BALANCE

SEMANA 43/2024

Cyber Noticias

El grupo Lazarus aprovecha una vulnerabilidad de Google Chrome para controlar los dispositivos infectados. Al actor de amenazas norcoreano conocido como Lazarus Group se le ha atribuido la explotación de día cero de una falla de seguridad ahora parcheada en Google Chrome para tomar el control de los dispositivos infectados, Esto activando un exploit de día cero simplemente al visitar un sitio web de juegos falso ("detankzone[.]com") que estaba dirigido a personas del sector de las criptomonedas.

Fuente: The Hacker News

WhatsApp ahora encripta las bases de datos de contactos para una sincronización que preserva la privacidad. La plataforma WhatsApp ha presentado Identity Proof Linked Storage (IPLS), un sistema de almacenamiento cifrado que preserva la privacidad, diseñado para la gestión de contactos, resolviendo dos problemas enfrentados por los usuarios, el riesgo de perder sus listas de contactos si pierden su teléfono y la imposibilidad de sincronizar contactos entre diferentes dispositivos.

Fuente: BleepingComputer

MODALIDAD PHREAKING O HACKEO TELEFÓNICO

Manipulación y exploración de los sistemas telefónicos con el fin de realizar llamadas gratuitas o acceder sin autorización a redes de telecomunicaciones.

- Los Phreakers recopilan información sobre las redes telefónicas y sus componentes. funcionamiento de los sistemas telefónicos, frecuencias utilizadas y cómo se enrutan las llamadas.
- Una vez reunida la suficiente información, los phreakers intentan acceder a la red telefónica con herramientas como "blue boxes", generando tonos para manipular el sistema de conmutación de las empresas telefónicas.
- Explotada la vulnerabilidad se llevan a cabo actividades delictivas, como llamadas sin pagar o el acceso no autorizado a servicios telefónicos premium, buscando mantener el acceso a la red.
- Los Phreakers utilizan técnicas para eliminar cualquier rastro de sus actividades para evitar ser rastreados.

RECOMENDACIONES

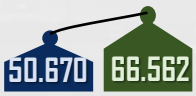
- **REVISE** que las configuraciones de seguridad sean adecuadas.
- **EVITE** conectarse a redes de Wi-Fi públicas o sin protección.
- **PROTEJA** la tarjeta sim y considere la posibilidad de bloquearla ante sospechas de vulnerabilidad.
- **REPORTE** cualquier incidente ocurrido al CAI Virtual a través de la web **https://caivirtual.policia.gov.co**.

Balance Cibercriminalidad – Ley 1273/09

Variación Porcentual	2023	2024	
35 %	24.000	32.384	Hurto por medios informáticos y semejantes
49 %	9.396	13.969	Acceso abusivo a un sistema informático
17 %	8.682	10.151	Violación de datos personales
44 %	3.740	5.388	Suplantación de sitios web
11 %	2.820	3.118	Transferencia no consentida de activos
-31 %	1.137	783	Interceptación de datos informáticos
14 %	279	318	Obstaculización ilegítima de sistema informático o red de telecomunicación
-24 %	350	265	Daño informático
-30 %	266	186	Uso de software malicioso

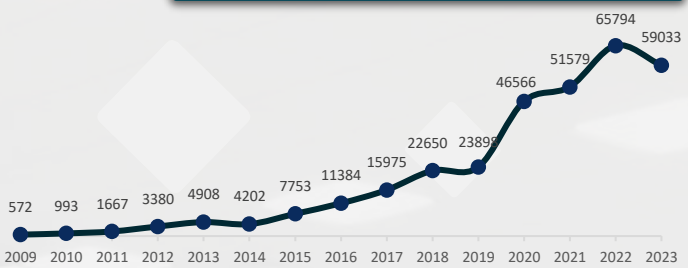
TOTAL 31%

Corte del 01 de enero al 25 octubre del 2023. vs del 01 de enero 25 octubre del 2024,



Las denuncias a la fecha representan el **113%** del total registrado en 2023.

Evolución histórica *(No. Denuncias vs año)*



Ciudades/Departamentos con mayor afectación

Estas ciudades y departamentos representan el **64%** del total del fenómeno a nivel nacional.

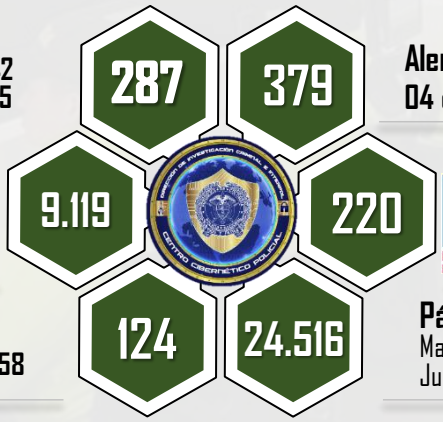
Datos extraídos el día 25 de octubre de 2024. Cifras sujetas a variación en atención al proceso de integración y consolidación con la información de la Fiscalía General de la Nación.

Fuente: SIEDCO Plus 2.0.

Actividades de gestión en seguridad digital

Capturas
Delitos informáticos. 242
Explotación sexual infantil en Internet. 45

Incidentes gestionados
a través del CAI Virtual



Alertas y contenidos preventivos
04 durante la semana

Actividades de relacionamiento estratégico

FISCALÍA · COP16 COLOMBIA · MINDEFENSA · Chainalysis

Charlas de ciberseguridad
Personas impactadas 11.858

Páginas bloqueadas
Material de abuso sexual infantil. 21.982
Juegos ilegales de azar. 2.534

Canales de atención y redes sociales

Página web

X

Instagram

WhatsApp

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