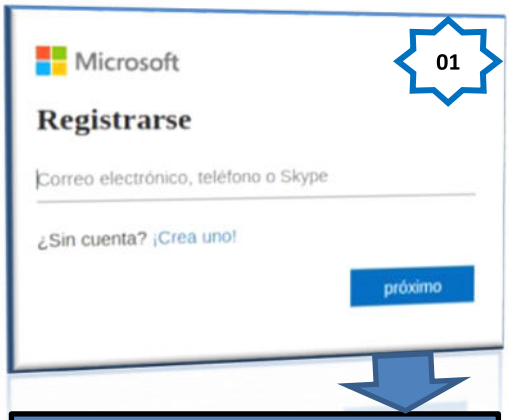
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 101	Fecha: 11-04-2022
		Página 7 de 9

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de Alerta	Detección de falso servicio del correo electrónico de Microsoft.		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medio 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

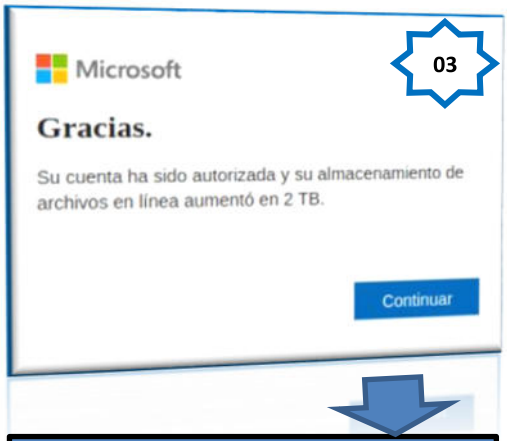
1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que los ciberdelincuentes vienen llevando a cabo una campaña de Phishing dirigidos a usuarios del servicio de correo electrónico proporcionados por Microsoft, por medio de la creación de un sitio web falso similar al oficial 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.



Luego de registrarse, abre una ventana donde indica que <Su cuenta ha sido autorizada y su almacenamiento de archivos ha aumentado 2 TB> y darle <continuar> para ingresar a la cuenta.

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 QUINCE (15) proveedores de seguridad informática alertan como **SUPLANTACIÓN DE IDENTIDAD - PHISHING**.

Avira	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	kaspersky	Suplantación de identidad
Leonico	Suplantación de identidad	netcraft	Malicioso

4. INDICADORES DE COMPROMISO

- **URL** : hxxps://microsoft365.inh.com.au/
- **SERVIDOR**: Microsoft-IIS/10.0
- **SHA-256** : 0a497344ed3cc1a642015657a5ce821b78e3c16f0618fcec902bd478c90c2258
- **IP** : 163[.]53[.]249[.]205
- **Dominio** : inh[.]com[.]au

5. OTRAS DETENCIONES

6. Apreciación de la información:

- La presente campaña de Phishing, permite a los actores de amenazas obtener las credenciales de acceso del servicio del correo electrónico en la web de la compañía Microsoft (Outlook, Hotmail, etc.).
- El medio de propagación del sitio web fraudulento es a través de los correos electrónicos, donde ciberdelincuentes adjuntando enlaces de sitios web preparados con la finalidad de obtener información sensible de las víctimas; asimismo, a través de las aplicaciones de mensajería instantánea entre ellos WhatsApp, Telegram, Messenger y mensajes de textos SMS.

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.

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