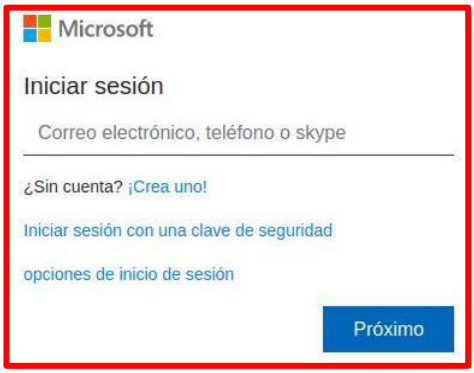
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 067	Fecha: 18-03-2023
		Página 12 de 14

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



01

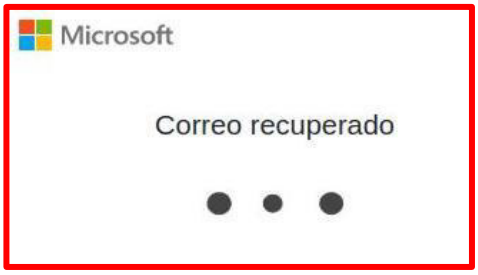
Paso N.º 01

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

Paso N.º 02

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

02



03

Paso N.º 03

Luego de completar las credenciales de acceso y darle clic en <Acceso>, el atacante le informa a la víctima que no a podido recuperar su correo.

Paso N.º 04

Al darle clic en intentar otra vez en recuperar correo, es redirigido al sitio oficial de Microsoft, aludiendo un aparente error de autenticación; sin embargo, los datos ya fueron capturados.

04

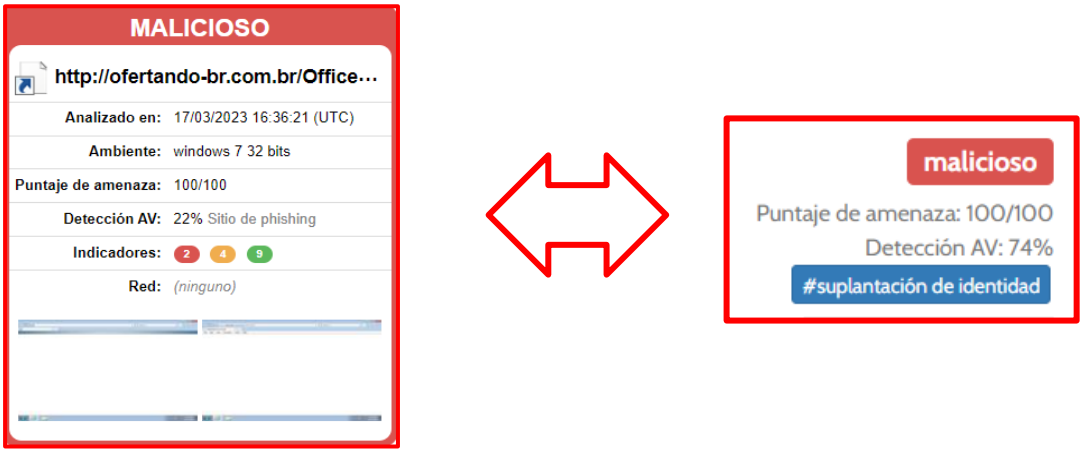
3. La URL sospechosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo como resultado que VEINTIUNO (21) proveedores de seguridad informática alertan como **SUPLANTACIÓN DE IDENTIDAD - PHISHING**.

alphaMountain.ai	Suplantación de identidad	Avira	Suplantación de identidad
BitDefender	Suplantación de identidad	Clúster25	Suplantación de identidad
CRDF	Malicioso	CyRadar	Malicioso
Emsisoft	Suplantación de identidad	ESET	Suplantación de identidad
Buscador de amenazas de Forcepoint	Suplantación de identidad	Fortinet	Suplantación de identidad

4. Indicadores de Compromiso

- **URL** : hXXp://ofertando-br[.]com[.]br/Office365/
- **SHA-256** : 4a32f051950f11a92ffcac8f2b01fcf1ee8dacdcb40757b2e02bc97ea52b4eac
- **IP** : 162[.]241[.]124[.]47
- **Servidor** : Apache
- **Dominio** : ofertando-br[.]com[.]br
- **Tipo** : texto/html

5. Otras Detenciones



6. Que 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
- 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