permitiendo a la organización actuar a tiempo.

3. Mitigación y control:

Además de identificar amenazas, toman medidas preventivas, como eliminar contenido malicioso en línea y colaborar con autoridades locales para disuadir ataques, participando en la creación de planes de crisis.

4. Respuesta

En situaciones de crisis, emiten informes en tiempo real y asesoran a los responsables de la toma de decisiones, ayudando a gestionar problemas de seguridad y proteger la reputación de la organización.

5. Prevención:

Después de un evento de amenaza, realizan evaluaciones para revisar la efectividad de las medidas adoptadas, ajustando estrategias para mejorar la seguridad a futuro.

En conjunto, los profesionales de inteligencia son esenciales para garantizar que las organizaciones estén preparadas, puedan responder adecuadamente a las amenazas y mejoren continuamente sus capacidades de gestión de riesgos.

Ciber incidentes en Colombia y en el mundo

Colombia ha experimentado un aumento significativo en los ciberataques

En lo que va de 2025, Colombia ha sufrido un aumento considerable en ciberataques, alrededor de más de 20 mil millones de intentos registrados, según notificado por FortiGuard Labs de Fortinet.

Este sitúa al país como el tercero en el mundo con mayor actividad cibercriminal, identificando que el 76% de estos ataques son dirigidos a empresas y ciudadanos, siendo el mas afectado el sector financiero, enfrentando miles de ataques diarios que comprometen información confidencial.

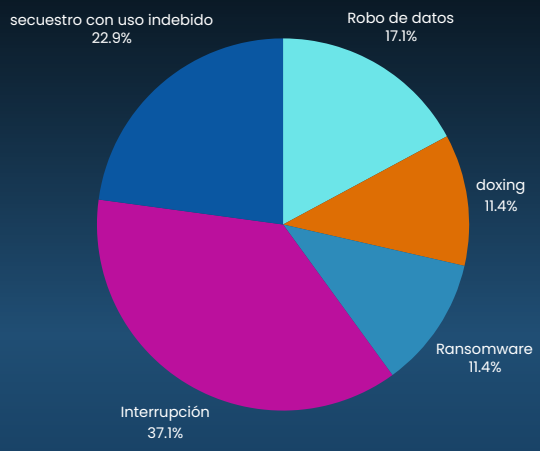
Más información

El mundo

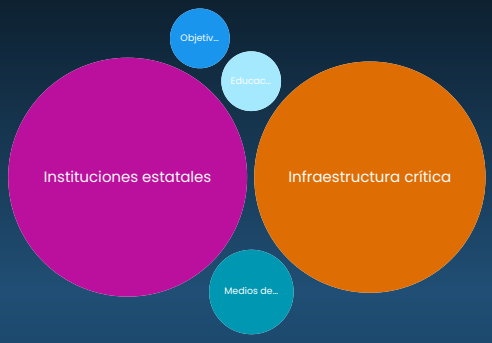
35

Ciber incidentes

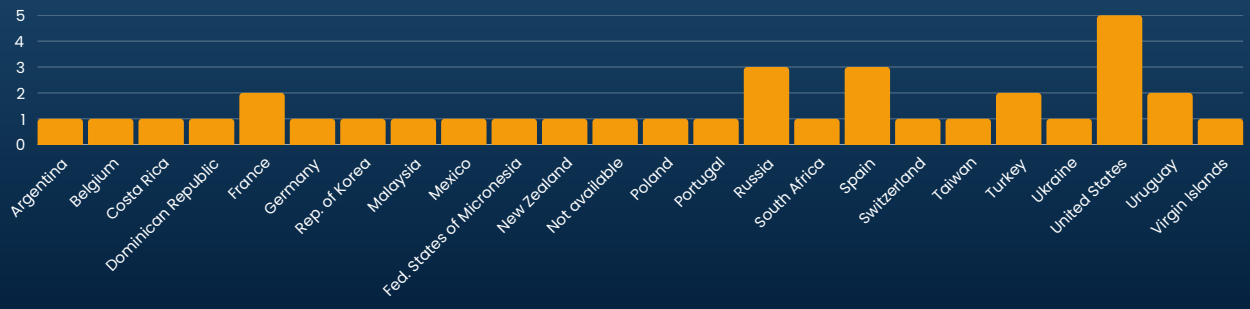
TIPO DE INCIDENTE



SECTORES AFECTADOS



PAISES ATACADOS



Más información

CYBER SECURITY

e-dea NETWORKS

CIBER E-DEA

Boletín de Seguridad

E-dea Networks

@e_deanetworks

E-dea Networks

Csirt E-dea

e-dea.co