Dirección de Investigación Criminal e INTERPOL
Centro Cibernético Policial

BALANCE **SEMANA 19/2023**

Cyber noticias

Nuevo ransomware CACTUS que explota vulnerabilidades en dispositivos VPN para infectar redes. Investigadores de ciberseguridad han identificado una nueva variante de ransomware que está explotando vulnerabilidades conocidas en las VPN (Virtual Private Network) con el fin de obtener acceso a las redes de las víctimas. Lo que destaca esta nueva variante de ransomware es su capacidad de cifrarse a sí misma para evitar ser detectada por herramientas de seguridad y monitorización de redes. **Fuente:** Derechodelared.

Twitter dejará hacer videollamadas y habrá cambios en mensajes y reacciones. El empresario y actual CEO de la red social no ocultó su intención de convertir la plataforma en una **"súper aplicación"** donde se pueda hacer de todo y es por ello que se está trabajando en la inclusión de nuevas características. **Elon Musk** afirmó que los usuarios podrán comunicarse sin necesidad de compartir su número de teléfono y aseguró que se incorporarán dos funciones nuevas como la posibilidad de hacer llamadas de video y voz desde la aplicación. **Fuente:** Infobae.

El autor intelectual detrás del hackeo de Twitter 2020 se declaró culpable y enfrentará hasta 70 años de prisión. Joseph James O'Connor, quien usaba el alias de **PlugwalkJoe**, admitió "su papel en el acoso cibernético incluyendo el hackeo de Twitter en julio de 2020". El individuo de 23 años fue extraditado desde España el 26 de abril después de que la Audiencia Nacional española aprobara en febrero la solicitud del Departamento de Justicia de entregar a O'Connor, quien enfrentará 14 cargos penales en EE. UU **Fuente:** Thehackernews.

Aumentan los actores de amenazas que utilizan videos de YouTube generados por IA. YouTube ha sido usado como señuelo para compartir enlaces de malware. Los videos atraen a los usuarios haciéndose pasar por tutoriales sobre cómo descargar versiones de softwares como Photoshop, Premiere Pro, Autodesk 3ds Max, AutoCAD y otros productos con licencia disponibles solo para usuarios con suscripción, con el fin de recopilar datos confidenciales como tarjetas de crédito, información del sistema, ubicación, etc. **Fuente:** Cloudsek.

FALSA ACTUALIZACIÓN DEL SISTEMA OPERATIVO WINDOWS EJECUTA MALWARE AURORA

La campaña maliciosa consiste en mostrar una animación de pantalla completa simulando una actualización de seguridad de Windows, que evade los sistemas de seguridad del dispositivo. **Aurora** es un malware de captura de datos que los ciberdelincuentes utilizan para obtener información confidencial de los navegadores, aplicaciones de criptomonedas, discos y ejecutar software malicioso.

1. Una campaña maliciosa redirige a los usuarios a una presunta actualización de seguridad de Windows.

Figura 1: Ventana del navegador que se muestra en pantalla completa simulando la actualización del sistema.

2. Invita al usuario a descargar el archivo de actualización llamado **ChromeUpdate.exe.**

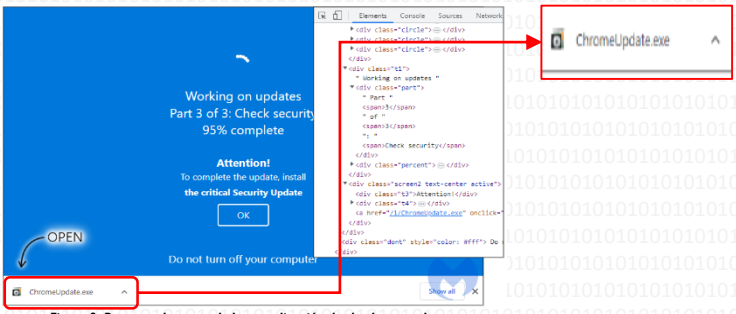


Figura 2: Presunta descarga de la actualización desde el navegador.

RECOMENDACIONES

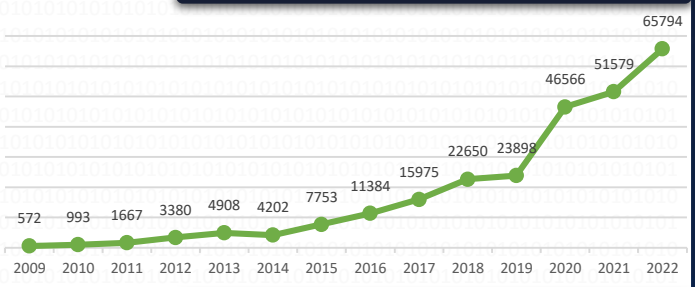
- **EVITE** dar clic sobre links o abrir archivos ejecutables desconocidos.
- **VERIFIQUE** ortografía y redacción, usualmente hay errores.
- **PROTEJA** su dispositivo instalando un antivirus.
- **No** de clic en el primer resultado de búsqueda del navegador.
- **CUIDADO,** los ciberdelincuentes utilizan anuncios maliciosos en sitios web del navegador para instalar software malicioso.
- **REQUIERA** credenciales de administrador para instalar el software o actualizaciones del sistema.
- **REALICE** copias de seguridad (**backups**) de la información de manera periódica.
- **ACTUALICE** desde el sitio oficial de Microsoft o manualmente así: Inicio > Configuración > Actualización y seguridad > Windows Update y luego elige **buscar actualizaciones**.
- **REPORTE** el correo electrónico allegado a través del canal de atención del CAI Virtual **https://caivirtual.policia.gov.co**.

Balance Cibercriminalidad – Ley 1273/09

Variación Porcentual	2022	2023	
5 %	8.800	9.290	Hurto por medios informáticos y semejantes
-7 %	4.878	4.512	Violación de datos personales
-4 %	4.590	4.389	Acceso abusivo a un sistema informático
-3 %	1.971	1.901	Suplantación de sitios web
-7 %	1.348	1.243	Transferencia no consentida de activos
2 %	671	689	Interceptación de datos informáticos
-1 %	211	208	Daño informático
63 %	103	168	Uso de software malicioso
-8 %	162	148	Obstaculización ilegítima de sistema informático o red de telecomunicación
TOTAL - 0,8 %	22.735	22.548	

Corte del 01 de enero al 13 de mayo2022.
vs 01 de enero al 13 de mayo 2023.

Evolución histórica (No. Denuncias vs año)



Ciudades/Departamentos de mayor afectación

(Ciudad y Dpto No. Eventos, %)

Fuente: SIEDCO Plus 2.0

Las denuncias a la fecha representan el **34 %** del total del 2022.
Corte del 01 de enero al 13de mayo 2023.

Actividades de gestión en seguridad digital

Capturas
Delitos informáticos. 98
Explotación sexual infantil en Internet. 30
128

231
Alertas y contenidos preventivos
21 durante la semana

Incidentes gestionados
a través del CAI Virtual
5.375

72
Actividades de relacionamiento estratégico, resaltando en la semana:
Universidad de los Andes
Grupo Bancolombia

Charlas de ciberseguridad
Personas impactadas **6.341**
52

10.663
Páginas bloqueadas
Material de abuso sexual infantil. 10.107
Juegos ilegales de azar. 556

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