	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 143		Fecha: 19-06-2023
Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ		
Nombre de la alerta	Suplantación de la identidad del sitio web de la red social Instagram		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G02
Clasificación temática familia	Fraude		

Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo una campaña de Phishing, a través de diferentes navegadores web, quienes vienen suplantando la identidad del sitio de la red social “Instagram”, el cual tiene como finalidad robar información sensible de las víctimas como usuario, correo electrónico y/o contraseña.

2. Proceso de estafa de Phishing:



3. Comparación del sitio web oficial y fraudulento.



- a) Existe una diferencia debido a que el dominio de sitio web fraudulento no coincide con el oficial.
- b) Ambos sitios webs, poseen el **PROTOCOLO SEGURO DE TRANSFERENCIA DE HIPERTEXTO** (HTTPS), lo que hace más convincente a que las víctimas accedan a dicho sitio web.

4. Proveedores de seguridad informática alertan como **SUPLANTACIÓN DE IDENTIDAD - PHISHING.**

alphaMountain.ai	⚠ Suplantación de identidad	BitDefender	⚠ Malware
CRDF	⚠ Malicioso	CyRadar	⚠ Malicioso
Emsisoft	⚠ Suplantación de identidad	ESET	⚠ Suplantación de identidad
Fortinet	⚠ Malware	G-datos	⚠ Malware
Navegación segura de Google	⚠ Suplantación de identidad	kaspersky	⚠ Suplantación de identidad
Leonico	⚠ Suplantación de identidad	netcraft	⚠ Malicioso
Búsqueda segura	⚠ Malicioso	Sophos	⚠ Suplantación de identidad
raíz web	⚠ Malicioso	Abusix	✅ Limpio

5. Indicadores de compromiso (IoC)

a) URL : http://instagram99083[.]iwowjsndns[.]cfd/vhsfhqpdhdsih6/



Clasificación de riesgo de Netcraft 10/10

Lenguaje primario Inglés

b) DOMINIO : whatsstore[.]click



Prueba	
❌	Registro DMARC publicado
❌	Registro DNS publicado
⚠	Política DMARC no habilitada

c) SHA-256 : 181e9141bddb14bc8e7ebca56dd26d2be876a56e92165d6e0126e74d1bde3a1f



información en vivo

Navegación segura de Google: ⚠ Malicioso para [freefire87499.iwowjsndns.cfd](#)

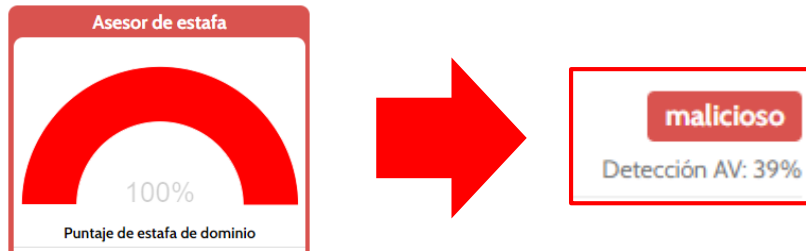
Registro DNS A actual: 188.114.97.3 (AS13335 - CLOUDFLARENET, EE. UU.)

d) IP : 172[.]67[.]129[.]129



Propietario de bloque de red	Cloudflare, Inc.
Compañía anfitriona	Llamada de la nube
país anfitrión	A NOSOTROS 🔗
dirección IPv4	172.67.129.129 (VirusTotal 🔗)
Sistemas autónomos IPv4	AS13335 🔗
dirección IPv6	2606:4700:3033:0:0:ac43:8181
Sistemas autónomos IPv6	AS13335 🔗
DNS inverso	desconocido

6. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD** en siete (07), **MALICIOSA** en cinco (05) y **MALWARE** tres (03) de ellas- – **PHISHING:**



7. Cómo funciona el Phishing:

- a) Los correos electrónicos incluyen enlaces a sitios web preparados por los ciberdelincuentes en los que solicitan información personal.
- b) Medios de propagación del Phishing: WhatsApp, telegram, redes sociales, SMS entre otros.
- c) Los ciberdelincuentes intentan suplantar a una entidad legítima (organismo público o privado, entidad financiera, servicio técnico, etc.)

8. Referencia:

- a) Phishing o suplantación de identidad: Es un método que los ciberdelincuentes, utilizan para engañar a los usuarios para conseguir que revele información personal, como contraseñas, datos de tarjetas de créditos, números de cuentas bancarias, entre otros.

9. Concepto de Instagram:

- a) Es una aplicación y red social de origen estadounidense, propiedad de Meta. Creada por Kevin Systrom y Mike Krieger, fue lanzada el 6 de octubre de 2010. Ganó rápidamente popularidad, llegando a tener más de 100 millones de usuarios activos en abril de 2012 y más de 300 millones en diciembre de 2014. Instagram sirve para subir las fotos desde nuestro teléfono móvil para que todos nuestros seguidores puedan verlas, comentarlas o dar un “me gusta”.

10. Algunas Recomendaciones:

- a) Mantener instalado un servicio de antivirus en el dispositivo.
- b) Verificar la información del sitio web correspondiente.
- c) Acceder al sitio web a través de fuentes oficiales.
- d) No abrir enlaces de dudosa procedencia.
- e) No seguir indicaciones de sitios web fraudulentos.
- f) No compartir la información con terceras personas, amigos o familiares.