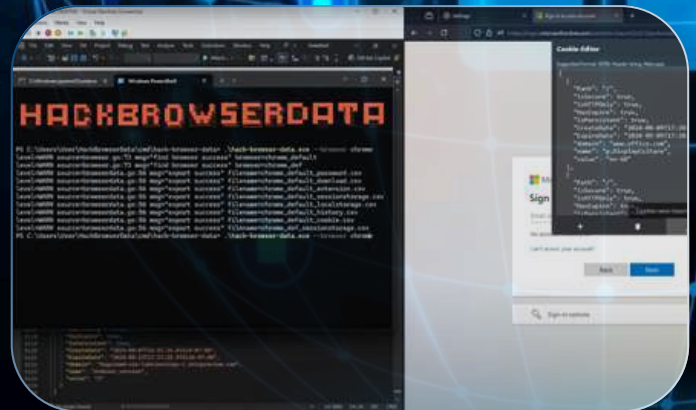


### **Secuestro de sesión 2.0: la última forma en que los atacantes eluden la MFA**

Hoy en día, el secuestro de sesiones es muy distinto. Ya no se basa en la red, sino que es un ataque basado en la identidad que se realiza a través de Internet público y que tiene como objetivo aplicaciones y servicios basados en la nube.

[ver artículo >>](#)



### **Una falla muy esperada en Linux permite la ejecución remota de código, pero es menos grave de lo esperado**

El 23 de septiembre, el investigador Simone Margaritelli reveló que, en menos de dos semanas, revelaría los detalles de una vulnerabilidad de ejecución remota de código (RCE) no autenticada que afecta a todos los sistemas GNU/Linux. Señaló que la falla había recibido una puntuación CVSS de 9,9, lo que llevó a muchos miembros de la industria de la ciberseguridad a creer que sería un problema muy crítico y de alto impacto.

[ver artículo >>](#)

### **Microsoft identifica a Storm-0501 como una amenaza importante en los ataques de ransomware en la nube híbrida**

La campaña de ataque de múltiples etapas está diseñada para comprometer entornos de nube híbrida y realizar un movimiento lateral desde el entorno local al entorno de nube, lo que en última instancia resulta en exfiltración de datos, robo de credenciales, manipulación, acceso persistente por puerta trasera y despliegue de ransomware, dijo Microsoft.

[ver artículo >>](#)



# INCIDENTES DE SISTEMAS



## Plugin The Events Calendar para WordPress - Vulnerabilidades

Desde el CSIRT de Gobierno informamos frecuentemente de vulnerabilidades importantes que pueden afectar sus aplicaciones, datos o equipos.

[ver artículo >>](#)



## Ivanti Cloud Service Appliance (CSA) - Vulnerabilidades

Ivanti reveló que una vulnerabilidad crítica identificada como CVE-2024-8963 está siendo explotada, y que puede ser usada por actores maliciosos en conjunto con CVE-2024-8190

[ver artículo >>](#)

# RECOMENDACIONES DE LECTURA DE SEGURIDAD



## RansomHub

gsdwi.org

4D 17h 57m 41s

Visits: 743

Data Size: 148 gb

Last View: 09-25 18:00:15

2024-09-24 14:10:05



## Explotación de vulnerabilidades: una tendencia que crece en los ciberataques

La explotación de vulnerabilidades se convirtió en un vector de ataque muy importante y recurrente por parte de los cibercriminales. En este contexto de crecimiento sostenido, analizamos puntualmente el panorama en América Latina.

[ver artículo >>](#)

## 3 grupos de ransomware emergentes que se ciñen sobre LATAM

De acuerdo con nuestro último ESET Security Report, el 23% de las empresas de América Latina encuestadas fue víctima de al menos un intento de ataque de ransomware y las industrias o sectores que recibieron más intentos de ataque de ransomware fueron Petróleo/Gas/Minería (36%), Telecomunicaciones (31%), Servicios Públicos (30%), y Retail/Mayorista (29%).

[ver artículo >>](#)

# NOTICIAS DE NUESTROS PARTNERS



## **IBM amplía su centro de datos cuánticos en Poughkeepsie, Nueva York, para impulsar el descubrimiento de algoritmos a nivel mundial**

El último sistema IBM Quantum, impulsado por un procesador IBM Quantum Heron, logra tasas de error reducidas con un rendimiento 16 veces mejor y un aumento de 25 veces en velocidad en comparación con los sistemas IBM Quantum 2022.(1)

IBM completa la instalación del segundo IBM Heron, su procesador cuántico de mayor rendimiento hasta la fecha, ahora disponible para clientes de todo el mundo.

[ver artículo >>](#)

## **Cómo detectar y protegerse contra amenazas de movimiento lateral**

El movimiento lateral es una actividad posterior a la explotación durante la cual un actor de amenazas intenta comprometer los sistemas de TI adyacentes. Después de obtener acceso inicial a un activo o red, el atacante comienza a autenticar o explotar vulnerabilidades en activos conectados electrónicamente para ejecutar comandos u obtener visibilidad de recursos adicionales.

[ver artículo >>](#)

## **Cómo la IA puede ayudar a los CISO a afrontar la escasez mundial de talento cibernético**

La brecha global de habilidades en materia de ciberseguridad se está ampliando, lo que deja a muchas organizaciones vulnerables a las crecientes amenazas cibernéticas. Este blog explora cómo los CISO pueden implementar estrategias de IA para aprovechar al máximo su fuerza laboral existente a través de la automatización, la consolidación y la educación.

[ver artículo >>](#)



# BENCHMARKING EN CIBERSEGURIDAD

Nos es muy grato informarle que, como parte de la estrategia de difusión de los servicios de Riesgo y Seguridad de Mainsoft, hemos creado una serie de benchmarkings sin costo para empresas seleccionadas.

MIDE LA SEGURIDAD DE TU ORGANIZACIÓN SIN COSTO

[HAZ CLICK](#)

## EVENTOS CERCANOS DE NUESTROS PARTNERS

**DARKTRACE**

[Más Información](#)

**BeyondTrust**

[Más Información](#)

**IBM**  
Gold Partner

[Más Información](#)