LITORALPRESS

Fecha: 13-02-2025
Medio: El Mercurio
Supl. : El Mercurio - Innovacion
Tipo: Noticia general
Título: **El cibercrimen organizado aumentó 30% durante el 2024**

Pág. : 5
Cm2: 477,3
VPE: $ 6.269.971

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

El cibercrimen organizado aumentó 30% durante el 2024

Según el reporte del Centro de Ciberinteligencia (CCI) de Entel Digital, las tecnologías más utilizadas para evadir defensas y dirigir ataques de forma masiva y precisa fueron la inteligencia artificial y las plataformas de Ransomware-as-a-Service (RaaS). Esto permitió que incluso actores con menos experiencia llevaran a cabo ataques a gran escala, incrementando en 30% el cibercrimen organizado en comparación al 2023.

Durante 2024, hubo un aumento sostenido en la frecuencia y tecnologización de los ciberataques, siendo el *ransomware* la principal amenaza en Latinoamérica y el Caribe (38% de todas las ciberamenazas registradas). De acuerdo con el Reporte de Ciberseguridad 2025 del CCI de Entel Digital, los grupos de *ransomware* han escalado sus operaciones globales, desarrollando ataques más eficientes, masivos y muy personalizados. Aquí los principales hallazgos para tener en cuenta:

1. En Latinoamérica y el Caribe los países más afectados fueron Brasil (46%), México (17%) y Argentina (10%), sumando el 73% de los incidentes. Chile se posicionó cuarto (7%), seguido por Colombia, también con 7%, evidenciando un creciente interés de parte de los ciberdelincuentes hacia las economías emergentes con infraestructuras tecnológicas consolidadas.

2. El 32% de los ataques de *ransomware* se originaron en vulnerabilidades "no parcheadas", reflejando una falta de planes de mitigación y respuesta ante incidentes, así como la inexistencia de actualizaciones en los sistemas y controles para mitigar los riesgos.

3. El *ransomware* evolucionó a modelos más agresivos, afectando al 90% de las víctimas con amenazas de publicación de datos. Esto ha consolidado la extorsión como un riesgo cada vez más habitual en el panorama cibernético.

4. El impacto económico del cibercrimen también se incrementó en 2024. El gasto asociado a recuperación postincidentes de *ransomware* alcanzó un promedio de US$ 3 millones, cuatro veces más que el de casos de compromisos de credenciales, que alcanza en promedio los US$ 750.000.

5. Los sectores más afectados por el *ransomware* a nivel nacional fueron infraestructura de tecnologías de información (21%), banca y finanzas (17%) y agricultura y ganadería (13%), siendo las medianas y grandes empresas el principal foco para los cibercriminales en 2024.

6. Los incidentes en la nube aumentaron un 61% en comparación con 2023 y, además, evolucionaron en su forma de ataque. Hoy las amenazas se relacionan principalmente con la existencia de brechas de seguridad de datos (21%), uso indebido de los servicios en la nube (17%) y errores de configuración y administración (12%).

Según explica Eduardo Bouillet, director del CCI de Entel Digital, "la ciberseguridad está cada vez más desafiada, por ello es vital invertir en una cultura organizacional que priorice la seguridad digital y adopte una gestión proactiva de vulnerabilidades. Al mismo tiempo, es muy importante informarse, entender qué está pasando, cuáles son los riesgos existentes y qué grupos de ciberamenazas pueden afectar a mi organización".

El Reporte de Ciberseguridad 2025 se encuentra disponible en www.enteldigital.cl

ENTEL

El reporte analizó un total de 768 casos de *ransomware* y *data leak* de América Latina y el Caribe ocurridos en 2024.

Descarga el reporte completo.