# Dirección de Investigación Criminal e INTERPOL
# Centro Cibernético Policial

BALANCE **SEMANA 7/2023**

## Cyber noticias

**Los hackers de RedEyes usan nuevo malware para robar datos de Windows y teléfonos.** Un grupo de hackers envía correos electrónicos de phishing que contienen un archivo malicioso a sus objetivos. El exploit hará que el shellcode se ejecute en la computadora de una víctima que descarga y ejecuta el archivo malicioso almacenado dentro de una imagen JPG. Este archivo de imagen JPG utiliza esteganografía, una técnica que permite ocultar código dentro de archivos, para introducir sigilosamente el ejecutable del malware **M2RAT** ("lskdjfei.exe") en el sistema e inyectarlo en "explorer.exe". **Fuente:** Bleepingcomputer.

**Cómo los mercados de la darknet y las tiendas de fraude lucharon por los usuarios a raíz del colapso de Hydra.** Hydra Market lideró el camino una vez más como el mercado de darknet con mayores ingresos en 2022, a pesar de que fue sancionado por la OFAC y cerrado. El año 2022 vio una disminución en los ingresos del año anterior para los mercados de la red oscura y las tiendas de fraude. Los ingresos totales del mercado de darknet para el año 2022 terminaron en $ 1.5 mil millones, por debajo de los $ 3.1 mil millones en el años 2021. **Fuente:** Chainalysis.

**DHL y los correos electrónicos de phishing de MetaMask se dirigen a clientes de Namecheap.** Una campaña de envíos de correos electrónicos de phishing que se hacen pasar por la empresa DHL y la extensión de navegador MetaMask comenzó a llegar a los correos de los clientes de Namecheap la semana pasada, intentando engañar a los destinatarios para que compartan información personal o compartan la frase de recuperación secreta de su billetera criptográfica. **Fuente:** Helpnetsecurity.

**Los estafadores se benefician del terremoto entre Turquía y Siria.** Estas estafas pretenden recaudar dinero para los sobrevivientes, que se quedaron sin calefacción ni agua después de los desastres donde fallecieron más de 35,000 personas. Pero en lugar de ayudar a los necesitados, los estafadores están canalizando donaciones lejos de organizaciones benéficas reales y en sus propias cuentas PayPal y billeteras de criptomonedas. En TikTok Live, los creadores de contenido pueden ganar dinero recibiendo regalos digitales. **Fuente:** Bleepingcomputer.

## Modalidad reportada al CAI Virtual

# ¡FALSA CONVOCATORIA DE INTERPOL!

Al servicio 24/7 CAI virtual, la ciudadanía ha reportado una campaña de la modalidad Phishing, se trata de una modalidad de fraude, bajo el engaño de una supuesta **convocatoria** de un proceso investigativo, busca obtener la información personal de las víctimas, comisión de estafas y/o descargas de softwares maliciosos. Lo anterior asociado al asunto: **"CARTA JURÍDICA".**

**De:** POLICÍA INTERPOL <police.federale1010@gmail.com>
**Enviado:** lunes, 13 de febrero de 2023 9:07 a. m.
**Para:**
**Asunto:** CARTA JURIDICA

DIRECCIÓN GENERAL DE LA POLICÍA INTERPOL

*Acciones legales contra usted*

INTERPOL

**Convocatoria**

Soy la comisaria Veronique Bechu de la policía de Interpol.

A raíz de una incautación informática por ciberinfiltración en su servidor, usted está sujeto a varios procedimientos judiciales en vigor, en particular en lo que se refiere a:

* PORNOGRAFÍA INFANTIL
* SITIO PORNOGRÁFICO
* CIBERPORNOGRAFÍA

Para su información, **Ley nº 390-1 del Código de Procedimiento Penal de marzo de 2007** agrava las penas cuando la proposición, la agresión sexual o la violación se hayan cometido a través de Internet y se hayan cometido delitos de pornografía contra menores en sitios privados.

En aras de la confidencialidad, le enviamos este correo electrónico; que se le escuche escribiéndonos sus justificaciones para que puedan ser examinadas y verificadas con el fin de evaluar las sanciones; esto en un plazo estricto de 48 horas.

En este caso, su expediente también se transmitirá a las asociaciones de lucha contra la pedofilia y a los medios de comunicación para su publicación como persona inscrita en el RN DS. En caso de desatención de este correo electrónico, y del incumplimiento del procedimiento, así como del retraso tras la recepción de este correo (48 horas como máximo), se le enviará una carta de convocatoria por correo postal.

Dirección de contacto: **police.federale1010@gmail.com**

Después de este plazo, estaremos obligados a presentar nuestro informe a Sr. James Kirkpatrick Stewart, Fiscal Adjunto de la Corte Penal Internacional y especialista en ciberdelincuencia para que elabore una orden de detención contra usted, la envíe a la gendarmería más cercana a su lugar de residencia para su arresto y sea registrado como delincuente sexual.

