	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°283	Fecha: 27-11-2023
		Página: 9 de 12

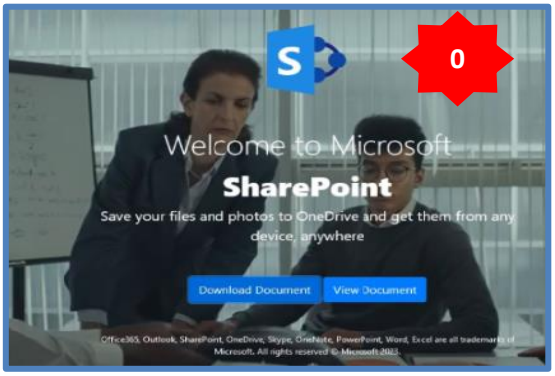
Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Nueva campaña de phishing que suplanta la identidad de Microsoft SharePoint		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

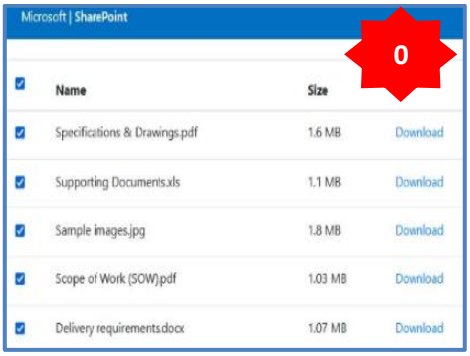
1. ANTECEDENTES:

A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes 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.

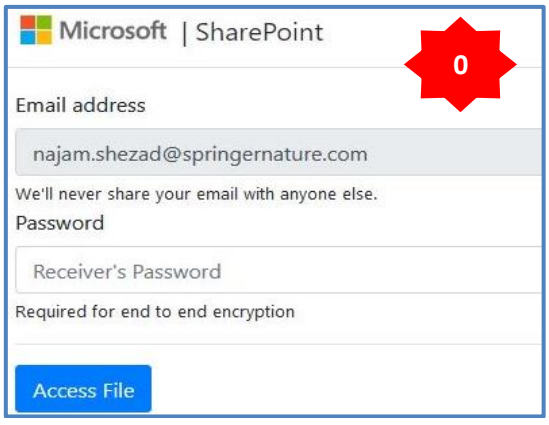
2. DETALLES:



Paso Nº 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 Nº 02
Luego de haber ingresado aparece 6 archivos como especificaciones, imágenes entre otros, con la finalidad de descargar estos archivos.

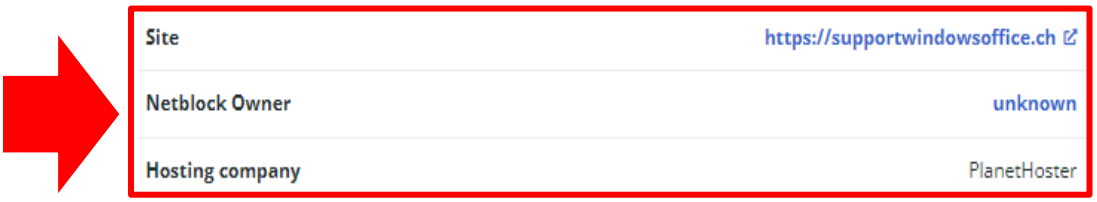


Paso Nº 03
Luego de haber colocado el correo electrónico y contraseña y darle clic en <<Ingresar>>, pasado unos segundos le indica que ha registrado mal los datos, aludiendo un aparente error de autenticación; sin embargo, los datos fueron capturados por los cibercriminales.

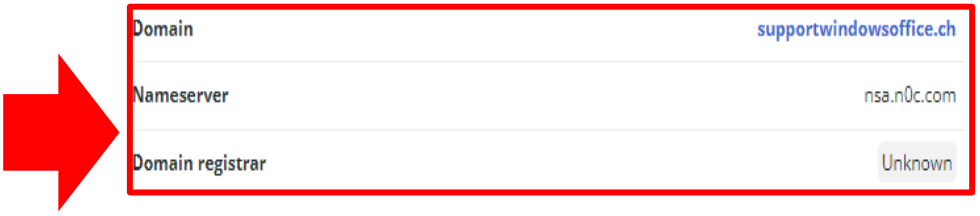
alphaMountain.ai	Malicious	AlphaSOC	Phishing
Antiy-AVL	Malicious	Avira	Phishing
BitDefender	Phishing	Cluster25	Phishing
CRDF	Malicious	CyRadar	Malicious
ESET	Phishing	Forcepoint ThreatSeeker	Phishing
Fortinet	Phishing	G-Data	Phishing
Kaspersky	Phishing	Lionic	Malicious
Phishing Database	Phishing	Seclookup	Malicious
SOCRadar	Malware	Sophos	Phishing
VIPRE	Malware	Webroot	Malicious

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

✓ URL https://supportwindowsoffice.ch

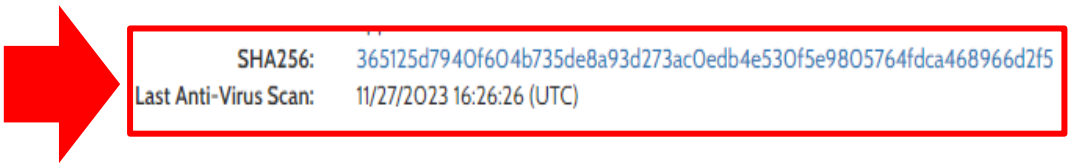


✓ Dominio : supportwindowsoffice.ch



✓ IP : 185 [.]221 [.]182 [.]46

✓ SHA-256 : 365125d7940f604b735de8a93d273ac0edb4e530f5e9805764fdca468966d2f5



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 envió 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.