	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°061	Fecha: 11-03-2024
		Página: 8 de 14

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:

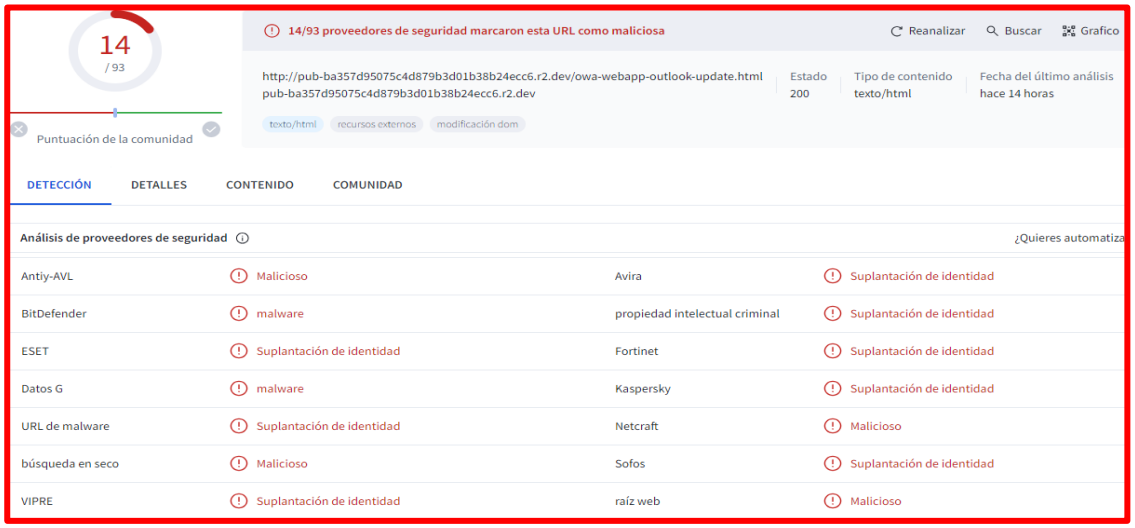
A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes se encuentran desarrollando una campaña de Phishing, a través de los diferentes navegadores web, quienes vienen suplantando la identidad del sitio oficial de Microsoft Outlook, (que es un programa 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 de la corporación tecnológica de Microsoft, solicita a la víctima que registre las credenciales de acceso como el correo electrónico y contraseña, para poder ingresar al sitio web.

Luego de registrar las credenciales de acceso, es redirigido al sitio web oficial del sitio web de Microsoft; sin embargo, los ciberdelincuentes 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:**



B. Indicadores de compromisos:

I. URL: https://pub-ba357d95075c4d879b3d01b38b24ecc6.r2.dev/owa-webapp-outlook-update.html

Site	http://pub-ba357d95075c4d879b3d01b38b24ecc6.r2.dev
Netblock Owner	Cloudflare, Inc.
Hosting company	Cloudflare
Hosting country	US

II. DOMINIO: r2[.]dev

Domain	r2.dev
Nameserver	camilo.ns.cloudflare.com
Domain registrar	nic.google
Nameserver organisation	whois.cloudflare.com

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

IPv4 address (104.18.3.35)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
↳ 104.0.0.0-104.255.255.255	United States	NET104	American Registry for Internet Numbers
↳ 104.16.0.0-104.31.255.255	United States	CLOUDFLARENET	Cloudflare, Inc.
↳ 104.18.3.35	United States	CLOUDFLARENET	Cloudflare, Inc.

IV. SHA-256:
5d4a96ecbdd1b1787ba4c1d12f764b8a4fdf68641e0a7d6daf8383927aede829

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 legitima (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 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