

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°240		Fecha: 10-10-2023
			Página: 9 de 12
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 SharePoint		
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:

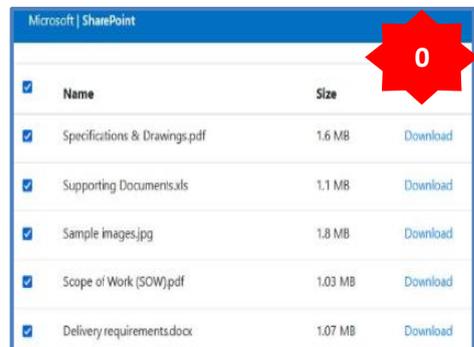
A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelinquentes vienen llevando a cabo una campaña de Phishing, a través de los diferentes navegadores web, quienes vienen suplantando la identidad de la corporación de aplicativos web y de escritorio “Microsoft SharePoint”, el supuesto sitio web cuenta con colores y logos característicos idénticos al sitio web oficial, el cual tiene como finalidad robar información confidencial de las posibles víctimas, el cual requiere que descargue documentos e ingrese la dirección de correo electrónico y contraseña.

2. DETALLES:



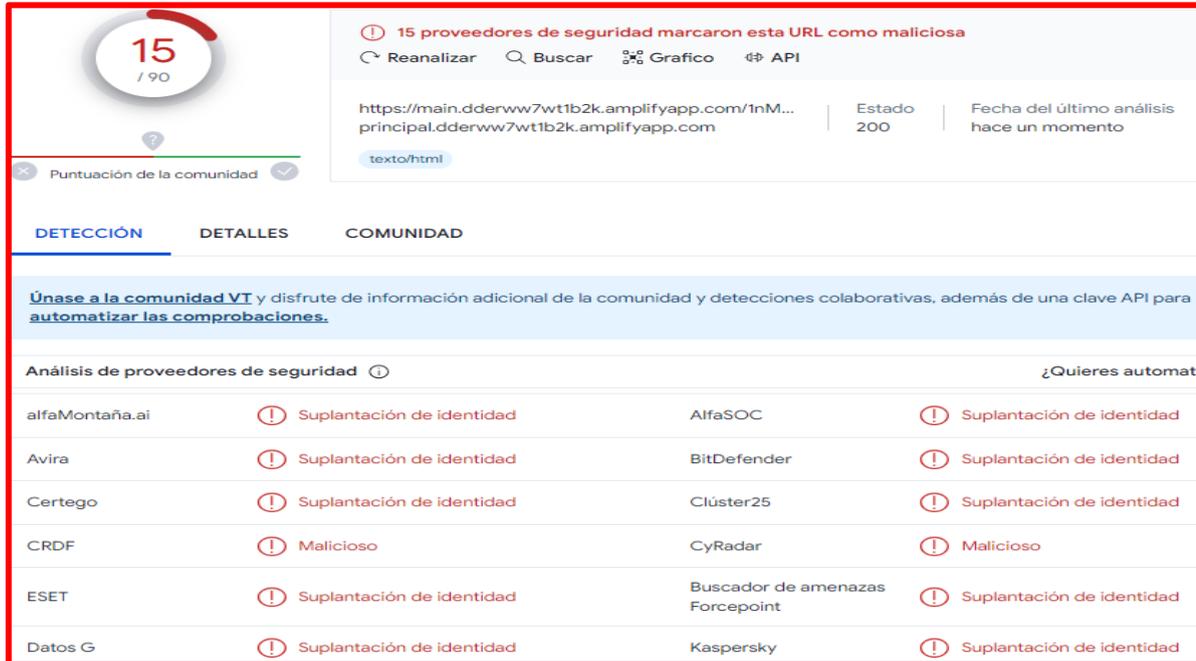
Paso N° 01
 Sitio web falso que suplanta la identidad de Microsoft SharePoint, solicita a la víctima que le dé clic en Descargar documento o ver Documento para continuar.

