

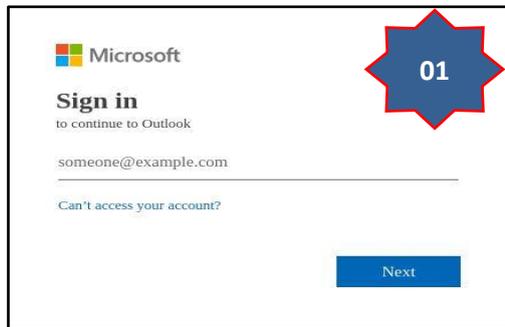
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°290		Fecha: 05-12-2023
			Página: 11 de 14
Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ		
Nombre de la alerta	Detección de falso servicio del correo electrónico de Microsoft		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que actores de amenazas vienen realizando una campaña de Phishing, activando un falso servicio del correo electrónico de la compañía Microsoft (Outlook, Hotmail, etc.), con la finalidad de obtener las credenciales de acceso (correos y contraseñas) de los usuarios de la compañía tecnológica.

2. DETALLES:



Solicita el correo electrónico de la víctima, para acceder al servicio en la web de la compañía Microsoft (Outlook, Hotmail, etc.)

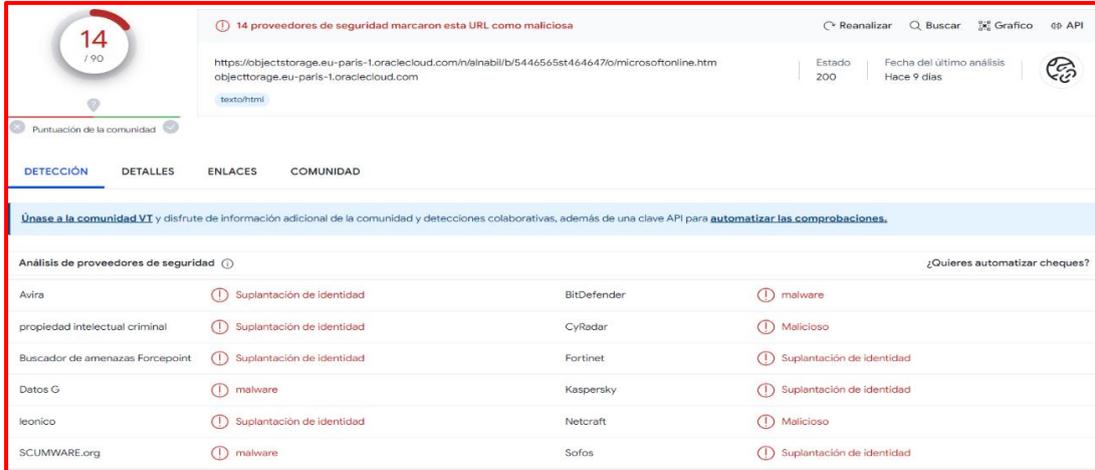
Requieren la contraseña de acceso para el servicio web de Microsoft, para luego dar clic en <Iniciar sesión>; sin embargo, después de unos segundos redirige al servicio del correo electrónico de la compañía Microsoft.

A. Comparación del sitio web oficial y fraudulento.



- Existe diferencias entre la URL original y la fraudulenta.
- La URL del sitio web fraudulento NO POSEE protocolo de seguridad de red (https)
- Existe una similitud entre ambas páginas en imagen, fondo y colores de ambos sitios web.

B. Proveedores de seguridad informática alertan como **SUPLANTACIÓN DE IDENTIDAD - PHISHING.**



14 proveedores de seguridad marcaron esta URL como maliciosa

https://objectstorage.eu-paris-1.oraclecloud.com/n/alnabil/b/5446565st46447/o/microsoftonline.htm

Estado: 200 Fecha del último análisis: Hace 9 días

Proveedor de seguridad	Alerta	Proveedor de seguridad	Alerta
Avira	Suplantación de identidad	BitDefender	malware
propiedad intelectual criminal	Suplantación de identidad	CyRadar	Malicioso
Buscador de amenazas Forcepoint	Suplantación de identidad	Fortinet	Suplantación de identidad
Datos G	malware	Kaspersky	Suplantación de identidad
Iconico	Suplantación de identidad	Netcraft	Malicioso
SCUMWARE.org	malware	Sofos	Suplantación de identidad

C. Indicadores de compromiso (IoC)

- Dominio : oraclecloud[.]com
- SHA-256 : f9a76f238ad305ebd2738a70e6e241a7111ae2e37eb02c4cfee11dd3b3c588b3
- IP : 134[.]70[.]180[.]1

D. Otras detecciones:



MALICIOUS

https://objectstorage.eu-paris-...

Analyzed on: 12/05/2023 21:33:43 (UTC)

Environment: Windows 10 64 bit

Threat Score: 100/100

AV Detection: 15% Phishing site

Indicators: 2 4 11

Network: 🇺🇸

malicioso

Puntuación de amenaza: 100/100

Detección AV: Marcado como limpio

Etiquetado como: Sitio de phishing

#suplantación de identidad

Informe para dirección web

https://objectstorage.eu-paris-1.oraclecloud.com

Categorías: Suplantación de identidad

Peligroso

Amenazas detectadas

02 / 8 MOTORES

- X Suplantación De Identidad Avira.Com
- X Suplantación De Identidad Openphish.Com

E. 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.).
- La propagación del sitio web fraudulento se realiza mediante envío masivos de email, adjuntando enlaces de sitios web fraudulentos con la finalidad de obtener información sensible de las víctimas; asimismo, dicho enlace malicioso, es enviado a través de las plataformas digitales como el WhatsApp, Telegram, Messenger y mensajes de textos SMS.

3. 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.
- Descargar aplicaciones de fuentes confiables.
- Realizar las actualizaciones correspondientes desde fuentes originales.

Fuente de Información:

Análisis propio de redes sociales y fuente abierta.