A la espera de su prueba para abrir el PV (Procès-verbal).

Ya estáis avisados.

BRIGADA DE PROTECCIÓN DE MENORES

*Jürgen Stock*
*Secretaire generale interpol*

1. Se identifica el correo electrónico remitente police.federale1010@gmail.com , el cual es utilizado como supuesto correo oficial para emitir notificaciones fraudulentas de un proceso investigativo.
2. Teniendo en cuenta la verificación y análisis de esta notificación se puede evidenciar que este correo tiene dominio @gmail.com, evidenciando que no es un correo institucional de INTERPOL

En este caso, su expediente también se transmitirá a las asociaciones de lucha contra la pedofilia y a los medios de comunicación para su publicación como persona inscrita en el RN DS. En caso de desatención de este correo electrónico, y del incumplimiento del procedimiento, así como del retraso tras la recepción de este correo (48 horas como máximo), se le enviará una carta de convocatoria por correo postal.

Dirección de contacto: **police.federale1010@gmail.com**

### RECOMENDACIONES

- **No** abra el PDF y **EVITE** dar clic, sobre links o archivos adjuntos en correos electrónicos desconocidos.
- **RECUERDE que** INTERPOL jamás se pone en contacto directamente con un ciudadano, ni le pide dinero, ni sus datos bancarios o que haga una transferencia.
- **VERIFIQUE** ortografía y redacción, usualmente hay errores.
- **VERIFIQUE** que el dominio del correo del remitente corresponda a INTERPOL o agencias de ley.
- **INFORME** si recibe un correo electrónico o un escrito sospechoso cuyo remitente aparente sea INTERPOL, comuníquelo a través de INTERPOL.
- **REPORTE** el correo allegado con el CAI Virtual a través de la web: https://caivirtual.policia.gov.co

# Dirección de Investigación Criminal e INTERPOL
# Centro CIBERNÉTICO Policial

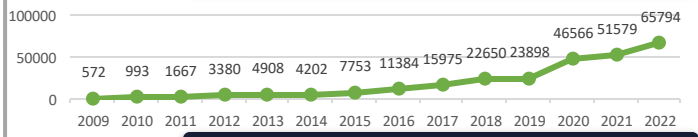
BALANCE SEMANA 7/2023

## Balance Cibercriminalidad – Ley 1273/09

| | 2022 | 2023 | Variación Porcentual | |
|---|---|---|---|---|
| Hurto por medios informáticos y semejantes | 2.878 | 2.799 | -3 % | |
| Violación de datos personales | 1.576 | 1.325 | -16 % | |
| Acceso abusivo a un sistema informático | 1.389 | 1.234 | -11 % | |
| Suplantación de sitios web | 719 | 586 | -18 % | |
| Transferencia no consentida de activos | 415 | 352 | -15 % | |
| Interceptación de datos informáticos | 203 | 175 | -14 % | |
| Daño informático | 72 | 53 | -26 % | |
| Obstaculización ilegítima de sistema informático o red de telecomunicación | 65 | 48 | -26 % | |
| Uso de software malicioso | 38 | 35 | -8% | |
| **TOTAL** | 7,356 | 6,607 | - 10 % | |

Corte del 01 de enero al 18 de febrero 2022 vs 01 de enero al 18 de febrero 2023.

### Evolución histórica *(No. Denuncias vs año)*




### Ciudades/Departamentos de mayor afectación

*(Ciudad y Dpto No. Eventos, %)*

- Bogotá: 32% — 2.112
- Medellín: 8% — 560
- Cundinamarca: 7% — 447
- Cali: 5% — 337
- Barranquilla: 4% — 258
- Cartagena: 2% — 134
- Ibagué: 1,9% — 129
- Villavicencio: 1,7% — 115
- Cúcuta: 1,6% — 110
- Bucaramanga: 1,5% — 99

Las denuncias a la fecha representan el **10 %** del total del 2022.
Corte del 01 de enero al 18 de febrero 2023.

### CAPTURAS 2023

| | | |
|---|---|---|
| Delitos Ley 1273. | 33 | 5 Durante la semana |
| Explotación sexual infantil en Internet | 2 | |

*fuente: SIEDCO Plus*

## Actividades de gestión en seguridad digital

**Incidentes gestionados** a través del CAI Virtual — 1.667

**Alertas y contenidos preventivos** 16 durante la semana — 73

**Muestras de malware analizadas** — 222

**Actividades de relacionamiento estratégico,** resaltando en la semana: — 24

Coljuegos ASOBANCARIA

**Charlas de ciberseguridad** Personas impactadas **852** — 07

**Páginas bloqueadas** Material de abuso sexual infantil. — 3.242

Para sugerencias sobre este producto, por favor diligencie este formulario : https://bit.ly/3k6gutl