Dirección de Investigación Criminal e INTERPOL
Centro Cibernético Policial

BALANCE SEMANA 4/2023

Cyber noticias

Los hackers pueden usar GitHub Codespaces para alojar y distribuir malware. Se ha demostrado cómo los actores de amenazas pueden utilizar GitHub Codespaces, implementando plataformas IDE (Entorno de Desarrollo Integrado), que se configuran fácilmente para actuar como un servidor web y distribuir contenido malicioso. **Fuente:** Bleepingcomputer.

Google trabaja en un rastreador inteligente similar a Apple AirTag. Google está trabajando para ampliar su gama de dispositivos conectados mediante la introducción de una nueva etiqueta de **localización inteligente**. El nuevo dispositivo funcionará en una red de seguimiento distribuida similar a **AirTag de Apple y SmartTag de Samsung**. **Fuente:** Gadgets360.

Autoridades cerraron el exchange Bitzlato argumentando que era un "refugio" del ciberdelito. Las autoridades estadounidenses arrestaron el miércoles al fundador de **Bitzlato**, un exchange de criptomonedas considerado como un paraíso financiero para los ciberdelincuentes alineados con Rusia. Estos ciberdelincuentes están involucrados en ataques de ransomware y ventas ilícitas de drogas en la web oscura. **Fuente:** Hackwise.

Mercado ilegal de darknet de Solaris hackeado por su competidor Kraken. Solaris, un gran mercado de darknet centrado en drogas y sustancias ilegales, ha sido pirateado por un competidor más pequeño llamado **'Kraken'** desde el 13 de enero de 2022. El sitio Tor de **Solaris** actualmente redirige a **Kraken,** quien anunció que se habían realizado esta acción gracias a "errores enormes en el código". **Fuente:** Bleepingcomputer.

Modalidad reportada al CAI Virtual ¡APP PRESTAMOS ON-LINE!

En reportes al CAI virtual, se evidenció una modalidad que se caracteriza por realizar **créditos** mediante engaños y posteriormente cobrar excesivas cantidades de dinero.

1 Los supuestos prestamistas ganan la **confianza** de las personas, ofreciendo **préstamos sin requisitos** en redes sociales.

2 Para la **adquisición** del préstamo la víctima debe descargar **una app** de la tienda de aplicaciones, donde debe digitar sus **datos personales.**

3 Dichas apps **solicitan permisos** de acceso a información y funciones del dispositivo y **capturan los datos de la víctima**, como por ejemplo los **contactos**.

4 Una vez entregado el dinero, el prestamista **cambia los acuerdos de pago**, exigiendo cobros exagerados u ofreciendo otros servicios que generan incumplimientos de pago.

5 Ante el incumplimiento del pago, los prestamistas envían **cadenas de mensajes** a los contactos de la víctima **con acusaciones e intimidaciones,** para que los usuarios realicen los pagos exigidos.

RECOMENDACIONES

- **NO** acceda a las exigencias e intimidaciones utilizadas para cobrar.
- **BLOQUEE Y REPORTE** los números de los que le escriben con intimidaciones o amenazas.
- **ALERTE** a sus contactos sobre los posibles mensajes en su contra, indicando que la información es falsa.

EN CASO DE SER VÍCTIMA

- **DESACTIVE** los permisos innecesarios otorgados a las aplicaciones.
- **ELIMINE** el caché de las aplicaciones.
- **REPORTE** cualquier incidente al CAI Virtual a través de la web **https://caivirtual.policia.gov.co**
- **COLOQUE** en conocimiento de la **Superintendencia de Industria y Comercio de Colombia** lo hechos acontecidos con las aplicaciones involucradas a través del siguiente link **https://www.sic.gov.co/atencion-al-ciudadano/canales-de-atencion**

REDES SOCIALES @caivirtual

Instagram facebook. twitter

Dirección de Investigación Criminal e INTERPOL
Centro Cibernético Policial

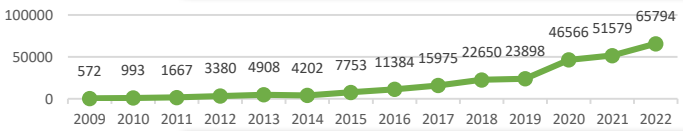
BALANCE SEMANA 4/2023

Balance Cibercriminalidad – Ley 1273/09

Variación Porcentual	2022	2023	
-15%	1.304	1.104	Hurto por medios informáticos y semejantes
-25%	780	588	Violación de datos personales
-28%	669	482	Acceso abusivo a un sistema informático
-29%	356	253	Suplantación de sitios web
-39%	195	119	Transferencia no consentida de activos
-6%	96	90	Interceptación de datos informáticos
-38%	34	21	Daño informático
-44%	32	18	Obstaculización ilegítima de sistema informático o red de telecomunicación
-18%	22	18	Uso de software malicioso
TOTAL - 23%	3.488	2.693	

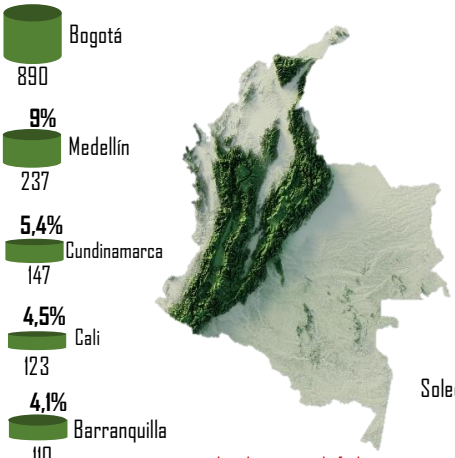
Corte del 01 de enero al 28 de enero 2022. vs 01 de enero al 28 de enero 2023.

Evolución histórica *(No. Denuncias vs año)*



Ciudades/Departamentos de mayor afectación

(Ciudad y Dpto No. Eventos, %)



- Bogotá 33% 890
- Medellín 9% 237
- Cundinamarca 5,4% 147
- Cali 4,5% 123
- Barranquilla 4,1% 110
- Cartagena 3% 170
- Ibagué 2,1% 57
- Cúcuta 2% 50
- Bucaramanga 1,3% 37
- Soledad (Atlántico) 1,2% 34

Las denuncias a la fecha representan el **4,09** del total del 2022.

Corte del 01 de enero al 28 de enero 2023.

CAPTURAS 2023

Delitos Ley 1273.	19
Explotación sexual infantil en Internet.	2

5 Durante la semana

Fuente: SIEDCO Plus

Actividades de gestión en seguridad digital

Incidentes gestionados a través del CAI Virtual: 802

Alertas y contenidos preventivos 12 durante la semana: 35

Muestras de malware analizadas: 64

Actividades de relacionamiento estratégico, resaltando en la semana: 15

Charlas de ciberseguridad Personas impactadas 224: 03

Páginas bloqueadas Material de abuso sexual infantil 2.105: 2.105

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