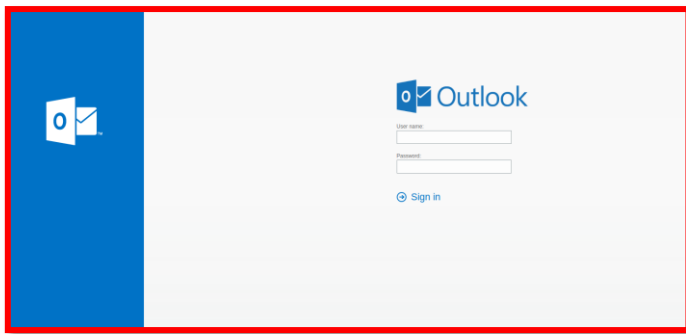
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°218		Fecha: 15-09-2023
			Página: 8 de 11
Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ		
Nombre de la alerta	Nueva campaña de Phishing que suplanta la identidad de Microsoft Outlook		
Tipo de Ataque	Phishing	Abreviatura	Phishing
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 Microsoft Outlook, (que es un programa informático gestor de correo electrónico desarrollado por Microsoft); 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:	<code>hxxps[:]//pub-749b686f620d4a78877b378ce1e6fbb2.r2.dev/outlook-owa-skjuehenje.html</code>
Tamaño:	103B
Tipo:	URL
Mimica:	Texto sin formato
Sistema operativo:	ventanas
Último análisis antivirus:	15/09/2023 15:03:14 (UTC)
Último informe de Sandbox:	07/09/2023 17:53:08 (UTC)

II. SHA-256:

`https://pub-749b686f620d4a78877b378ce1e6fbb2.r2.dev/outlook-owa-skjuehenje.html`

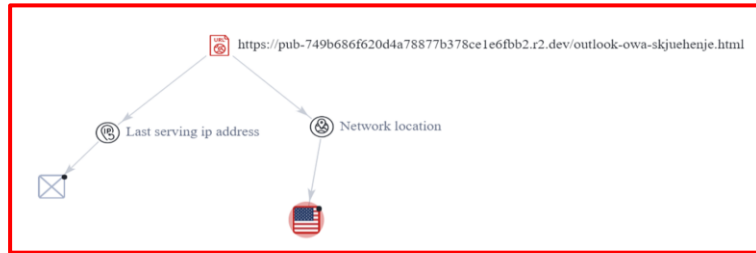
<code>_A5FEO218-4D98-11EE-8328-00505691D89B_dat</code>	suspicioso
<code>_FA9C855C-4D96-11EE-8328-00505691D89B_dat</code>	suspicioso
<code>_OOCBE9CA-4D97-11EE-8328-00505691D89B_dat</code>	suspicioso
<code>RecoveryStore_88B090C0-D917-11E7-B67B-080027A49DD6_dat</code>	suspicioso
<code>bafybeibhyk62ldhyswm5besczf6pslwxus2cfjycj3si6gkqhdubcu_1.txt</code>	malicioso

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



Connection		Detection	
Representative Domain	N/A	Proxy IP	False
SSL Certificate	False	VPN IP	False
IP Address Owner	CLOUDFLARENET	Tor IP	False
Hostname	N/A	Hosting IP	! True
Connected Domains	! 254	Mobile IP	False
Country	-	CDN IP	False
		Scanner IP	False
		Special Issue	0

IV. TIPOLOGÍA:



Se puede apreciar como la URL, esta alojada en un servidor ubicado en **EE.UU.**

B. Se hallaron 17 proveedores de seguridad que marcaron este dominio como malicioso.

alphaMountain.ai	! Phishing	Avira	! Phishing
BitDefender	! Malware	Cluster25	! Phishing
CRDF	! Malicious	Criminal IP	! Phishing
CyRadar	! Malicious	ESET	! Phishing
Forcepoint ThreatSeeker	! Phishing	Fortinet	! Phishing
G-Data	! Malware	Kaspersky	! Phishing
Lionic	! Phishing	Netcraft	! Malicious
Sophos	! Phishing	Trustwave	! Phishing
VIPRE	! Malicious	Abusix	✓ Clean

C. Otras detecciones:

MALICIOSO

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

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

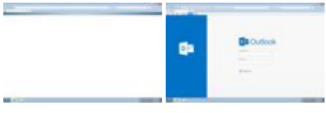
Ambiente: Windows 7 de 32 bits

Puntuación de amenaza: 100/100

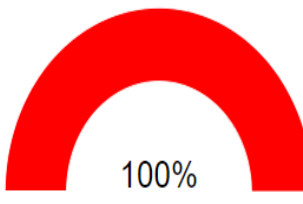
Detección AV: 20% sitio de phishing

Indicadores: 2 2 12

Red:



urlscan.io



100%

Análisis de escaneo de URL

Última actualización: 15/09/2023 15:03:14 (UTC)

Ver detalles: [🔗](#)

Visitar proveedor: [🔗](#)

malicioso

Puntuación de amenaza: 100/100

Detección AV: 39%

#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 sospechosos 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.