Dirección de Investigación Criminal e INTERPOL
Centro Cibernético Policial

BALANCE **SEMANA 29/2023**

Cyber noticias

Grupo «Charming Kitten» lanza una nueva campaña de malware a sistemas macOS. Investigadores de seguridad identificaron una nueva campaña de malware atribuida al grupo APT *"Charming Kitten"*, en la cual utilizaron un malware denominado *"NokNok"* para atacar sistemas operativos macOS. Esta campaña comenzó en mayo y emplea una cadena de infección distinta a la observada anteriormente. En lugar de utilizar los habituales documentos de Word, con actividad maliciosa en ataques anteriores, ahora emplean archivos LNK para desplegar payloads. **Fuente:** Uad.

Los ciberdelincuentes aprovechan las vulnerabilidades de Microsoft Word para implementar el malware LokiBot. *"LokiBot"*, es un troyano activo de el año 2015. Está dirigido principalmente a los sistemas operativos Windows y tiene como objetivo recopilar información confidencial de las máquinas infectadas, a través de documentos de Word explotan fallas de ejecución remota de código, utilizando señuelos de phishing para colocar el malware en los sistemas comprometidos. **Fuente:** Thehackernews.

CISA comparte herramientas gratuitas para ayudar a proteger los datos en la nube. La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA), ha compartido una hoja informativa que proporciona detalles sobre herramientas gratuitas y orientación, para proteger los activos digitales después de cambiar a la nube desde entornos locales, estas herramientas ayudan a analistas de respuesta a incidentes y profesionales de ciberseguridad a mitigar el riesgo de robo y exposición de información, así como el cifrado de datos. **Fuente:** Bleepingcomputer.

Vulnerabilidad CVE-2023-36884, afecta a productos de Microsoft Windows y Office. Un actor malicioso, podría crear un documento de Microsoft Office especialmente diseñado para realizar la ejecución remota de código (RCE) sobre el sistema de la victima. Sin embargo, el atacante tendría que realizar procesos de ingeniería social a la víctima, para convencerla de que abra el archivo malicioso. Ante esta situación, Microsoft proporcionará una actualización de seguridad y una serie de pasos para reducir los riesgos de vulneración en los sistemas informáticos. Fuente: Microsoft.

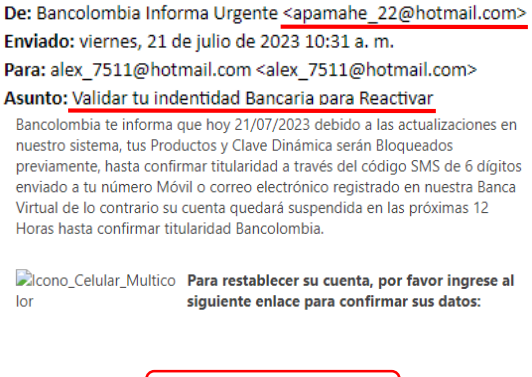
Modalidad más reportada al CAI Virtual ¡Phishing!

A través de reportes allegados al servicio CAI Virtual, se evidenció una campaña de phishing vía correo electrónico, la cual mediante la modalidad de suplantación de sitios web, informan a la ciudadanía sobre un falso bloqueo de productos financieros. El objetivo de esta campaña, es realizar la captura de credenciales de acceso a los servicios financieros y la transferencia no consentida de activos.
Este correo está asociado al asunto: **"VALIDAR TU IDENTIDAD BANCARIA PARA REACTIVAR"**

1. El correo adjunto, solicita al usuario que para reactivar presuntamente su cuenta bancaria, deber dar clic en **"actulizadnamica.vatserve[.]com"**.

2. Al dar clic al enlace, es remitido a un sitio web, simulando ser el portal de acceso a la plataforma financiera.

3. Después, le solicitará a la persona digitar las credenciales de acceso de la cuenta en la presunta plataforma y dar por terminada la fase de captura de datos financieros.



4. **RECOMENDACIONES**

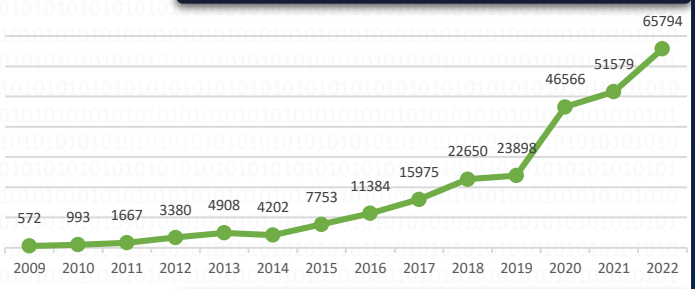
- **EVITE** dar clic sobre links o abrir archivos adjuntos en correos electrónicos desconocidos.
- **VERIFIQUE** ortografía y redacción, usualmente hay errores.
- **VERIFIQUE** que el remitente del correo electrónico, corresponda a una entidad bancaria.
- **No** ingrese ningún tipo de información en el formulario mostrado en este sitio web.
- **CONTACTESE** con la identidad financiera ante cualquier duda
- **VERIFIQUE** los enlaces o archivos antes de ejecutarlos en un entorno de prueba (sandbox), **Ej:**Any.Run, Csirt.Ponal.
- **REPORTE** el correo electrónico allegado, a través de nuestro canal de

Balance Cibercriminalidad – Ley 1273/09

Variación Porcentual	2022	2023	
3 %	13.591	13.963	Hurto por medios informáticos y semejantes
-14 %	7.229	6.093	Acceso abusivo a un sistema informático
-21 %	7.156	5.648	Violación de datos personales
-19 %	2.793	2.266	Suplantación de sitios web
-8 %	1.962	1.803	Transferencia no consentida de activos
-8 %	971	895	Interceptación de datos informáticos
-16 %	305	256	Daño informático
26 %	166	210	Uso de software malicioso
-11 %	215	190	Obstaculización ilegítima de sistema informático o red de telecomunicación
TOTAL	**- 8,91 %**	34.389	31.324

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

Evolución histórica *(No. Denuncias vs año)*



Ciudades/Departamentos de mayor afectación

(Ciudad y Dpto No. Eventos, %)

Fuente: SIEDCO Plus 2.0

- Bogotá: 32% — 10.045
- Medellín: 8% — 2.515
- Cundinamarca: 7,6% — 2.377
- Cali: 5,5% — 1.710
- Barranquilla: 3% — 929
- Ibagué: 2% — 651
- Bucaramanga: 1,9% — 585
- Cartagena: 1,84% — 576
- Villavicencio: 1,76% — 551
- Santa Marta: 1,63% — 511

Las denuncias a la fecha representan el **47%** del total del 2022.
Corte del 01 de enero al 22 de julio 2023.

Actividades de gestión en seguridad digital

Capturas
Delitos informáticos. 134
Explotación sexual infantil en Internet. 40
174

368
Alertas y contenidos preventivos
12 durante la semana

Incidentes gestionados
a través del CAI Virtual
8.749

125
Actividades de relacionamiento estratégico, resaltando en la semana:
Cámara de Comercio de Bogota

Charlas de ciberseguridad
Personas impactadas **10.232**
87

16.401
Páginas bloqueadas
Material de abuso sexual infantil. 15.262
Juegos ilegales de azar. 1.139

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 | Threads | WhatsApp