Dirección de Investigación Criminal e INTERPOL
Centro Cibernético Policial

BALANCE 48
2025

Cyber Noticias

Investigadores de CERT Polska descubrieron **NGate**, un nuevo malware para Android que aprovecha la función **NFC** del teléfono para robar datos bancarios. El virus intercepta pagos sin contacto, incluyendo PIN y códigos de autenticación, y envía esa información a los atacantes. Con estos datos, los delincuentes pueden acercarse a un cajero automático y retirar dinero de la cuenta de la víctima en tiempo real.

Fuente: Yahoo!finanzas

Investigadores de ciberseguridad descubrieron Crypto Copilot, una extensión maliciosa en la Chrome Web Store que engaña a los usuarios al inyectar una transferencia oculta de Solana durante intercambios en el DEX Raydium. Aunque se presenta como una herramienta para operar criptomonedas en X, la extensión desvía automáticamente pequeñas cantidades hacia una billetera digital. La extensión utiliza código ofuscado para manipular transacciones sin que el usuario lo note.

Fuente: thehackernews

NGate

Malware que infecta el celular y, mediante NFC, intercepta la información bancaria durante retiros sin tarjeta en cajeros automáticos. Esto permite clonar la tarjeta y los datos financieros del usuario, así los delincuentes realizan retiros sin tarjeta física.

- ✓ **Infección inicial:** la víctima recibe un mensaje falso del banco y, al abrir un enlace, instala sin saberlo el malware **NGate**.
- ✓ **Activación NFC:** el malware toma control de la función NFC del teléfono y empieza a captar información bancaria cuando el usuario hace pagos o retiros sin tarjeta.
- ✓ **Clonación de la tarjeta:** con los datos capturados, los delincuentes crean una tarjeta clonada o una emulada digitalmente.
- ✓ **Fraude financiero:** El ciberdelincuente utiliza la tarjeta digital creada en otro dispositivo para hacer retiros en cajeros automáticos o pagos sin necesidad de la tarjeta física.

RECOMENDACIONES

- **No instale** aplicaciones ni abra enlaces provenientes de mensajes o correos sospechosos, especialmente si solicitan información bancaria o activar funciones como NFC.
- **Mantenga** siempre actualizado el sistema operativo y las aplicaciones, y use soluciones de seguridad móvil confiables que detecten y bloqueen malware.
- **Desactive** la función NFC en el teléfono cuando no se use para evitar que aplicaciones maliciosas accedan a datos de tarjetas cercanas.
- **Reporte** cualquier incidente ocurrido ante el CAI Virtual, a través de la línea de **WhatsApp 3232733411**.

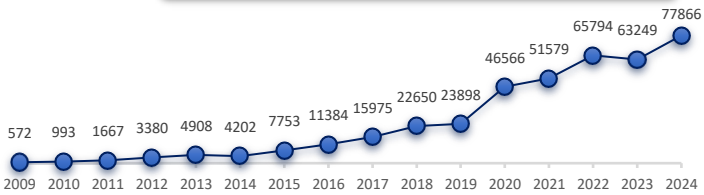
Balance Cibercriminalidad – Ley 1273/09

Variación Porcentual	2024	2025	
1 %	34.882	35.316	Hurto por medios informáticos y semejantes
-9%	14.785	13.381	Acceso abusivo a un sistema informático
-19%	10.221	8.280	Violación de datos personales
-29%	5.246	3.716	Suplantación de sitios web
-15%	3.195	2.690	Transferencia no consentida de activos
-24%	750	565	Interceptación de datos informáticos
-11%	350	311	Obstaculización ilegitima de sistema informático o red de comunicación
-19%	263	211	Daño informático
-9%	175	158	Uso de software malicioso

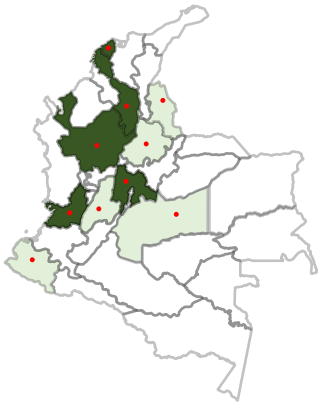
TOTAL -7% 69.867 64.628

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

Evolución histórica *(No. Denuncias vs año)*



Ciudades con mayor afectación



- 27% Bogotá 19.288
- 7% Medellín 5.087
- 5% Cali 4.115
- 3% Barranquilla 2.275
- 3% Cartagena 1.299
- 3% Bucaramanga 1.201
- 2% Ibagué 1.150
- 1 % Pasto 1.055
- 1 % Villavicencio 1.033
- 1 % Cúcuta 860

Estas ciudades y departamentos representan el **53%** del total del fenómeno a nivel nacional.

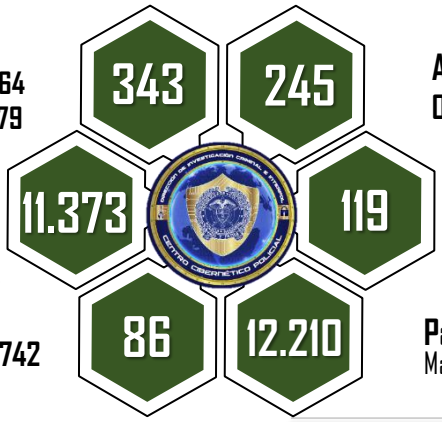
Datos extraídos el día 28 de noviembre de 2025. Cifras sujetas a variación en atención al proceso de integración y consolidación con la información de la Fiscalía General de la Nación. ***Fuente: SIEDCO Plus 2.0.***

Actividades de gestión en seguridad digital

Capturas ESCIB
Delitos informáticos 264
Explotación sexual infantil en Internet. 79

Incidentes gestionados
a través del CAI Virtual 11.373

Charlas de ciberseguridad
Personas impactadas 21.742



Alertas y contenidos preventivos
03 durante la semana

Actividades de relacionamiento estratégico
TOYOTA Defensa FORTINET

Páginas bloqueadas
Material de abuso sexual infantil. 12.210

Documento no controlado

Página web

X
@Centro Cibernético

Instagram
@Caivirtual_dijin

Facebook
CAI Virtual

WhatsApp

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