Dirección de Investigación Criminal e INTERPOL
Centro Cibernético Policial

BALANCE **SEMANA 17/2023**

Cyber noticias

La Guardia Civil de España alerta sobre una nueva estafa vía WhatsApp. Los ciberdelincuentes están suplantando el Grupo de Delitos Telemáticos (GDT), con la intención de convencer a los usuarios que requieren su colaboración para desarticular bandas cibercriminales. Esto es un ataque de Smishing, el cual corresponde al envío masivo de SMS o de WhatsApp, simulando ser una entidad legítima con el objetivo de capturar datos personales, distribuir malware o estafar. **Fuente:** Escudodigital

Google agregará cifrado de extremo a extremo a *"Google Authenticator"*. Esta semana, Google Authenticator finalmente obtuvo una función muy esperada, la capacidad de respaldar tokens de autenticación de dos factores (2FA) en la nube. Esta nueva función permite a los usuarios sincronizar sus tokens 2FA de Google Authenticator con su cuenta, proporcionando respaldo en caso de pérdida o daño de su dispositivo móvil. **Fuente:** Bleepingcomputer

La nueva campaña del troyano bancario QBot, secuestra correos electrónicos comerciales para propagar malware. Expertos de Kaspersky, han descubierto una campaña masiva de correo electrónico, que envía mensajes con archivos PDF maliciosos adjuntos. Estos correos electrónicos, intentan convencer a las víctimas para que abra el archivo y lo haga pasar por una declaración de gastos o cualquier otro documento corporativo que requiera algún tipo de respuesta rápida.
Fuente: Kaspersky

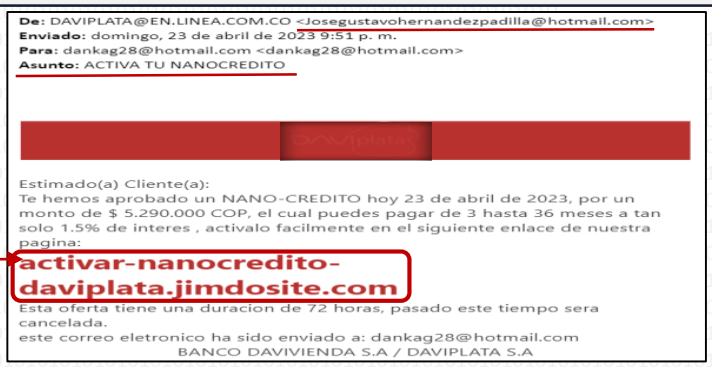
Falso sitio de Le Qoc Sportif en los primeros resultados de Google. Estafadores lograron posicionar un sitio web falso dirigido a usuarios argentinos en el primer resultado de búsqueda de Google, haciéndose pasar por la tienda oficial de Le Qoc Sportif para capturar datos de tarjetas de pago. Los ciberdelincuentes, suelen utilizar Google Ads para clasificar los sitios web falsos en los resultados de los motores de búsqueda para determinadas palabras claves. **Fuente:** ESET

Modalidad más reportada al CAI Virtual ¡ Phishing!

A través del servicio de CAI Virtual, se identificó una campaña de **phishing** vía correo electrónico, la cual busca evadir los sistemas de seguridad de detección y análisis, difundiendo una falsa aprobación de un NANO-CREDITO por parte de la entidad bancaria, con el objetivo de realizar la captura de credenciales de acceso a los servicios financieros y posteriormente la transferencia no consentida de activos. Este correo esta asociado al asunto: **"ACTIVA TU NANOCREDITO"**.

1. El correo allegado, notifica de una presunta aprobación de un NANO-CREDITO (crédito de bajo monto a través del aplicativo móvil).

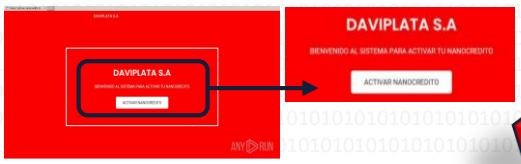
2. Solicita acceder al enlace : "**activar-nanocredito-daviplata.jimdosite.com**", que redireccionará a un sitio web, sugiriendo dar clic en el botón "ACTIVAR NANOCREDITO".


