Dirección de Investigación Criminal e INTERPOL
Centro Cibernético Policial

BALANCE **SEMANA 12/2023**

Cyber noticias

Kaspersky lanza descifrador para ransomware basado en el código fuente de Conti. Conti es un ransomware que ha dominado la escena del cibercrimen desde 2019, cuyos datos, incluido el código fuente, se filtraron en marzo de 2022 tras un conflicto interno provocado por la crisis geopolítica en Europa. Kaspersky lanzó una nueva versión del descifrador público para ayudar a las víctimas de ransomware. **Fuente:** Kaspersky.

Microsoft está probando una billetera criptográfica. Se está trabajando en una billetera criptográfica sin custodia de Ethereum integrada para **Microsoft Edge,** que permitirá a los usuarios enviar y recibir criptomonedas y NFT. Las claves públicas se pueden compartir con otros para recibir pagos, mientras que las claves privadas deben mantenerse en secreto y se pueden usar para autorizar transacciones en criptomonedas. **Fuente:** Bleepingcomputer.

Utilizan el nuevo malware PowerMagic y CommonMagic con fines de espionaje. Cuando los hackers se encuentran dentro de la red, usan complementos para capturar documentos y archivos **(DOC, XLSX, ZIP, RAR, PDF, etc.)**, así como capturas de pantalla cada tres segundos utilizando la API de interfaz de dispositivo gráfico (**GDI**) de Windows. El vector de infección inicial es spear-phishing o un método similar para entregar una URL que apunta a un archivo ZIP con acceso directo malicioso (LNK). **Fuente:** Cyberscoop.

Bill Gates: La Inteligencia Artificial es el avance tecnológico más importante en décadas. Lo llamó tan fundamental como la creación del microprocesador, la computadora personal, Internet y el teléfono móvil. Dijo: "Cambiará la forma en que las personas trabajan, aprenden, viajan, reciben atención médica y se comunican entre sí, las mejoras impulsadas por la **IA** serán especialmente importantes para los países pobres, donde ocurre la gran mayoría de las muertes de menores de 5 años". **Fuente:** Bbc.

¡Phishing AUDITORÍA DE TRANSACCIÓN INUSUAL!

Se ha reportado una campaña de **phishing**, difundiendo el malware **Remcos**, tipo RAT (troyano de acceso remoto). Los ciberdelincuentes lo utilizan para realizar acciones en máquinas infectadas remotamente, como obtener información personal, afectar el patrimonio de las personas y/o ejecutar software malicioso.
Está asociado al asunto: **"AUDITORÍA DE TRANSACCIÓN INUSUAL"**.

1

El correo allegado informa sobre una presunta auditoría por realizar transacciones bancarias de forma inusual.

De: Firma jose <firmajosealbertoescag@gmail.com>
Enviado el: jueves, 9 de marzo de 2023 3:15 p. m.
Asunto: AUDITORIA DE TRANSACCIÓN INUSUAL

Buenas tardes

Cordial Saludo

Enviamos la carta de auditoría por transacciones inusuales a través de nuestros

portales bancarios. verifique la carta enviada

VER CARTA AQUÍ
CÓDIGO DE ACCESO:5580

https://docs.google.com/uc?export=download&id=1UZnMfbELcinAV3R0pGpJmd1yS3WlcL4k

2

Solicita que el destinatario dé clic en el enlace : **"VER CARTA AQUÍ"**, el cual redireccionará a la descarga de un fichero comprimido **.tar**, que requiere un código de acceso que iniciará la ejecución del malware.

3

RECOMENDACIONES

- **EVITE** dar clic, sobre links o archivos adjuntos en correos electrónicos desconocidos y no abra archivos adjuntos.
- **VERIFIQUE** ortografía y redacción, usualmente hay errores.
- **TENGA EN CUENTA**, que ninguna entidad bancaria solicitará información de productos por correos electrónicos.
- **VERIFIQUE** que el remitente del correo corresponda a una entidad real.
- **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, Csirt.Ponal.
- **REALICE** copias de seguridad (**backups**) de su información de manera periódica.
- **REPORTE** el correo allegado con el CAIVirtual a través de la web: https://caivirtual.policia.gov.co

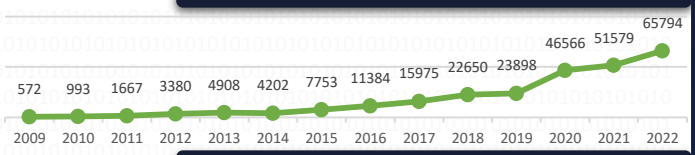
Fuente: Csirt Defensa

Balance Cibercriminalidad – Ley 1273/09

Variación Porcentual	2022	2023	
-6 %	5.045	4.725	Hurto por medios informáticos y semejantes
-12 %	2.509	2.211	Violación de datos personales
-7 %	2.284	2.131	Acceso abusivo a un sistema informático
-19 %	1.097	888	Suplantación de sitios web
-22 %	749	584	Transferencia no consentida de activos
-16 %	321	271	Interceptación de datos informáticos
-12 %	92	81	Daño informático
-29 %	112	80	Obstaculización ilegítima de sistema informático o red de telecomunicación
35 %	55	74	Uso de software malicioso
TOTAL	**- 10 %**	**12.265**	**11.045**

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

Evolución histórica *(No. Denuncias vs año)*



Ciudades/Departamentos de mayor afectación

(Ciudad y Dpto No. Eventos, %)

- Bogotá 29% — 3.169
- Medellín 8% — 926
- Cundinamarca 7% — 807
- Cali 5% — 584
- Barranquilla 4% — 431
- Ibagué 2,1% — 237
- Cartagena 2,1% — 233
- Bucaramanga 1,9% — 211
- Villavicencio 1,7% — 193
- Cúcuta 1,7% — 186

Las denuncias a la fecha representan el **17 %** del total del 2022.
Corte del 01 de enero al 18 de marzo 2023.

CAPTURAS 2023

Delitos Ley 1273.	**56**	**6** Durante la semana
Explotación sexual infantil en Internet.	**13**	

Fuente: SIEDCO Plus

Actividades de gestión en seguridad digital

Incidentes gestionados a través del CAI Virtual — **3.155**

135 — **Alertas y contenidos preventivos** 12 durante la semana

Muestras de malware analizadas — **223**

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

Charlas de ciberseguridad — **31**
Personas impactadas **3.953**

5.568 — **Páginas bloqueadas**
Material de abuso sexual infantil. **5.252**
Juegos ilegales de azar. **316**

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

Canales de atención y redes sociales

Página web — Twitter — Instagram — Facebook — WhatsApp