Dirección de Investigación Criminal e INTERPOL
Centro Cibernético Policial

BALANCE **SEMANA 10/2023**

Cyber noticias

Los ataques de malware de Emotet regresan después de un descanso de tres meses. Emotet es un malware distribuido a través de correo electrónico que contiene archivos maliciosos de documentos de Microsoft Word y Excel. Cuando abren estos documentos y las macros están habilitadas, la DLL de **Emotet** se descargará y ejecutará en la memoria. El malware se sentará en silencio, esperando instrucciones de un servidor de comando y control remoto. **Fuente:** Bleepingcomputer.

Hackers que usan Final Cut Pro pirateado para instalar criptomineros en dispositivos Apple. Hackers están utilizando versiones pirateadas del software de edición de video **Final Cut Pro** para instalar software malicioso de criptominería en dispositivos Apple. El malware disfrazado o incrustado dentro de aplicaciones pirateadas ha sido un problema desde los primeros días de la piratería de software, dijo Jaron Bradley, gerente senior de detecciones de MacOS. **Fuente:** Therecord.

El FBI y el Pentágono ayudaron a investigar el reconocimiento facial para cámaras callejeras y drones. El FBI y el Departamento de Defensa participaron activamente en la investigación y el desarrollo de software de reconocimiento facial que esperaban pudiera usarse para identificar a las personas a partir de imágenes de video. Este procesaría de manera rápida y precisa las "imágenes faciales verdaderamente sin restricciones" grabadas por cámaras de vigilancia en lugares públicos, incluidas estaciones de metro. **Fuente:** Washingtonpost.

Desafíos de la ciberseguridad ¿Cómo combatirlos riesgos cibernéticos? Las empresas, los gobiernos y las personas del común son cada vez más conscientes de los riesgos cibernéticos a los que se enfrentan y están más dispuestos a abordarlos. En ese sentido, afrontar las causas estructurales, a la mayor brevedad, permitirá, si no es demasiado tarde, hacerle frente a un fenómeno que afectará a toda la población por igual. **Fuente:** Caracol.

Modalidad más reportada al CAI Virtual

¡USO DE PLATAFORMA *REPLIT* POR CIBERDELINCUENTES!

En reportes al CAI virtual se han evidenciado campañas de Phishing e Email Spoofing, donde los enlaces maliciosos adjuntados tienen como finalidad afectar el patrimonio de las personas, esto utilizando técnicas de ingeniería social con el fin de tener mayor impacto en sus víctimas. Lo anterior relacionado con URL`s con el dominio **repl.co** **(dominio de la plataforma REPLIT).**

REPLIT

Replit es una plataforma online donde se puede editar y ejecutar código Javascript de una manera rápida y segura. Los ciberdelincuentes usan esta plataforma para no tener que configurar y preparar un entorno de desarrollo y mucho menos tener que pagar un dominio.

RECOMENDACIONES

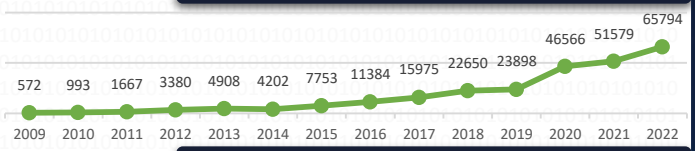
- **EVITE** dar clic sobre links o archivos adjuntos en correos electrónicos desconocidos.
- **VERIFIQUE** que la dirección del enlace sea la misma que la dirección de la URL, los ciberdelincuentes suelen camuflar la URL original.
- **VERIFIQUE** ortografía y redacción, usualmente hay errores.
- **VERIFIQUE** que la dirección del remitente corresponda a quien envía dicho correo.
- **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	
-9 %	4.675	4.275	Hurto por medios informáticos y semejantes
-10 %	2.229	1.999	Violación de datos personales
-7 %	2.067	1.930	Acceso abusivo a un sistema informático
-17 %	996	831	Suplantación de sitios web
-20 %	678	541	Transferencia no consentida de activos
-15 %	286	242	Interceptación de datos informáticos
-16 %	86	72	Daño informático
-35 %	104	68	Obstaculización ilegítima de sistema informático o red de telecomunicación
35 %	48	65	Uso de software malicioso
TOTAL	**- 10 %**	11.169	10.023

Corte del 01 de enero al 11 de marzo 2022.
vs 01 de enero al 11 de marzo 2023.

Evolución histórica *(No. Denuncias vs año)*



Ciudades/Departamentos de mayor afectación

(Ciudad y Dpto No. Eventos, %)

- Bogotá: 29% — 2.925
- Medellín: 8% — 842
- Cundinamarca: 7% — 717
- Cali: 5% — 525
- Barranquilla: 4% — 397
- Ibagué: 2% — 215
- Cartagena: 2% — 206
- Bucaramanga: 1,7% — 178
- Villavicencio: 1,7% — 175
- Cúcuta: 1,6% — 164

Las denuncias a la fecha representan el **15 %** del total del 2022.
Corte del 01 de enero al 11 de marzo 2023.

CAPTURAS 2023

Delitos Ley 1273.	**50**	**5** 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 — **2.722**

111 — **Alertas y contenidos preventivos** 10 durante la semana

Muestras de malware analizadas — **223**

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

Charlas de ciberseguridad Personas impactadas **3.032** — **24**

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