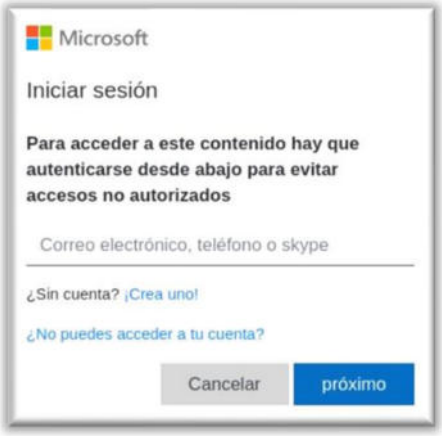
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 131	Fecha: 15-05-2022
		Página 9 de 11

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Detección falso servicio del correo electrónico de Microsoft.		
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 dirigidos a usuarios del servicio de correo electrónico proporcionados por Microsoft, por medio de la creación de un sitio web falso similar al oficial Microsoft Office, con el objetivo de robar credenciales de acceso (correo electrónico y contraseña) de los usuarios de la compañía tecnológica.

2. Detalles del proceso de Phishing



Paso Nº 01
Sitio web falso que suplanta la identidad de Microsoft Office, solicita a la víctima, iniciar sesión del usuario (correo electrónico, teléfono o Skype).

01

02

Paso Nº 02
Una vez ingresado el usuario y hecho clic en <Próximo>, requiere ingresar la contraseña para continuar con el acceso.

03

Paso Nº 03
Al completar el registro, abre una ventana donde la cuenta de Microsoft tiene problemas técnicos y vuelva intentarlo de nuevo en otro momento.

04

Paso Nº 03
Pasado unos segundos, es redirigido al sitio oficial de Microsoft, aludiendo un aparente error de autenticación; sin embargo, los datos fueron capturados.

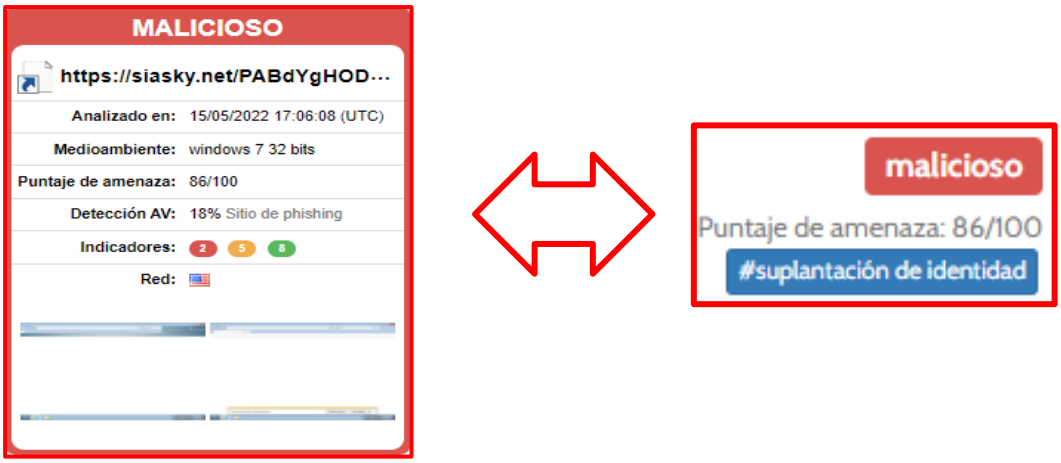
3. La URL sospechosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo como resultado que DIECISIETE (17) proveedores de seguridad informática alertan como **SUPLANTACIÓN DE IDENTIDAD - PHISHING**.

CRDF	Malicioso	CyRadar	Malicioso
Emsisoft	Suplantación de identidad	ESET	Suplantación de identidad
Buscador de amenazas de Forcepoint	Suplantación de identidad	Fortinet	Suplantación de identidad
G-datos	Suplantación de identidad	Seguridad Heimdal	Malicioso
netcraft	Malicioso	Base de datos de phishing	Suplantación de identidad
tanque de phishing	Suplantación de identidad	Sophos	Suplantación de identidad
raíz web	Malicioso	Abusix	Correo no deseado

4. INDICADORES DE COMPROMISO

- **URL** : https://siasky.net/PABdYgHODLQRv9AmtIdFAJWPv0jGjJfzejdDDrqwMVr8Wg
- **SERVIDOR** : openresty/1.19.9.1
- **SHA-256** : a32a7fab553127b2b5e60845cad5c05f5cfdb9c7ac63a57c1be632c13a1558e8
- **IP** : 162[.]244[.]80[.]231
- **Dominio** : siasky.net

5. OTRAS DETENCIONES



6. Qué es un Phishing:

- Es un término informático que distingue a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza, para manipularla y hacer que realice acciones que no debería realizar.

7. ALGUNAS RECOMENDACIONES:

- Verificar detalladamente las URL de los sitios web
- No abrir o descargar archivos sospechosos.
- Mantener el antivirus actualizado.
- Descargar aplicaciones de fuentes confiables.
- Contar con una solución de seguridad, constantemente actualizada tanto en dispositivos de escritorio como en móviles, ya que sirven como barrera inicial protectora ante sitios web maliciosos.

Fuentes de información	▪ Análisis propio de redes sociales y fuente abierta