Dirección de Investigación Criminal e INTERPOL
Centro Cibernético Policial

BALANCE **SEMANA 9/2023**

Cyber noticias

Las víctimas de MortalKombat ahora pueden descifrar sus archivos de forma gratuita. La empresa rumana de ciberseguridad Bitdefender ha lanzado una herramienta de descifrado gratuita para este **ransomware,** una variedad dirigida principalmente a usuarios de criptomonedas. **MortalKombat**, que lleva el nombre de la popular franquicia de videojuegos, fue observado por primera vez por investigadores de Cisco Talos en enero. **Fuente:** Techcrunch.

Entidades de criptomonedas en riesgo: actor de amenazas usa Parallax RAT para la infiltración. ParallaxRAT es un malware que realiza actividades maliciosas como leer credenciales de inicio de sesión, acceder a archivos, registro de teclas y control remoto de escritorio; este se ha distribuido a través de campañas de spam o correos electrónicos de phishing (con archivos adjuntos). **Fuente:** Uptycs.

Presidente Petro pide capacitación a las Fuerzas Militares. Señaló que es importante una preparación "integral", no sólo en el manejo de las armas, si no también en la seguridad que impida entre otras cosas "las caídas de páginas". "Por ejemplo, la ciberseguridad que tratamos de impulsar en el Plan Nacional de Desarrollo, estamos en pañales, las caídas de páginas de información delicada de la Fiscalía, de los mismos organismos de inteligencia, ni más ni menos que se tienen del Estado en cualquier ministerio" **Fuente:** Rcnradio.

Tercera temporada: curso rápido de seguridad "El link del engaño". Tenga cuidado con los mensajes que le pueden llegar a través de su correo electrónico, mensajes de texto o redes sociales en donde le envían un link o le piden que se comunique con un número que allí comparten para que usted verifique una información. Los ciberdelincuentes pueden aprovechar estos medios para engañarlo. Dictado por Policías expertos en estudiar delitos. **Fuente:** Spotify.

Modalidad más reportada al CAI Virtual

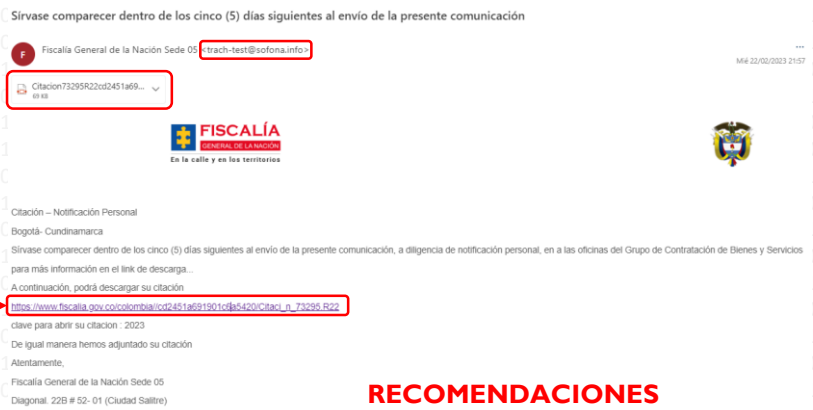
¡FALSA citación de la Fiscalía!

En reportes al CAI virtual se evidenció una campaña de phishing, diseñado por ciberdelincuentes, usando técnicas de ingeniería social que suplantan a autoridades judiciales con el propósito de obtener acceso remoto al sistema con un enlace malicioso y relacionando el siguiente asunto: ***"Sírvase comparecer dentro de los cinco (5) días siguientes al envío de la presente comunicación".***

1. El correo allegado solicita dar clic en el enlace https://gtly.to/50qMckT2.

2. Al dar clic, redireccionará a https://www.mediafire.com/file/ejku39sjw2kxx5y/Citacion73295R22cd2451a691901c6a5420.LHA/file, donde se descargará un PDF con la supuesta citación.

3. Al ejecutar el archivo tipo RAT (remote access trojan), permite al ciberdelincuente tener acceso o control no autorizado del dispositivo.


