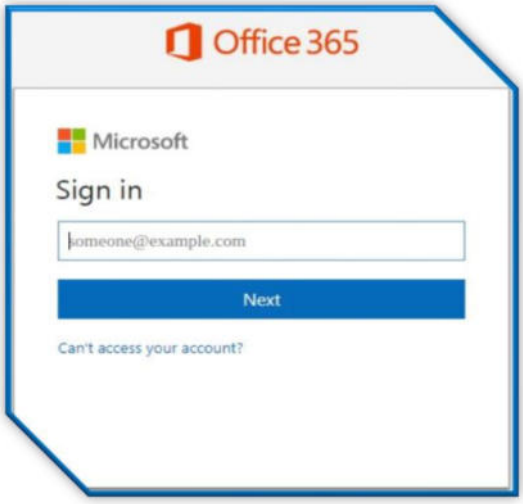
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 076	Fecha: 17-03-2022
		Página 6 de 8

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Phishing, suplantando la identidad de la compañía tecnológica multinacional 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		

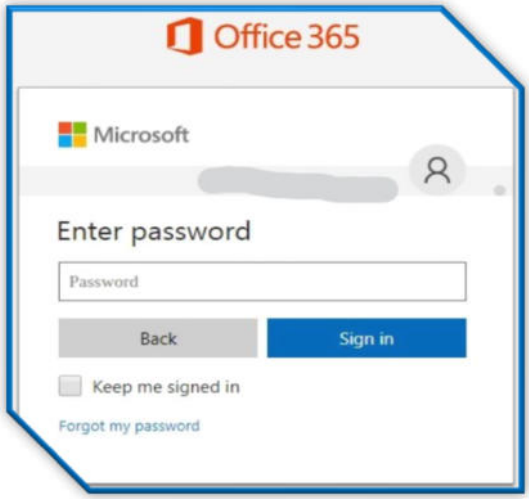
Descripción

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 365, con el objetivo robar credenciales de acceso (usuarios y contraseñas) de la cuenta del usuario.

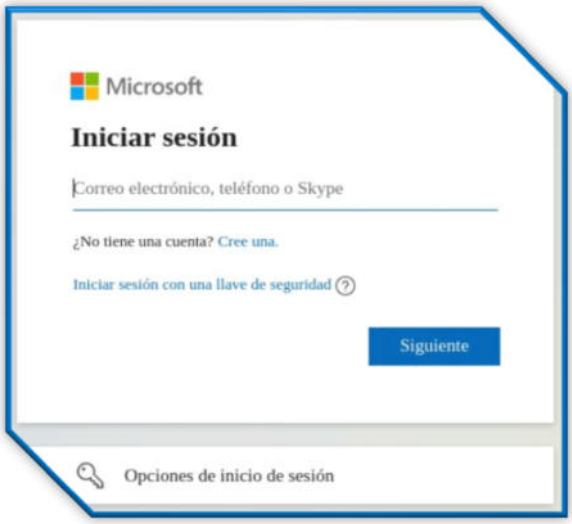
2. ***Imagen: detalles del proceso de la estafa del Phishing***.



Paso Nº 01
Sitio web falso que suplanta la identidad de Microsoft Office, solicita a la víctima ingresar el correo electrónico.



Paso Nº 02
Requiere ingresar la contraseña para continuar con el acceso.



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

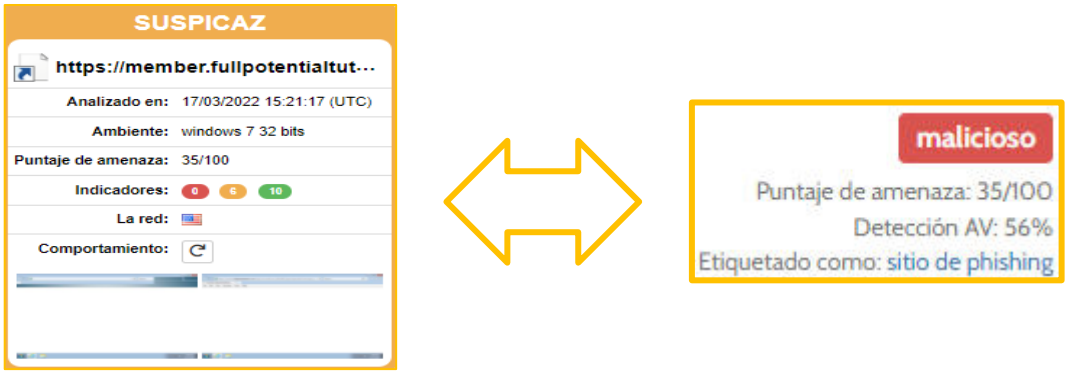
3. ***Se procedió a analizar la URL fraudulenta, obteniendo como resultado que ONCE (11) proveedores de seguridad informática alertan como SUPLANTACIÓN DE IDENTIDAD – PHISHING.***

CRDF	Malicioso	CyRadar	Malicioso
Emsisoft	Suplantación de identidad	ESET	Suplantación de identidad
Buscador de amenazas de Forcepoint	Suplantación de identidad	Fortinet	Suplantación de identidad
kaspersky	Suplantación de identidad	Leonico	Suplantación de identidad
netcraft	Malicioso	Base de datos de phishing	Suplantación de identidad
Sophos	Suplantación de identidad	Abusix	Limpio

4. ***Indicadores de compromiso (IoC)***

- ✓ SHA-256 : 814d279211f63c425bce9a7ea327f61fd0605700c0b66427cc2902124e262e9e
- ✓ Dominio : fullpotentialtutor[.]com
- ✓ Servidor : Apache/2.4.29(Ubuntu)
- ✓ IP : 140[.]82[.]25[.]187

5. ***Otras detecciones:***



6. ***Apreciación de la información*:**

- La presente campaña de Phishing, permite a los actores de amenazas obtener información personal, del correo electrónico y cuentas bancarias.
- La propagación del sitio web fraudulento se realiza mediante envió masivos de email (SPAM), con la finalidad de obtener información sensible de las víctimas; asimismo, a través de las aplicaciones de mensajería instantánea entre ellos WhatsApp, Telegram y Messenger.

7. ***Referencia.***

- 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.

8. ***Algunas recomendaciones:***

- Verificar detalladamente las URL de los sitios web.
- No abrir o descargar archivos sospechosos.
- No seguir las instrucciones de sitio web sospechoso.
- Mantener el antivirus actualizado.
- Tener precaución al abrir enlaces de dudosa procedencia.

Fuente de Información:	Análisis propio de redes sociales y fuente abierta