Paso N° 02
 Luego de haber ingresado aparece 6 archivos como especificaciones, imágenes entre otros, con la finalidad de descargar estos archivos.



Paso N° 03
 Luego de haber colocado el correo electrónico y contraseña y darle clic en <<Ingresar>>, pasado unos segundos le indica que ha registrado mal los datos, aludiendo un aparente error de autenticación; sin embargo, los datos fueron capturados por los cibercriminales.

A. La URL sospechosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo como **SUPLANTACIÓN DE IDENTIDAD - PHISHING.**



15 / 90
 Puntuación de la comunidad

15 proveedores de seguridad marcaron esta URL como maliciosa
 Reanalizar | Buscar | Grafico | API

https://main.dderww7wt1b2k.amplifyapp.com/1nM... | Estado 200 | Fecha del último análisis hace un momento

texto/html

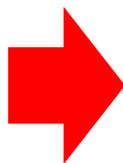
DETECCIÓN | DETALLES | COMUNIDAD

Únase a la comunidad VT y disfrute de información adicional de la comunidad y detecciones colaborativas, además de una clave API para automatizar las comprobaciones.

Análisis de proveedores de seguridad | ¿Quieres automatizar?

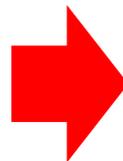
Proveedor	Detección	Proveedor	Detección
alfaMontaña.ai	Suplantación de identidad	AlfaSOC	Suplantación de identidad
Avira	Suplantación de identidad	BitDefender	Suplantación de identidad
Certego	Suplantación de identidad	Clúster25	Suplantación de identidad
CRDF	Malicioso	CyRadar	Malicioso
ESET	Suplantación de identidad	Buscador de amenazas Forcepoint	Suplantación de identidad
Datos G	Suplantación de identidad	Kaspersky	Suplantación de identidad

✓ URL :



Netblock Owner	Amazon.com, Inc.
Hosting company	Amazon
Hosting country	US

✓ Dominio : amplificarapp[.]com



Domain	amplifyapp.com
Nameserver	ns-904.awsdns-49.net
Domain registrar	comlaude.com
Nameserver organisation	whois.markmonitor.com

✓ IP : 13[.]249[.]85[.]118

IP range	Country	Name	Description
::ffff:0.0.0./96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
18.0.0-18.255.255	United States	NET18	American Registry for Internet Numbers
18.32.0-18.255.255	United States	AT-88-Z	Amazon Technologies Inc.
18.64.0-18.67.255	United States	AMAZO-CF	Amazon.com, Inc.
18.66.171.101	United States	AMAZO-CF	Amazon.com, Inc.

✓ SHA-256 : 3c025f2def7f8bb9ed08c82dc5c5a60da498445a0d02eef767e335b4c94e1ba
 ✓ Servidor : AmazonS3

✓ Otras detecciones del análisis:

MALICIOSO

<https://main.dderww7wt1b2k.am...>

Analizado en: 10/10/2023 16:43:00 (UTC)

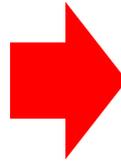
Ambiente: Windows 7 de 32 bits

Puntuación de amenaza: 100/100

Detección AV: 16% Sitio de phishing

Indicadores: 2 2 8

Red: 🇺🇸



malicioso

Puntuación de amenaza: 100/100

#suplantación de identidad

B. Apreciación de la información:

- La presente campaña de Phishing permite a los actores de amenazas obtener información personal de los usuarios de la corporación Microsoft.
- La propagación del sitio web fraudulento se realiza mediante envío masivos de email (SPAM), con la finalidad de obtener información sensible de las víctimas; asimismo, a través de las aplicaciones de mensajería instantánea entre ellos 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.
- Contar con una solución de seguridad, constantemente actualizada tanto en dispositivos de escritorio como en móviles, ya que sirven como barrera inicial protectora ante sitios web maliciosos.

Fuente de Información:

Análisis propio de redes sociales y fuente abierta.