Dirección de Investigación Criminal e INTERPOL
Centro Cibernético Policial

BALANCE **SEMANA 16/2023**

Cyber noticias

Cae en España ciberacosador, quien a través de un videojuego pedía fotos a una niña de 8 años en Colombia. Tras la denuncia en Colombia de la madre de una menor, en la que informó que su hija era acosada sexualmente por un adulto, que la chantajeaba para obtener imágenes sexuales a cambio de recompensas en un videojuego. Según informó la Policía española, la investigación que condujo a la captura del ciberacosador, contó con la colaboración de la Policía Nacional de Colombia. **Fuente:** Bluradio.

Los anuncios de Google impulsan el malware BumbleBee utilizado por bandas de ransomware. El malware Bumblebee es distribuido a través de anuncios de Google y envenenamiento SEO (técnica para obtener una alta clasificación en los motores de búsqueda), promocionando los softwares: **Zoom**, **Cisco AnyConnect**, **ChatGPT** y **Citrix Workspace**. Bumblebee es un cargador de malware utilizado para obtener acceso inicial a las redes y realizar ataques de ransomware. **Fuente:** Bleepingcomputer.

Banco de Venezuela sufre ataque cibernético. Este 19 de abril, varios expertos en el área digital advirtieron que el Banco de Venezuela, que controla el Estado, ha sufrido un ciberataque y recibe la amenaza de publicar información confidencial de sus clientes si no paga. El ataque, no obstante, permite a la web operar con normalidad. La infección se produjo luego que lograran acceder a las computadoras del Banco de Venezuela, a través del ransomware LockBit, que encriptó la data y no permite a la entidad acceder a ella. **Fuente:** NTN

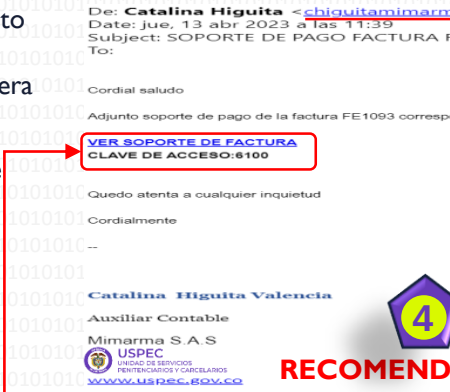
AgentTesla: el malware que está robando datos en Latinoamérica. Un nuevo tipo de malware está atacando a personas en varios países de Latinoamérica con el objetivo de robar contraseñas, tomar capturas de pantalla y enviar la información a los ciberdelincuentes. Los expertos en ciberseguridad han identificado que los atacantes utilizan correos electrónicos falsos, haciéndose pasar por marcas conocidas, y adjuntando archivos ZIP que oculta el virus. **Fuente:** colombia.com.

Modalidad más reportada al CAI Virtual ¡ Phishing !

USPEC UNIDAD DE SERVICIOS PENITENCIARIOS Y CARCELARIOS

A través del servicio de CAI Virtual, se identificó una campaña de **phishing**, difundiendo el malware Remcos tipo RAT (troyano de acceso remoto) y keylogger (registrador de teclas). Los ciberdelincuentes lo utilizan para realizar acciones en dispositivos infectados remotamente, como obtener información personal, realizar seguimiento y registrar cada tecla que se pulsa en una computadora, sin el permiso ni el conocimiento del usuario, afectando el patrimonio, información y datos de las personas; y/o ejecutando software malicioso, asociado al asunto: **"SOPORTE DE PAGO FACTURA FE1093"**.

1. El correo allegado, notifica de un presunto soporte de pago de la factura FE1093 correspondiente a honorarios de la primera quincena del mes de abril.


De: **Catalina Higuita** <chiguitamimarmasas@gmail.com>
Date: jue, 13 abr 2023 a las 11:39
Subject: SOPORTE DE PAGO FACTURA FE1093
To:

Cordial saludo

Adjunto soporte de pago de la factura FE1093 correspondiente a honorarios primera quincena del mes de Abril .

