	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 144	Fecha: 20-06-2023
		Página 26 de 29

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Detección de una nueva campaña de Phishing a Microsoft Office 365		
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 Sub familia	G02
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES

A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes se encuentran desarrollando una nueva campaña de Phishing, a través de los diferentes navegadores web, quienes vienen suplantando la identidad del sitio oficial de Microsoft Office 365, con el objetivo de robar las credenciales de inicio de sesión de las posibles víctimas.

2. DETALLES

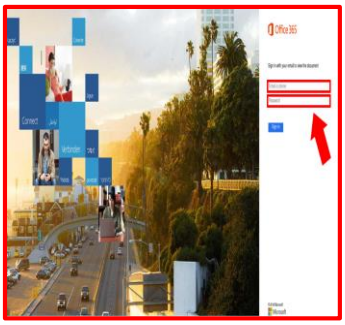


Imagen 1: Sitio web fraudulento; donde los ciberdelincuentes incitan a las víctimas a ingresar sus credenciales de acceso.

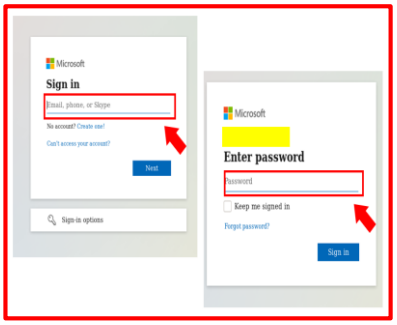


Imagen 2: Una vez ingresada las credenciales de acceso la página web redirige Microsoft online, solicitando ingresar un e-mail y contraseña.

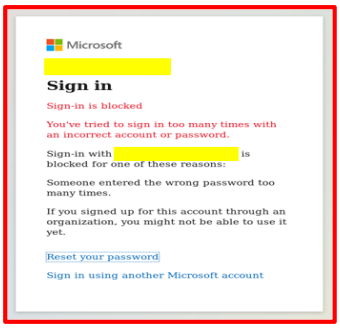


Imagen 3: Una vez ingresada el e-mail y contraseña, redirige a un mensaje en la que indica que la cuenta se encuentra bloqueada; dando por concluida la estafa.

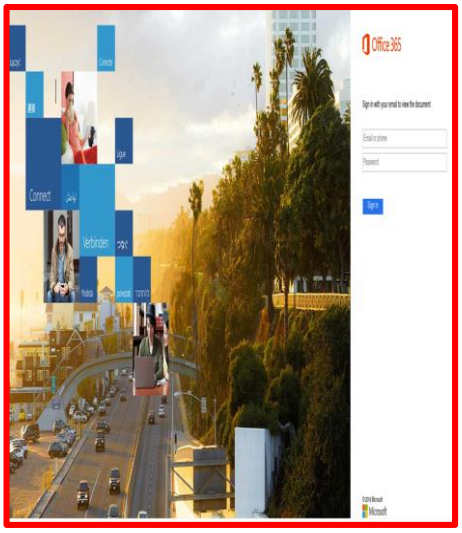
3. Comparación del sitio web oficial y fraudulento.

https://www[.]office.com

hxxps://nekesah[.]githubo1.lio/office[.]github[.]io/

COMPARACIÓN DOMINIO

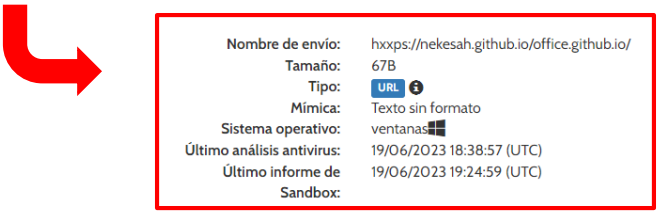
- Existen diferencia entre el fondo y forma de cada sitio web.
- Ambas URL´s utilizan el protocolo HTTPS, lo que hace convincente a que las víctimas accedan al sitio web.
- La diferencia está en la URL, debido el dominio del sitio web fraudulento no corresponde con el oficial.



4. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD:**

a) Indicadores de compromisos:

I. **URL:** hxxps[:]//nekesah[.]github[.]io/office[.]github[.]io/



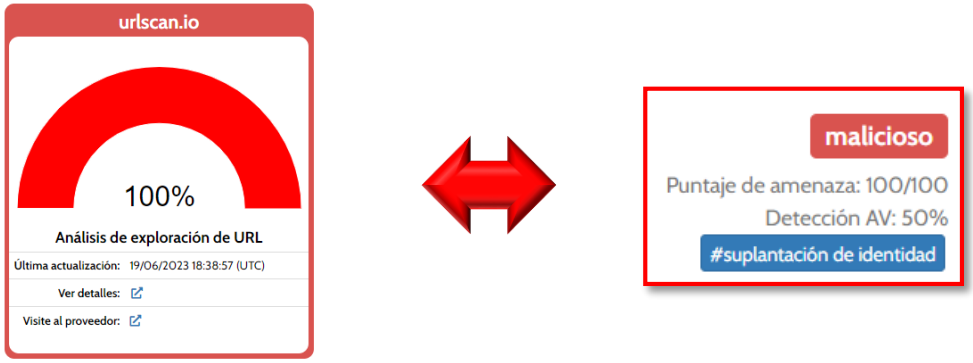
II. **SHA-256:** ffd962b2b34864196a17aa038c6c8d0f0ad6240d122c3cee8380092b8dd177ea

III. **IP:** 185[.]199[.]111[.]153

5. Se hallaron **04 proveedores** de seguridad que marcaron este dominio como malicioso.

ESET	Suplantación de identidad	Base de datos de phishing	Suplantación de identidad
Segasec	Suplantación de identidad	Onda de confianza	Suplantación de identidad

6. Otras detecciones:



7. Cómo funciona el Phishing:

- Los correos electrónicos incluyen enlaces a sitios web preparados por los ciberdelincuentes en los que solicitan información personal.
- Medios de propagación del Phishing: WhatsApp, Telegram, redes sociales, SMS entre otros.
- Los ciberdelincuentes intentan suplantar a una entidad legitima (organismo público o privado, entidad financiera, servicio técnico, etc.)

8. 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.

9. Microsoft Office 365

- Se trata de una herramienta que permite crear, acceder y compartir documentos de Word, Excel, OneNote y PowerPoint. En este sentido presenta cambios con un paquete Office normal, pero la diferencia está en que puede acceder a todos los programas en tiempo real. Además, puede acceder desde cualquier dispositivo que tenga acceso a Internet y OneDrive.

10. Algunas Recomendaciones:

a) Mantener instalado un servicio de antivirus en el dispositivo.
b) Verificar la información del sitio web correspondiente.
c) Acceder al sitio web a través de fuentes oficiales.
d) No abrir enlaces de dudosa procedencia.
e) No seguir indicaciones de sitios web fraudulentos.
f) No compartir la información con terceras personas, amigos o familiares.

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