Dirección de Investigación Criminal e INTERPOL
Centro Cibernético Policial

BALANCE 09
2025

Cyber Noticias

El malware GitVenom roba 456.000 dólares en bitcoins utilizando proyectos falsos de GitHub para secuestrar billeteras. Los investigadores de ciberseguridad están llamando la atención sobre una campaña en curso que apunta a jugadores e inversores en criptomonedas bajo la apariencia de proyectos de código abierto alojados en GitHub. La campaña, que abarca cientos de repositorios, ha sido bautizada como GitVenom por Kaspersky, dejando **580** victimas.

Fuente: The Hacker News.

Hackers norcoreanos vinculados a robo de criptomonedas por 1.500 millones de dólares en ByBit. El grupo de hackers Lazarus, está detrás del robo de más de 1.500 millones de dólares en criptomonedas de Bybit. Durante el fin de semana, expertos en seguridad informática confirmaron que los atacantes interceptaron una transferencia de fondos entre billeteras, desviando los activos a una dirección de blockchain controlada por ellos, convirtiéndose en el robo de criptomonedas más grande de la historia.

Fuente: BleepingComputer

Modalidad "Pig Butchering"

Modalidad de estafa en la cual, los atacantes ganan la confianza de sus víctimas, generalmente entablando conversaciones de índole romántico, a través de aplicaciones de citas y redes sociales, solicitando posteriormente inversión de activos, especialmente en esquemas de criptomonedas.

1. **Contacto inicial**: el estafador inicia conversaciones con la víctima, usualmente a través de redes sociales o plataformas de citas. Posteriormente, construirá confianza compartiendo fotos, videos y planes a futuro.
2. **Introducción a la estafa**: tras haber generado confianza, el estafador introducirá en la víctima una oportunidad de inversión, la cual parecerá lucrativa y de bajo riesgo.
3. **Fomento de inversión**: se convencerá a la víctima de invertir pequeñas sumas de dinero, las cuales aparentarán mostrar ingresos, los cuales son fabricados para mantener el interés del usuario.
4. **Incremento de inversión**: el estafador presionará a la víctima para invertir altas sumas de dinero, mostrando grandes ingresos que se pudiesen obtener.
5. **"Salida"**: una vez obtenidas altas sumas de dinero, el estafador desaparecerá con las ganancias obtenidas de la víctima, generando una pérdida financiera significante.

RECOMENDACIONES

- **Sea** cauteloso al recibir mensajes de perfiles no deseados, especialmente en portales de citas.
- **Evite** compartir información financiera o confidencial en relaciones en línea.
- **Investigue** sobre cualquier oportunidad de inversión antes de entregar dinero.
- **Reconozca** factores de riesgo como manipulación emocional o promesas de dinero fácil.
- **Reporte** cualquier incidente ocurrido al CAI Virtual, a través del portal web https://caivirtual.policia.gov.co.

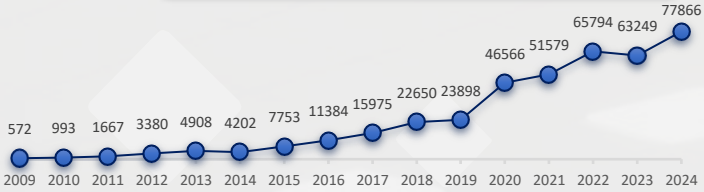
Balance Cibercriminalidad – Ley 1273/09

Variación Porcentual	2024	2025	
-26%	5.556	4.105	Hurto por medios informáticos y semejantes
46%	1.633	2.387	Acceso abusivo a un sistema informático
2%	1.363	1.399	Violación de datos personales
-22%	755	587	Suplantación de sitios web
-20%	573	462	Transferencia no consentida de activos
-41%	154	89	Interceptación de datos informáticos
10%	56	64	Obstaculización ilegitima de sistema informático o red de comunicación
-33%	51	34	Daño informático
-54%	35	16	Uso de software malicioso

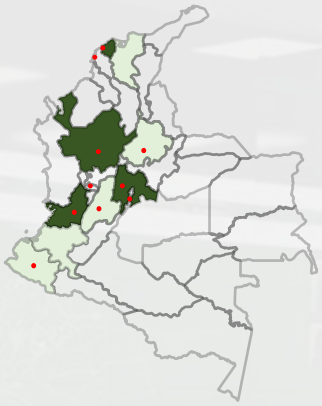
TOTAL -10 % 10.173 9.143

Corte del 01 de enero al 28 de febrero del 2024. vs del 01 de enero al 28 de febrero del 2025.

Evolución histórica *(No. Denuncias vs año)*



Ciudades/Departamentos con mayor afectación



- **20%** Bogotá 2.755
- **8%** Cali 723
- **6.7%** Cundinamarca 614
- **4.9%** Medellín 448
- **3.2%** Barranquilla 293
- **2%** Pasto 182
- **1.8%** Pereira 172
- **1.8%** Cartagena 169
- **1.8%** Ibagué 167
- **1.7%** Bucaramanga 156

Estas ciudades y departamentos representan el **59.6 %** del total del fenómeno a nivel nacional.

Datos extraídos el día 28 de febrero 2025. Cifras sujetas a variación en atención al proceso de integración y consolidación con la información de la Fiscalía General de la Nación.

Fuente: SIEDCO Plus 2.0

Actividades de gestión en seguridad digital

Capturas ESCIB
Delitos informáticos **31**
Explotación sexual infantil en Internet. **06**

Incidentes gestionados
a través del CAI Virtual

Charlas de ciberseguridad
Personas impactadas **848**

Alertas y contenidos preventivos
03 durante la semana

Actividades de relacionamiento estratégico

Páginas bloqueadas
Material de abuso sexual infantil. **2.516**
Juegos ilegales de azar. **1.251**

Documento no controlado

Canales de atención y redes sociales

Página web

X
@CaiVirtual

Instagram
@caivirtual

Facebook
CAI Virtual

WhatsApp

Para sugerencias sobre este producto, por favor diligencie este formulario: https://bit.ly/3mz5C8d