VER SOPORTE DE FACTURA
CLAVE DE ACCESO:6100

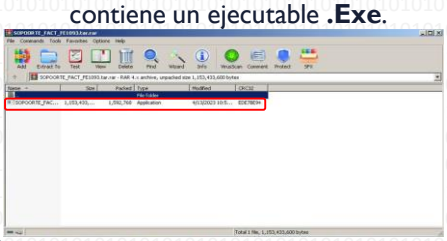
Quedo atenta a cualquier inquietud

Cordialmente

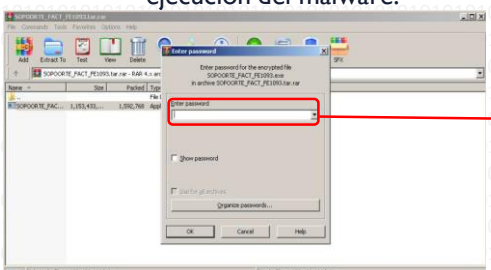
--

Catalina Higuita Valencia
Auxiliar Contable
Mimarma S.A.S
USPEC UNIDAD DE SERVICIOS PENITENCIARIOS Y CARCELARIOS
www.uspec.gov.co

2. Adjuntan un archivo formato **.TAR** que contiene un ejecutable **.Exe**.



3. Solicita que el destinatario ejecute el archivo **.Exe**, y este requiere un código de acceso que iniciará la ejecución del malware.



4. **RECOMENDACIONES**

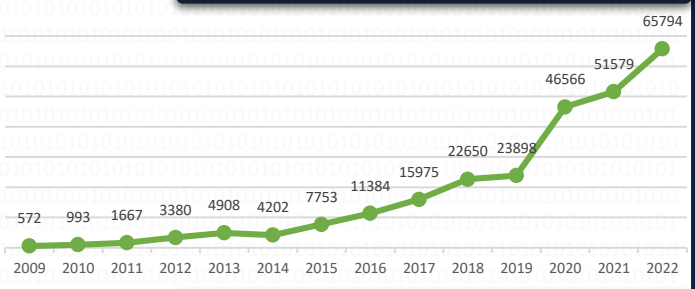
- **EVITE** dar clic sobre links o abrir archivos adjuntos en correos electrónicos desconocidos.
- **VERIFIQUE** ortografía y redacción, usualmente hay errores.
- **TOME CONTACTO**, ante alguna duda en inquietud con la **USPEC**, en el **SERVICO AL CIUDADANO**.
- **VERIFIQUE** que el remitente del correo 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 CAI Virtual a través de la web: https://caivirtual.policia.gov.co

Balance Cibercriminalidad – Ley 1273/09

Variación Porcentual	2022	2023	
2 %	7.447	7.578	Hurto por medios informáticos y semejantes
-8 %	4.043	3.736	Violación de datos personales
-0,6 %	3.637	3.613	Acceso abusivo a un sistema informático
-3 %	1.634	1.577	Suplantación de sitios web
-12 %	1.140	993	Transferencia no consentida de activos
-10 %	548	492	Interceptación de datos informáticos
-3 %	176	170	Daño informático
-1 %	137	135	Obstaculización ilegítima de sistema informático o red de telecomunicación
42 %	85	121	Uso de software malicioso
TOTAL	**- 2,3 %**	18.848	18.415

Corte del 01 de enero al 22 de abril 2022.
vs 01 de enero al 22 de abril 2023.

Evolución histórica *(No. Denuncias vs año)*



Ciudades/Departamentos de mayor afectación

(Ciudad y Dpto No. Eventos, %)

Fuente: SIEDCO Plus 2.0

- **31%** Bogotá 5.694
- **8%** Medellín 1.474
- **7%** Cundinamarca 1.360
- **5%** Cali 949
- **4%** Barranquilla 773
- **2%** Ibagué 371
- **1,9%** Cartagena 350
- **1,69%** Bucaramanga 312
- **1,55%** Cúcuta 285
- **1,52%** Villavicencio 279

Las denuncias a la fecha representan el **28 %** del total del 2022.
Corte del 01 de enero al 22 de abril 2023.

Actividades de gestión en seguridad digital

Capturas
Delitos informáticos. 90
Explotación sexual infantil en Internet. 27
117

Alertas y contenidos preventivos
11 durante la semana
191

Incidentes gestionados
a través del CAI Virtual
5.148

Actividades de relacionamiento estratégico, resaltando en la semana:
66

IATA

Charlas de ciberseguridad
Personas impactadas **5.423**
46

Páginas bloqueadas
Material de abuso sexual infantil. 8.309
Juegos ilegales de azar. 556
8.865

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