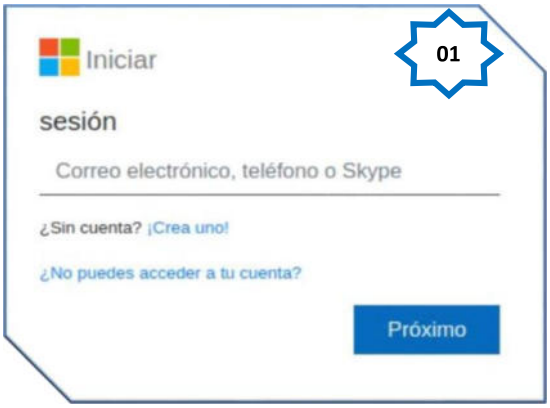
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 097	Fecha: 07-04-2022
		Página 10 de 13

Componente que Reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ		
Nombre de la alerta	Detección de 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 robar credenciales de acceso de la cuenta del usuario.

2. Detalles del proceso de Phishing



Sitio web falso que suplanta la identidad de Microsoft Office, solicita a la víctima, registrar el usuario (correo electrónico, teléfono o Skype).

Una vez ingresado el usuario y hecho clic en <Próximo>, requiere ingresar la contraseña para continuar con el acceso.

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 DIECINUEVE (19) proveedores de seguridad informática alertan como **SUPLANTACIÓN DE IDENTIDAD - PHISHING**.

Avira	Malware	BitDefender	Malware
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	Malware	Seguridad Heimdal	Malicioso

4. INDICADORES DE COMPROMISO

- **URL** : hxxps://magicreator[.]com/owa/outlook/index[.]html
- **SERVIDOR**: Apache
- **SHA-256** : 77f6fcf95298a710dcf84e702411593f49b47f7173e88536d702e760089a682a
- **IP** : 74[.]119[.]238[.]38
- **Dominio** : magicreator[.]com

5. OTRAS DETENCIONES