Dirección de Investigación Criminal e INTERPOL
Centro Cibernético Policial

BALANCE **SEMANA 1/2023**

Cyber noticias

Los hackers abusan de Google Ads para propagar malware en software legítimo. Los operadores de malware han estado abusando cada vez más de la plataforma Google Ads (**Plataforma de publicidad online de Google**) para propagar malware a usuarios desprevenidos que buscan productos de software populares. Los actores de la amenaza clonan los sitios web oficiales y distribuyen versiones troyanizadas del software cuando los usuarios hacen clic en la descarga. Fuente: Bleepingcomputer.

La banda de Ransomware BlackCat clona sitios webs para filtrar datos robados. Los operadores de Ransomware **ALPHV** se han vuelto creativos con su táctica de extorsión y en al menos un caso, crearon una réplica del sitios web para publicar datos robados en él. Parece que **ALPHV**, también conocido como **BlackCat** Ransomware, es conocido por probar nuevas tácticas de extorsión como una forma de presionar y avergonzar a sus víctimas para que paguen. Fuente: Bleepingcomputer.

Shc Linux malware Instalación de CoinMiner. El equipo de análisis de ASEC, descubrió recientemente que un malware de Linux desarrollado con Shc ha estado instalando un CoinMiner. Se presume que después de una autenticación exitosa a través de un ataque de diccionario en servidores SSH Linux administrados inadecuadamente, se instalaron varios programas maliciosos en el sistema de destino. Entre los descargados se encuentra Shc, XMRig CoinMiner y DDoS IRC Bot. Fuente: Asec.

Espiar llamadas telefónicas a través de vibraciones de altavoces auditivos capturadas por acelerómetro. A medida que los fabricantes de teléfonos inteligentes están mejorando los altavoces auditivos en sus dispositivos, también es más fácil para los actores maliciosos aprovechar un canal lateral particular y escuchar las conversaciones de un usuario específico. Fuente: Securityweek.

BlackCat

¡El Ransomware que amenaza a Colombia!

BlackCat o ALPVH es un grupo reconocido por la criptografía aplicada, la cual no permite atacar el algoritmo utilizado actualmente y será necesario contar con las llaves de los atacantes en caso de querer recuperar la información secuestrada.

Un Ransomware es un software malicioso (**malware**) que **infecta** los dispositivos y **cifra** los archivos del sistema; su propósito es la obtención de un rescate a través de **Bitcoins** a cambio de eliminar la restricción para que el usuario pueda recuperar sus datos.

MÉTODOS DE PROPAGACIÓN

Entre algunas de las formas en que estos programas informáticos se propagan, están:

- Usan correos con enlaces para infectar sistemas, que alguien en la organización afectada abre engañosamente.
- Al visitar sitios web de dudosa reputación.
- Al conectar dispositivos USB infectados con este software.

Características

- Uso de software legítimo para acceder a las organizaciones y tomar control del mayor número de sistemas a su alcance.
- Configura archivos de encriptación para múltiples sistemas operativos que permiten generar un mayor impacto a las organizaciones afectadas.
- Incluyen una herramienta identificada como **ExMatter**, la cual ha sido desarrollada para extraer información usando mecanismos de división de grandes volúmenes de datos en piezas más pequeñas, que tratan de simular tráfico de navegación y pueden evadir los controles de monitoreo.

RECOMENDACIONES

- ❑ **Evite** dar clic, sobre links o archivos adjuntos en correos electrónicos desconocidos.
- ❑ **Realice** copias de seguridad de datos con regularidad y protéjalas con contraseña.
- ❑ **Cree** un air gap (desconectar los dispositivos de la red), ya que es una forma efectiva de preservar los datos de los daños ante un ataque Ransomware.
- ❑ **Requiera** credenciales de administrador para instalar el software.
- ❑ **Evite** ingresar a sitios web de dudosa reputación o contenido censurado.
- ❑ **Verifique** los correos, ejecutando los enlaces o archivos en un entorno **sanbox.**
- ❑ **Utilice** la autenticación multifactor cuando sea posible.
- ❑ **REPORTE** cualquier incidente al CAI Virtual a través de la web https://caivirtual.policia.gov.co

REDES SOCIALES @caivirtual

Instagram facebook twitter

Dirección de Investigación Criminal e INTERPOL
Centro Cibernético Policial

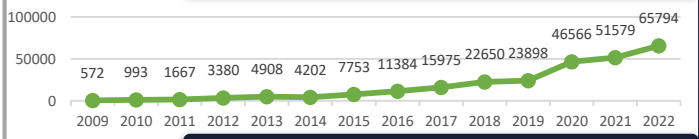
BALANCE SEMANA 1/2023

Balance Cibercriminalidad – Ley 1273/09

	Variación Porcentual	2022	2023	
Hurto por medios informáticos y semejantes	-40%	285	171	
Violación de datos personales	-58%	191	80	
Acceso abusivo a un sistema informático	-56%	171	74	
Suplantación de sitios web	-52%	75	36	
Transferencia no consentida de activos	-42%	47	27	
Interceptación de datos informáticos	-48%	25	13	
Daño informático	-66%	9	3	
Uso de software malicioso	-87%	8	1	
Obstaculización ilegítima de sistema informático o red de telecomunicación	-75%	4	1	
TOTAL	**- 50%**	**807**	**406**	

Corte del 01 de enero al 07 de enero 2022.
vs 01 de enero al 07 de enero 2023.

Evolución histórica *(No. Denuncias vs año)*



0,63 %

Ciudades/Departamentos de mayor afectación

(Ciudad y Dpto No. Eventos, %)

- Bogotá: 29% — 140
- Medellín: 8,37% — 34
- Cali: 6,16% — 25
- Cundinamarca: 4,43% — 18
- Barranquilla: 3,94% — 16

- Cartagena: 2,46% — 10
- Santa Marta: 2,46% — 10
- Ibagué: 1,72% — 7
- Cúcuta: 1,72% — 7
- Pasto: 1,72% — 6

Corte del 01 de enero al 07 de enero 2023.

CAPTURAS 2023

Delitos Ley 1273.	0
Explotación sexual infantil en Internet.	2

Fuente: SIEDCO Plus

Actividades de gestión en seguridad digital

Incidentes gestionados a través del CAI Virtual — 212

Alertas y contenidos preventivos — 10
10 durante la semana

Muestras de malware analizadas — 61

Actividades de relacionamiento estratégico, resaltando en la semana: — 02

BINANCE WOM

Operaciones proyectadas — 15

Divididas así:

Nivel desconcentrado	7
CECIP	8

Páginas bloqueadas — 16

Material de abuso sexual infantil	16
Juegos Ilegales de Azar	0

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