DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°176**	**Fecha: 26-07-2023**
		Página: 5 de 8

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Nueva campaña de malware de acceso inicial “Nitrogen” dirigido a organizaciones tecnológicas		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Investigadores de Sophos han detectado una nueva campaña de malware de acceso inicial denominado “Nitrogen”, que utiliza anuncios de búsqueda de Google y Bing para dirigirse a usuarios que buscan ciertas herramientas de TI, con el objetivo de obtener acceso a entornos empresariales para implementar un ataque de segunda etapa. Un ataque exitoso podría permitir a un actor de amenazas el robo de datos, realizar actividades de ciberespionaje e implementar el ransomware BlackCat/ALPHV y herramientas como Cobalt Strike.

2. DETALLES:

Investigadores de Sophos indicaron que esta campaña de malware “Nitrogen” se dirige principalmente a organizaciones tecnológicas y sin fines de lucro en América del Norte, se hace pasar por varios tipos de software como: AnyDesk, Cisco AnyConnect VPN, TreeSize Free y WinSCP.

Sophos señalo que la infección comienza cuando la potencial víctima realiza una búsqueda en Google o Bing de varias aplicaciones de software pirateados usados como señuelos: AnyDesk (aplicación de escritorio remoto), WinSCP (cliente SFTP/FTP para Windows), Cisco AnyConnect (paquete VPN) y TreeSize Free (administrador y calculadora de espacio en disco).

Según los criterios de orientación, el motor de búsqueda mostrará un anuncio que promociona el software buscado. Luego, al hacer clic en el enlace malicioso, la víctima accede a un sitio web de alojamiento de WordPress previamente comprometida que imita a los sitios de descarga del software legítimos.

Los investigadores indicaron que, solo las víctimas de regiones geográficas específicas son redirigidas a los sitios web de phishing, mientras que los accesos directos a las URL maliciosas desencadenan una redirección a videos de YouTube.

Luego de ser redirigido a los sitios web de phishing, los usuarios descargan instaladores ISO troyanizados ("install.exe"), que contienen y descargan un archivo DLL malicioso ("msi.dll"). El msi.dll es el instalador para el malware de acceso inicial “Nitrogen” llamado internamente "NitrogenInstaller", que además instala la aplicación solicitada para evitar sospechas y un paquete Python malicioso.

El “NitrogenInstaller” también crea una clave de ejecución de registro llamada "Python" para la persistencia, apuntando a un binario malicioso ("pythonw.exe") que se ejecuta cada cinco minutos. El componente Python ejecutará "NitrogenStager" ("python.311.dll"), que es responsable de establecer la comunicación con el C2 del actor de amenazas y lanzar un shell Meterpreter y Cobalt Strike Beacons en el sistema de la víctima.

En algunos casos observados por los analistas de Sophos, los atacantes pasaron a la actividad práctica una vez que se ejecutó el script Meterpreter en el sistema de destino, ejecutando comandos manuales para recuperar archivos ZIP adicionales y entornos de Python 3. Este último es necesario para ejecutar Cobalt Strike en la memoria, ya que NitrogenStager no puede ejecutar scripts de Python.

A. Indicadores de Compromiso (IoC):

- Un conjunto completo de indicadores de compromiso está disponible en GitHub.

3. RECOMENDACIONES:

- Evitar hacer clic en los resultados "promocionados" en los motores de búsqueda cuando descarguen software y, en su lugar, sólo descargar desde el sitio web oficial del desarrollador.
- Tener cuidado con cualquier descarga que utilice archivos ISO para software, ya que es un método poco común para distribuir software legítimo de Windows, que generalmente viene como un archivo .exe o .zip.

Fuente de Información:	• hxxps://news.sophos.com/en-us/2023/07/26/into-the-tank-with-nitrogen/