Dirección de Investigación Criminal e INTERPOL
Centro Cibernético Policial

BALANCE **SEMANA 8/2023**

Cyber noticias

Si descargaste ChatGPT, es posible que tus cuentas estén hackeadas. Kaspersky advirtió de un nuevo malware que roba credenciales de redes sociales haciéndose pasar por una app de ChatGPT. Si descargaste un archivo ejecutable en tu computadora para usar ChatGPT, el famoso chatbot que ha sido capaz de revivir al buscador y explorador de Microsoft, es posible que tus credenciales de redes sociales estén en riesgo, ya que los cibercriminales crean grupos que imitan de manera convincente las cuentas oficiales del laboratorio de inteligencia artificial **OpenAI** o comunidades de entusiastas de **ChatGPT**. **Fuente:** Forbes.

Apple advierte sobre 3 nuevas vulnerabilidades que afectan a dispositivos iPhone, iPad y Mac. Apple revisó los avisos de seguridad que publicó el mes pasado para incluir tres nuevas vulnerabilidades que afectan a iOS, iPadOS y macOS. Las vulnerabilidades de gravedad media a alta se han parcheado en iOS 16.3, iPadOS 16.3 y macOS Ventura 13.2 que se enviaron el 23 de enero de 2023. **Fuente**: Thehackernews.

El "ecosistema del cibercrimen" de Telegram rivaliza con la Dark Web. Un ecosistema de delitos cibernéticos se está basando en Telegram, y el alcance de los servicios que ofrece está creciendo para rivalizar con los foros de la Darkl web, según el informe de inteligencia de delitos cibernéticos KELA. Teniendo en cuenta, que Telegram es más fácil de acceder para la persona promedio y sus cientos de millones de usuarios pueden estar a una simple búsqueda de ofertas por los ciberdelincuentes. **Fuente:** Swarmnetics.

Tercera temporada: Curso Rápido de Seguridad "Una imagen fatal". Tenga cuidado cuando comparte información e imágenes con contenido sexualmente explícito. Usted puede ser una potencial víctima del Sexting . En este episodio se explica cómo prevenir esta modalidad y los canales de atención dispuestos para las víctimas. Dictado por Policías expertos en estudiar delitos. **Fuente:** Spotify.

¡ Email-spoofing DIVRI !

Se ha reportado una campaña de email spoofing, donde difunden el malware **Remcos,** que es de tipo RAT (troyano de acceso remoto). Los ciberdelincuentes lo utilizan para realizar acciones en las máquinas infectadas de forma remota, obtener información personal de las víctimas, afectar el patrimonio de las personas y/o ejecución de software malicioso. Lo anterior asociado al asunto: **"DEMANDA PENAL .DIVRI"**.

1

El correo allegado le informa a la víctima de una presunta **"DEMANDA PENAL"** Dirección de Veteranos y Rehabilitación Inclusiva – DIVRI.

2

Solicita que la víctima dé clic en el archivo adjunto: **"DEMANDA PENAL .DIVRI.Uue"**, que a su vez debe ingresar una contraseña que lo redireccionará a la ejecución del malware.

3

RECOMENDACIONES

- **No** abra el archivo y **EVITE** dar clic, sobre links o archivos adjuntos en correos electrónicos desconocidos.
- **VERIFIQUE** ortografía y redacción, usualmente hay errores.
- **REQUIERA** credenciales de administrador para instalar el software.
- **VERIFIQUE** los enlaces o archivos antes de ejecutarlos en un entorno de prueba (sanbox), **Ej:**Any.Run.
- **COMUNÍQUESE** directamente con los sitios oficiales de agencias de ley ante cualquier duda.
- Como se trata de **EMAIL SPOOFING**, revise en detalles del mensaje el RECEIVED-SPF. Debería decir: **"Pass" (**remitente permitido).
- **REPORTE** el correo allegado con el CAI Virtual a través de la web: https://caivirtual.policia.gov.co

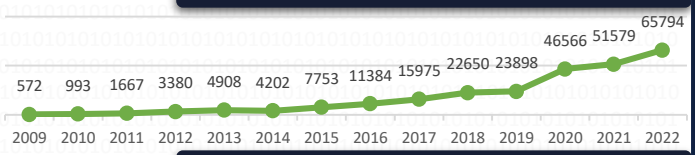
Fuente: *Csirt defensa*

Balance Cibercriminalidad – Ley 1273/09

Variación Porcentual	2022	2023	
-5 %	3.505	3.335	Hurto por medios informáticos y semejantes
-11 %	1.760	1.575	Violación de datos personales
-5 %	1.592	1.513	Acceso abusivo a un sistema informático
-18 %	822	698	Suplantación de sitios web
-16 %	506	426	Transferencia no consentida de activos
-5 %	222	212	Interceptación de datos informáticos
-28 %	83	60	Daño informático
-13 %	69	60	Obstaculización ilegítima de sistema informático o red de telecomunicación
14 %	44	50	Uso de software malicioso
TOTAL	**- 8 %**	8.604	7.909

Corte del 01 de enero al 25 de febrero 2022.
vs 01 de enero al 25 de febrero 2023.

Evolución histórica *(No. Denuncias vs año)*



Ciudades/Departamentos de mayor afectación

(Ciudad y Dpto No. Eventos, %)

- Bogotá: 32% — 2.556
- Medellín: 8% — 665
- Cundinamarca: 7% — 526
- Cali: 5% — 405
- Barranquilla: 4% — 297
- Ibagué: 2% — 166
- Cartagena: 2% — 159
- Villavicencio: 1,7% — 134
- Cúcuta: 1,7% — 134
- Bucaramanga: 1,4% — 99

Las denuncias a la fecha representan el **12 %** del total del 2022.
Corte del 01 de enero al 25 de febrero 2023.

CAPTURAS 2023

Delitos Ley 1273.	**38**
Explotación sexual infantil en Internet.	**3**

5 Durante la semana

Fuente: SIEDCO Plus

Actividades de gestión en seguridad digital

Incidentes gestionados a través del CAI Virtual — **2.017**

88 — **Alertas y contenidos preventivos** 15 durante la semana

Muestras de malware analizadas — **223**

25 — **Actividades de relacionamiento estratégico,** resaltando en la semana:

UNODC Oficina de las Naciones Unidas contra la Droga y el Delito · ASOBANCARIA

Charlas de ciberseguridad Personas impactadas **1.252** — **11**

3.702 — **Páginas bloqueadas** Material de abuso sexual infantil.

Para sugerencias sobre este producto, por favor diligencie este formulario : https://bit.ly/3Zf2HAc

Canales de atención y redes sociales

Página web · Twitter · Instagram · facebook · WhatsApp