

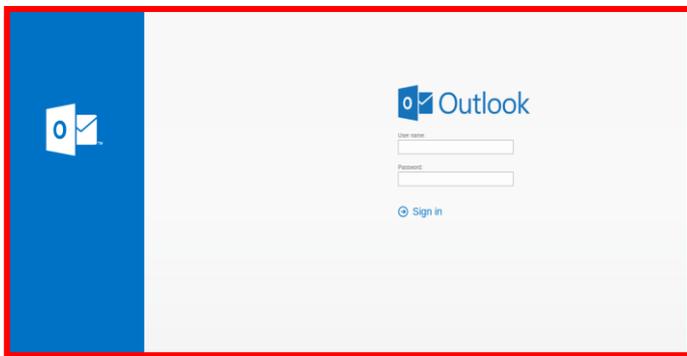
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°211		Fecha: 07-09-2023
			Página: 8 de 11
Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ		
Nombre de la alerta	Nueva campaña de Phishing que suplanta la identidad de Outlook		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios 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, los ciberdelincuentes se encuentran desarrollando una campaña de Phishing, a través de los diferentes navegadores web, quienes vienen suplantando la identidad del sitio oficial de "Outlook"; con el objetivo de acceder u obtener credenciales de inicio de sesión de las posibles víctimas.

2. DETALLES:



Sitio web fraudulento; donde los atacantes buscan persuadir a sus víctimas, solicitando ingresar las credenciales de acceso, sin embargo, la información otorgada es capturada por los ciberdelincuentes.

A. 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[:]//pub-749b686f620d4a78877b378ce1e6fbb2[.]r2[.]dev/outlook-owa-skjuehenje[.]html



Descripción general del análisis	
Nombre del envío:	hxxps[:]//pub-749b686f620d4a78877b378ce1e6fbb2[.]r2[.]dev/outlook-owa-skjuehenje.html
Tamaño:	103B
Tipo:	URL ⓘ
Mímica:	Texto sin formato
Sistema operativo:	ventas:⌨
Último análisis antivirus:	07/09/2023 17:53:09 (UTC)
Último informe de Sandbox:	07/09/2023 17:53:08 (UTC)

II. SHA-256:

f652ca05a9336ae9931cbc7634bd98a19495cb356ab2f4de0d20bb0644d90472



bafybeibhkyj62ldhyswm5beszczf6pslbwxs2cfjyc3si6gikcghdubcu_1_txt	malicioso
RecoveryStore_88B090C0-D917-11E7-B67B-080027A49DD6_dat	sospechoso
RecoveryStore_FA9C855A-4D96-11EE-8328-00505691D89B_dat	sospechoso
_OOCBE9CA-4D97-11EE-8328-00505691D89B_dat	sospechoso
_A5FEO218-4D98-11EE-8328-00505691D89B_dat	sospechoso
_FA9C855C-4D96-11EE-8328-00505691D89B_dat	sospechoso

III. IP: 104[.]18[.]3[.]35



Connection		Detection	
Representative Domain	N/A	Proxy IP	False
SSL Certificate	! True (*.websitewelcome.com)	VPN IP	False
IP Address Owner	NETWORK-SOLUTIONS-HOSTI...	Tor IP	False
Hostname	192-185-94-57.unifiedlayer.com	Hosting IP	! True
Connected Domains	! 73	Mobile IP	False
Country	! United States	CDN IP	False
		Scanner IP	False
		Special Issue	0

B. Se hallaron 18 proveedores de seguridad que marcaron este dominio como malicioso.

alphaMountain.ai	! Phishing	Avira	! Phishing
BitDefender	! Phishing	Cluster25	! Phishing
CRDF	! Malicious	CyRadar	! Malicious
Emsisoft	! Phishing	ESET	! Phishing
Forcepoint ThreatSeeker	! Phishing	Fortinet	! Phishing
G-Data	! Phishing	Kaspersky	! Phishing
Lionic	! Phishing	Netcraft	! Malicious
Phishtank	! Phishing	Sophos	! Phishing
Trustwave	! Phishing	VIPRE	! Malicious

C. Otras detecciones:

MALICIOSO

<https://pub-749b686f620d4a788...>

Analizado en: 07/09/2023 17:53:08 (...)

Ambiente: Windows 7 de 32 bits

Puntuación de amenaza: 100/100

Detección AV: 20% sitio de phishing

Indicadores: 2 2 12

Red: 





malicioso

Puntuación de amenaza: 100/100

#suplantación de identidad

D. 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 legítima (organismo público o privado, entidad financiera, servicio técnico, etc.)

E. 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.

3. RECOMENDACIONES:

- Evitar acceder a enlaces que llegan inesperadamente por correo electrónico u otros medios.
- No proporcionar datos personales (contraseñas, tarjetas, cuentas bancarias, etc.) por correo, teléfono o SMS.
- No introducir datos confidenciales en sitios web sospechosas o de dudosa procedencia.
- Verificar la fuente de información de tus correos entrantes.
- Introducir tus datos únicamente en webs seguras.
- Tener siempre actualizado el sistema operativo y el antivirus. En el caso del antivirus, comprobar que está activo.

Fuente de Información:

Análisis propio de redes sociales y fuente abierta