Dirección de Investigación Criminal e INTERPOL
Centro Cibernético Policial

BALANCE **SEMANA 2/2023**

Cyber noticias

Los piratas informáticos recurren a los anuncios de búsqueda de Google para impulsar malware que captura información. Los piratas informáticos están configurando sitios web falsos con software popular gratuito y de código abierto para promover descargas maliciosas a través de anuncios en los resultados de búsqueda de Google y obtener la información de las víctimas. **Fuente:** Bleepingcomputer.

Descifradores gratuitos lanzados para BianLian, MegaCortex Ransomware. Avast y Bitdefender han lanzado descifradores de forma gratuita para las víctimas del ransomware **BianLian** y **MegaCortex**. El descifrador **BianLian** (descarga directa) está disponible en el sitio web de Avast. A principios de este mes, Bitdefender anunció la disponibilidad de una herramienta de descifrado gratuita para las víctimas de **MegaCortex**, creada en cooperación con el Proyecto NoMoreRansom de Europol y la policía Suiza. El descifrador está disponible en el sitio web de Bitdefender (descarga directa) y la empresa también proporciona una guía paso a paso para usar la herramienta. **Fuente:** Bleepingcomputer.

MetaMask advierte sobre una nueva y peligrosa estafa llamada "envenenamiento de direcciones". El proveedor de billeteras de criptomonedas MetaMask, advirtió a los usuarios sobre una nueva estafa llamada "Envenenamiento de direcciones"; la estafa se utiliza para engañar a los usuarios para que envíen fondos a un estafador en lugar del destinatario previsto.
Fuente: Hackwise.

Cuidado: se utilizan VPN's contaminadas para difundir el software de vigilancia EyeSpy. Instaladores de VPN corruptos, están entregando un software de vigilancia denominado EyeSpy, como parte de una campaña de malware que comenzó en mayo de 2022. Utilizan "componentes de SecondEye, una aplicación de monitoreo legítima, para espiar a los usuarios de 20Speed VPN a través de instaladores troyanos", dijo Bitdefender en un análisis.
Fuente: Thehackernews.

Modalidad reportada al CAI Virtual ¡Spear-PHISHING!

Scotiabank. COLPATRIA

En reportes al CAI virtual se evidenció una campaña de **Spear-Phishing** (ataque dirigido a un objetivo específico), mediante ingeniera social, suplantando al sitio web oficial de la entidad bancaria **Scotiabank Colpatria**.

Modalidad

Mediante esta modalidad la víctima entrega datos personales y financieros en sitios web bancarios aparentemente oficiales. Estos datos están siendo usados para transferencias no consentidas de activos, suplantación y accesos abusivos a sistemas informáticos.

Características

El correo falso de la entidad bancaria suplantada, le indica a la víctima que para validar la información, debe dar clic en el botón titulado "Ingresar", que redirecciona a la potencial víctima al link: http://bitly.ws/yUdT

Captura de datos

Al momento en que la víctima accede al sitio web, ésta solicita datos específicos de cuentas bancarias, los cuales son captados por los ciberdelincuentes.

Transacción NO consentida

Con los datos financieros captados de la víctima, el ciberdelincuente realiza transferencias no consentidas de activos y a su vez, la información personal queda vulnerable ante posibles casos de suplantación.

Recomendaciones

- **Evite** dar clic, sobre links o archivos adjuntos en correos electrónicos desconocidos.
- **No** ingrese ningún tipo de información en el formulario mostrado en este sitio web.
- **REPORTE** el enlace con el CAI Virtual a través de la página web: https://caivirtual.policia.gov.co

En caso de ser víctima

- **REPORTE** al banco dicho incidente para que realicen las diligencias de acuerdo a su competencia.
- **CAMBIE** de inmediato la clave de su cuentas donde relacionen información de su entidad bancaria.

Correo allegado

From: Notificacion Importante <andre_berma@hotmail.com>
Date: January 13, 2023 at 1:01:03 PM EST
To: jo[redacted]
Subject: Tienes una nueva notificacion importante

Scotiabank. COLPATRIA

Estimado usuario jo[redacted]

Scotiabank Colpatria le informa que el 13/01/2023 se ha bloqueado preventivamente tu Clave Dinamica por riesgo de seguridad. Activela de inmediato a traves del siguiente formulario de seguridad. Sigue los pasos en la opcion de desbloqueo al ingresar en el boton en el costado inferior derecho e intenta usar tu llave seguridad, inquietudes al?6045109095/018000931987.

Ingresar

Dirección de Investigación Criminal e INTERPOL
Centro Cibernético Policial

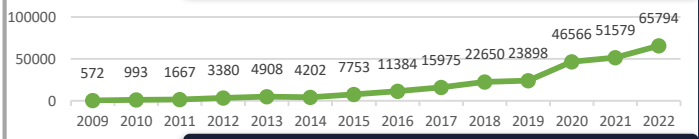
BALANCE SEMANA 2/2023

Balance Cibercriminalidad – Ley 1273/09

	Variación Porcentual	2022	2023	
Hurto por medios informáticos y semejantes	-25%	610	452	
Violación de datos personales	-42%	386	223	
Acceso abusivo a un sistema informático	-37%	325	204	
Suplantación de sitios web	-42%	182	105	
Transferencia no consentida de activos	-46%	96	51	
Interceptación de datos informáticos	-26%	49	36	
Daño informático	-36%	19	12	
Obstaculización ilegítima de sistema informático o red de telecomunicación	-45%	11	6	
Uso de software malicioso	-78%	14	3	
TOTAL	- 35%	1.692	1.092	

Corte del 01 de enero al 14 de enero 2022.
vs 01 de enero al 14 de enero 2023.

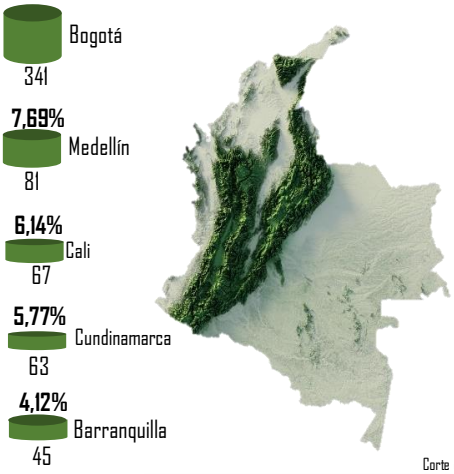
Evolución histórica *(No. Denuncias vs año)*



1,66 %

Ciudades/Departamentos de mayor afectación

(Ciudad y Dpto No. Eventos, %)



- 31,2% Bogotá 341
- 7,69% Medellín 81
- 6,14% Cali 67
- 5,77% Cundinamarca 63
- 4,12% Barranquilla 45
- Cartagena 3,11% 34
- Ibagué 2,38% 26
- Cúcuta 2,11% 23
- Santa Marta 1,65% 18
- Bucaramanga 1,37% 15

Corte del 01 de enero al 14 de enero 2023.

CAPTURAS 2023

Delitos Ley 1273.	7	7 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 — 448

Alertas y contenidos preventivos — 15
05 durante la semana

Muestras de malware analizadas — 62

Actividades de relacionamiento estratégico, resaltando en la semana: — 05

MINTIC · UNIVERSIDAD SERGIO ARBOLEDA · SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA · BOGOTÁ

Mensajes de información intercambiados mediante aplicativo SIENA de EUROPOL — 11

Páginas bloqueadas — 381
Material de abuso sexual infantil 381

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