Sírvase comparecer dentro de los cinco (5) días siguientes al envío de la presente comunicación

Fiscalía General de la Nación Sede 05 <trach-test@sofona.info>

Mié 22/02/2023 21:57

Citacion73295R22cd2451a69...

FISCALÍA GENERAL DE LA NACIÓN
En la calle y en los territorios

Citación – Notificación Personal

Bogotá- Cundinamarca

Sírvase comparecer dentro de los cinco (5) días siguientes al envío de la presente comunicación, a diligencia de notificación personal, en a las oficinas del Grupo de Contratación de Bienes y Servicios para más información en el link de descarga...

A continuación, podrá descargar su citación

https://www.fiscalia.gov.co/colombia/cd2451a691901c6a5420/Citaci_n_73295.R22

clave para abrir su citacion : 2023

De igual manera hemos adjuntado su citación

Atentamente,

Fiscalía General de la Nación Sede 05

Diagonal. 22B # 52- 01 (Ciudad Salitre)

+57 57(1)570 20 00 -57(1)414 90 00

Abierto : Atendemos hasta 5: PM

4.

RECOMENDACIONES

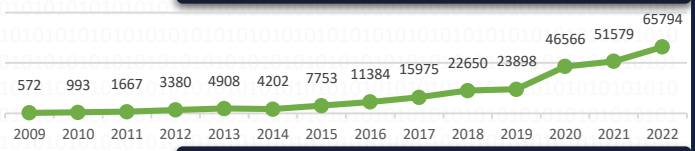
- **No** abra el documento y **EVITE** dar clic sobre links o archivos adjuntos en correos electrónicos desconocidos.
- **VERIFIQUE** ortografía y redacción, usualmente hay errores.
- **VERIFIQUE** que el dominio del correo del remitente corresponda a la Fiscalía General de la Nación o agencias de ley.
- **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.
- **COMUNÍQUESE** directamente con los sitios oficiales de agencias de ley ante cualquier duda.
- **REPORTE** el correo allegado con el CAI Virtual a través de la web: https://caivirtual.policia.gov.co

Balance Cibercriminalidad – Ley 1273/09

Variación Porcentual	2022	2023	
-6 %	3.936	3.683	Hurto por medios informáticos y semejantes
-10 %	1.934	1.733	Violación de datos personales
-7 %	1.767	1.641	Acceso abusivo a un sistema informático
-17 %	888	737	Suplantación de sitios web
-16 %	560	469	Transferencia no consentida de activos
-9 %	244	221	Interceptación de datos informáticos
-27 %	86	63	Daño informático
-17 %	76	63	Obstaculización ilegítima de sistema informático o red de telecomunicación
20 %	45	54	Uso de software malicioso
TOTAL - 9 %	9.537	8.664	

Corte del 01 de enero al 04 de marzo 2022.
vs 01 de enero al 04 de marzo 2023.

Evolución histórica *(No. Denuncias vs año)*



Ciudades/Departamentos de mayor afectación

(Ciudad y Dpto No. Eventos, %)

- Bogotá 31% — 2.598
- Medellín 8% — 718
- Cundinamarca 7% — 594
- Cali 5% — 442
- Barranquilla 4% — 340
- Ibagué 2% — 190
- Cartagena 2% — 172
- Villavicencio 1,7% — 149
- Cúcuta 1,6% — 144
- Bucaramanga 1,5% — 133

Las denuncias a la fecha representan el **13 %** del total del 2022.
Corte del 01 de enero al 04 de marzo 2023.

CAPTURAS 2023

Delitos Ley 1273.	**45**
Explotación sexual infantil en Internet.	**8**

7 Durante la semana

Fuente: SIEDCO Plus

Actividades de gestión en seguridad digital

Incidentes gestionados a través del CAI Virtual — **2.372**

Muestras de malware analizadas — **223**

Charlas de ciberseguridad Personas impactadas **1.732** — **19**

101 — **Alertas y contenidos preventivos** 13 durante la semana

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

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

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