

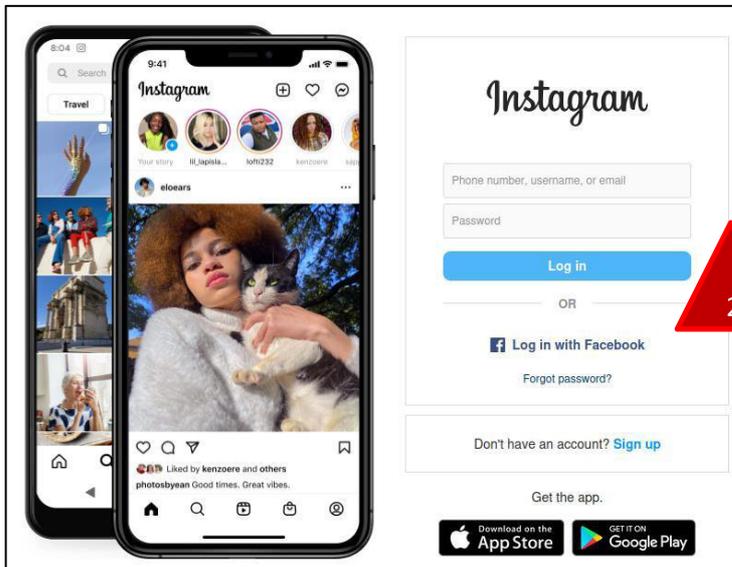
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 069	Fecha: 21-03-2023
		Página 26 de 29
Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ	
Nombre de la alerta	Suplantación de la identidad del sitio web de la red social Instagram	
Tipo de ataque	Phishing	Abreviatura Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros	
Código de familia	G	Código de subfamilia 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. Detalles del proceso de Phishing.



Solicitan a las posibles víctimas a ingreses las credenciales de inicio de sesión.



Al continuar con el proceso, redirige de manera automática al sitio web oficial, toda vez que los ciberdelincuentes ya se apoderaron de la información ingresada.

3. Comparación del sitio web oficial y fraudulento.



- Existe una diferencia debido a que el dominio de sitio web fraudulento no coincide con el oficial.
- 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	Avira	! Suplantación de identidad
BitDefender	! Malware	Clúster25	! Suplantación de identidad
CRDF	! Malicioso	CyRadar	! Malicioso
Emsisoft	! Suplantación de identidad	Buscador de amenazas de Forcepoint	! Suplantación de identidad
Fortinet	! Suplantación de identidad	G-datos	! Malware
kaspersky	! Suplantación de identidad	Leonico	! Suplantación de identidad
netcraft	! Malicioso	Base de datos de phishing	! Suplantación de identidad
Búsqueda segura	! Malicioso	Sophos	! Suplantación de identidad
Onda de confianza	! Suplantación de identidad	raiz web	! Malicioso

5. Indicadores de compromiso (IoC)

- URL : `hxtps://share-products hop[.]com/instagram`
- DOMINIO : `share-productshop[.]com`
- SHA-256 : `181e9141bddb14bc8e7 ebca56dd26d2be876a5 6e92165d6e0126e74d1 bde3a1f`
- IP : `84[.]32[.]230[.]157`

escaneo de URL Veredicto de io : potencialmente malicioso!

Apuntando a estas marcas: Instagram (red social)

información en vivo

Navegación segura de Google: **! Malicioso** para `share-productshop.com`

Registro DNS A actual: `84.32.230.57 (AS207709 - HIZHOSTING, TR)`

Dominio creado: 7 de enero de 2023, 02:49:47 (UTC)

Registrador de dominio: Hosting Concepts BV d/b/a Registrar.eu

6. Algunas recomendaciones:

- Verificar detalladamente las URL de los sitios web
- Ingresar desde fuentes oficiales.
- No seguir las instrucciones de sitio web sospechoso.
- Mantener el antivirus actualizado.
- No compartir la URL con amigos y/o familiares.

Fuentes de información

- Análisis propio de redes sociales y fuente abierta