De: DAVIPLATA@EN.LINEA.COM.CO <Josegustavohernandezpadilla@hotmail.com>
Enviado: domingo, 23 de abril de 2023 9:51 p. m.
Para: dankag28@hotmail.com <dankag28@hotmail.com>
Asunto: ACTIVA TU NANOCREDITO

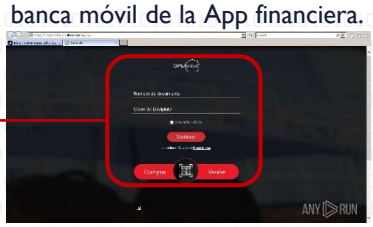
Estimado(a) Cliente(a):
Te hemos aprobado un NANO-CREDITO hoy 23 de abril de 2023, por un monto de $ 5.290.000 COP, el cual puedes pagar de 3 hasta 36 meses a tan solo 1.5% de interes , activalo facilmente en el siguiente enlace de nuestra pagina:

activar-nanocredito-daviplata.jimdosite.com

Esta oferta tiene una duracion de 72 horas, pasado este tiempo sera cancelada.
este correo eletronico ha sido enviado a: dankag28@hotmail.com
BANCO DAVIVIENDA S.A / DAVIPLATA S.A



3. Después de acceder al enlace "ACTIVAR NANOCREDITO" es remitido a un sitio web simulando ser la banca móvil de la App financiera.



En este sitio web, solicitan al usuario el inicio de sesión de la cuenta.

4. **RECOMENDACIONES**

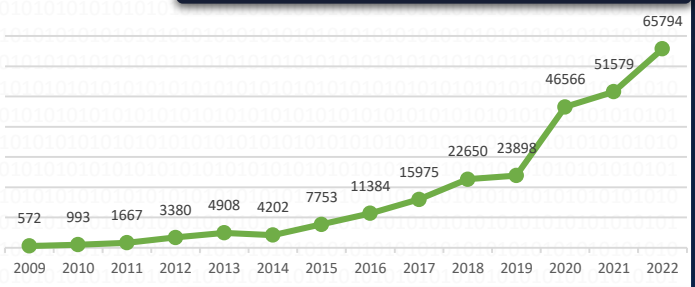
- **EVITE** dar clic sobre links o abrir archivos adjuntos en correos electrónicos desconocidos.
- **VERIFIQUE** ortografía y redacción, usualmente hay errores.
- **VERIFIQUE** que el remitente del correo electrónico, corresponda a una entidad bancaria.
- **No** ingrese ningún tipo de información en el formulario mostrado en este sitio web.
- **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 atención del CAI Virtual https://caivirtual.policia.gov.co.

Balance Cibercriminalidad – Ley 1273/09

Variación Porcentual	2022	2023	
-0,04 %	7.933	7.930	Hurto por medios informáticos y semejantes
-9,7 %	4.345	3.922	Violación de datos personales
-4,7 %	3.965	3.776	Acceso abusivo a un sistema informático
-6,1 %	1.746	1.639	Suplantación de sitios web
-14 %	1.213	1.036	Transferencia no consentida de activos
-11 %	590	524	Interceptación de datos informáticos
-1 %	185	183	Daño informático
-7,4 %	147	136	Obstaculización ilegítima de sistema informático o red de telecomunicación
40 %	93	131	Uso de software malicioso
TOTAL	**- 4,6 %**	20.217	19.277

Corte del 01 de enero al 29 de abril 2022.
vs 01 de enero al 29 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 5.944
- **8%** Medellín 1.572
- **7,45%** Cundinamarca 1,436
- **5%** Cali 989
- **4%** Barranquilla 813
- **2%** Ibagué 393
- Cartagena **1,85%** 357
- Bucaramanga **1,69%** 325
- Cúcuta **1,53%** 296
- Villavicencio **1,51%** 292

Las denuncias a la fecha representan el **29 %** del total del 2022.
Corte del 01 de enero al 29 de abril 2023.

Actividades de gestión en seguridad digital

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

202
Alertas y contenidos preventivos
11 durante la semana

Incidentes gestionados
a través del CAI Virtual
5.218

66
Actividades de relacionamiento estratégico, resaltando en la semana:
IATA

Charlas de ciberseguridad
Personas impactadas **5.451**
47

9.354
Páginas bloqueadas
Material de abuso sexual infantil. **8.798**
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

https://wa.me/message/PE3YLMYPOMFOE1