

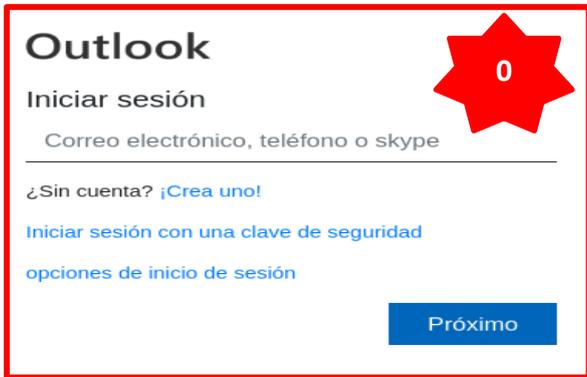
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°070		Fecha: 21-03-2024
			Página: 12 de 15
Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ		
Nombre de la alerta	Nueva campaña de Phishing que suplanta la identidad de Microsoft Outlook		
Tipo de Ataque	Phishing	Abreviatura	Phishing
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:

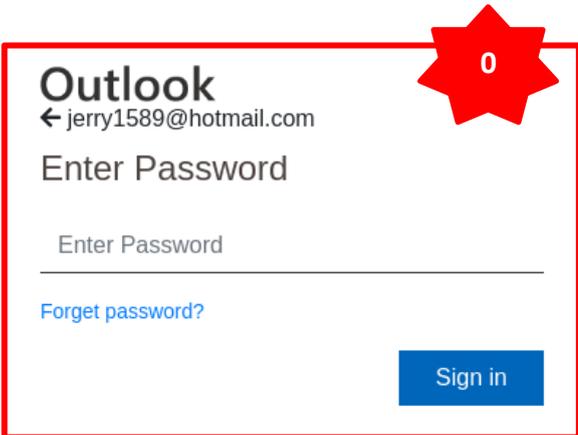
A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincentes se encuentran desarrollando una campaña de Phishing, a través de los diferentes navegadores web, quienes vienen suplantando la identidad del sitio oficial de Microsoft Outlook, (que es un programa informático 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 de la corporación tecnológica de Microsoft Outlook, solicita a la víctima que registre el correo electrónico, el teléfono o skype, para poder continuar.

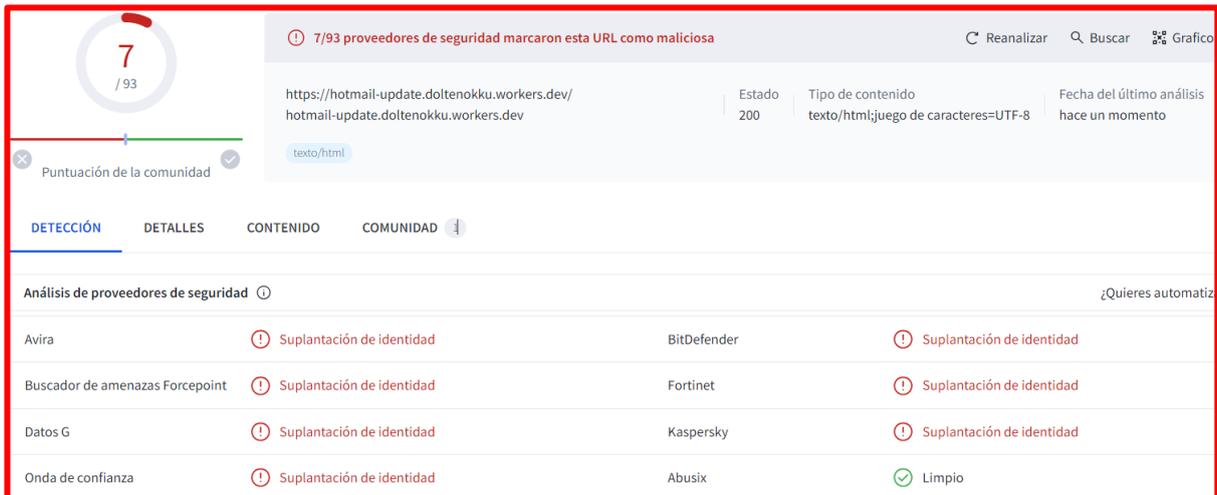
Luego de registrar el correo electrónico, el atacante le solicita a la víctima que registre la contraseña para poder ingresar.



Al registrar las credenciales de acceso, es redirigido al sitio web oficial del sitio web de Microsoft; sin embargo, los ciberdelincentes obtuvieron los datos proporcionados por la víctima.



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



7 / 93

7/93 proveedores de seguridad marcaron esta URL como maliciosa

Reanalizar Buscar Grafico

https://hotmail-update.doltenokku.workers.dev/ Estado 200 Tipo de contenido texto/html;juego de caracteres=UTF-8 Fecha del último análisis hace un momento

texto/html

Puntuación de la comunidad

DETECCIÓN DETALLES CONTENIDO COMUNIDAD

Análisis de proveedores de seguridad ¿Quieres automatiz

Proveedor	Resultado	Proveedor	Resultado
Avira	Suplantación de identidad	BitDefender	Suplantación de identidad
Buscador de amenazas Forcepoint	Suplantación de identidad	Fortinet	Suplantación de identidad
Datos G	Suplantación de identidad	Kaspersky	Suplantación de identidad
Onda de confianza	Suplantación de identidad	Abusix	Limpio

B. Indicadores de compromisos:

I. URL: `hxxps[:]//hotmail-update[.]doltenokku[.]workers[.]dev`



Site	https://hotmail-update.doltenokku.workers.dev
Netblock Owner	Cloudflare, Inc.
Hosting company	Cloudflare
Hosting country	US

II. DOMINIO: `workers[.]dev`



Domain	workers.dev
Nameserver	clyde.ns.cloudflare.com
Domain registrar	nic.google
Nameserver organisation	whois.cloudflare.com

III. IP: `172[.]67[.]199[.]20`



IP Range	Country	Name	Description
::ffff:0:0:0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
172.0.0-172.255.255	United States	NET172	Various Registries (Maintained by ARIN)
172.64.0.0-172.71.255.255	United States	CLOUDFLARENET	Cloudflare, Inc.
172.67.199.20	United States	CLOUDFLARENET	Cloudflare, Inc.

IV. SHA-256: `Obac060a8a6245abfcfeaa1d330a907dd5b9e1f73f919eeacf089163c4599938`

V. Servidor: Cloudflare

C. 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.)

D. 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