Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°175	Fecha: 30-07-2024
		Página: 4 de 8

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	La estafa de phishing de OneDrive engaña a los usuarios para que ejecuten un script malicioso de PowerShell		
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:

Las estafas de phishing continúan evolucionando y convirtiéndose en una amenaza cada vez más sofisticada para los usuarios de servicios en línea. Recientemente, se ha descubierto una nueva táctica que utiliza OneDrive como cebo, engañando a los usuarios para que ejecuten un script malicioso de PowerShell. Esta técnica no solo pone en riesgo la seguridad de tus datos, sino que también puede comprometer toda tu red.

2. DETALLES:

"Esta campaña se basa en gran medida en tácticas de ingeniería social para engañar a los usuarios para que ejecuten un script de PowerShell, comprometiendo así sus sistemas", dijo el investigador de seguridad de Trellix, Rafael Peña.

Denominada "OneDrive Pastejacking", la campaña inicia con un correo electrónico que contiene un archivo HTML adjunto. Al abrirlo, el archivo muestra una imagen que imita una página oficial de OneDrive y presenta un mensaje de error que afirma: "Error al conectarse al servicio en la nube 'OneDrive'. Para corregir el error, debe actualizar la caché DNS manualmente".

El mensaje ofrece dos opciones: "Cómo solucionarlo" y "Detalles". La opción de "Detalles" redirige a los usuarios a una página legítima de Microsoft Learn, donde se explican problemas comunes de DNS, lo que añade una capa de legitimidad al engaño. Sin embargo, al seleccionar "Cómo solucionarlo", los usuarios son guiados a realizar una serie de pasos que incluyen presionar "Tecla Windows + X" para abrir el menú Enlace rápido, iniciar la terminal de PowerShell, y pegar un comando codificado en Base64, que supuestamente resolverá el problema.

"El comando primero ejecuta ipconfig /flushdns, luego crea una carpeta en la unidad C: llamada 'downloads'", explicó Peña. "A continuación, descarga un archivo en esta ubicación, le cambia el nombre, extrae su contenido ('script.a3x' y 'AutoIt3.exe') y ejecuta script.a3x utilizando AutoIt3.exe", un programa que facilita la automatización de tareas en Windows.

En realidad, este comando ejecuta un script malicioso que puede comprometer la seguridad del sistema del usuario, permitiendo a los atacantes acceder a información sensible o controlar remotamente el equipo infectado. Este tipo de ataques, que explotan la confianza del usuario en servicios legítimos y su desconocimiento técnico, representan una amenaza significativa para la seguridad cibernética.

3. RECOMENDACIONES:

- No hacer clic en enlaces sospechosos o no solicitados, ni descargar adjuntos de correos desconocidos.
- Utilizar software de seguridad. Proteger sus dispositivos con software antivirus actualizado, que pueda ayudar a detectar y bloquear descargas y sitios maliciosos, así como también habilitar la protección de firewall para monitorear y controlar el tráfico de red entrante y saliente.
- Descargar aplicaciones exclusivamente de fuentes oficiales.
- Capacitar a los usuarios sobre las mejores prácticas de ciberseguridad.

Fuente de Información:	• hxxps://thehackernews.com/2024/07/onedrive-phishing-scam-tricks-users.html • hxxps://blog.tecnetone.com/phishing-en-onedrive-enga%C3%B1a-a-usuarios-para-ejecutar-script-powershell