Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°197	Fecha: 22-08-2023
		Página: 4 de 12

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	ATAQUE NOFILTER: El método de escalada de privilegios furtivos omite la seguridad de Windows		
Tipo de Ataque	Abuso de privilegios o de políticas de seguridad	Abreviatura	AbuPrivPolSeg
Medios de propagación	Red, Internet		
Código de familia	K	Código de Sub familia	K01
Clasificación temática familia	Uso inapropiado de recursos		

Descripción

1. ANTECEDENTES:

Se descubrió que un método de ataque no detectado previamente llamado NoFilter abusa de la plataforma de filtrado de Windows (WFP) para lograr una escalada de privilegios en el sistema operativo Windows.

Los hallazgos se presentaron en la conferencia de seguridad DEF CON durante el fin de semana.

El punto de partida de la investigación es una herramienta interna llamada RPC Mapper, utilizada por la empresa de ciberseguridad para mapear los métodos de llamada a procedimiento remoto (RPC), específicamente aquellos que invocan WinAPI, lo que llevó al descubrimiento de un método llamado «BfeRpcOpenToken», que es parte de la WFP.

Plataforma de Filtrado de Windows (WFP) es un conjunto de API y servicios del sistema que proporcionan una plataforma para crear aplicaciones de filtrado de red. La API de WFP permite a los desarrolladores escribir código que interactúa con el procesamiento de paquetes que tiene lugar en varias capas de la pila de red del sistema operativo. Los datos de la red se pueden filtrar y también modificar antes de que lleguen a su destino.

2. DETALLES:

“Si un atacante tiene la capacidad de ejecutar código con privilegios de administrador y el objetivo es realizar modificaciones en LSASS, estos privilegios no son suficientes”, explicó Ron Ben Yizhak, un investigador de seguridad en Deep Instinct. "En su lugar, se requiere ejecutar como NT AUTHORITY\SYSTEM".

El aspecto innovador de NoFilter Attack radica en su capacidad para manipular el WFP.

“La tabla de identificadores de otro proceso se puede recuperar llamando a NtQueryInformationProcess”, dijo Ben Yizhak. “Esta tabla enumera los tokens mantenidos por el proceso, y los identificadores de esos tokens pueden duplicarse para otro proceso, permitiendo la escalada a SYSTEM”.

Aunque los tokens de acceso se utilizan para identificar al usuario involucrado al ejecutar una tarea privilegiada, un malware en modo de usuario puede acceder a los tokens de otros procesos mediante funciones específicas (como DuplicateToken o DuplicateHandle) y luego utilizar ese token para iniciar un proceso secundario con privilegios de SYSTEM.

"Lo innovador de esta técnica radica en la capacidad para manipular el WFP en el kernel para realizar la duplicación de tokens, lo que lo hace increíblemente discreto y difícil de detectar" Advierten los investigadores.

En otras palabras, NoFilter puede iniciar una nueva consola como "NT AUTHORITY\SYSTEM" o como otro usuario que ha iniciado sesión en la máquina.

"La conclusión es que se pueden descubrir nuevos vectores de ataque al investigar los componentes integrados en el sistema operativo, como la Plataforma de Filtrado de Windows", mencionó Ben Yizhak, señalando que estos métodos "evitan el uso de las WinAPI que son monitoreadas por productos de seguridad".

La revelación se produce cuando SafeBreach reveló enfoques novedosos que podrían ser abusados por un actor de amenazas para cifrar archivos sin ejecutar código en el punto final objetivo utilizando un ransomware basado en la nube (DoubleDrive), neutralizar el agente de detección y respuesta de punto final (EDR) de Windows Defender y permitir que cualquier código malicioso se ejecute sin ser detectado (Defender-Pretender) y eliminar de forma remota bases de datos completas de servidores completamente parcheados (Borrar datos de forma remota).

3. RECOMENDACIONES:

- Adoptar medidas de ciberseguridad para mitigar este tipo de ataques.
- Mantener el sistema parchado y actualizado.
- Desarrollar un plan de respuesta a incidentes.
- Programar copias de seguridad.
- Aplicar políticas del mínimo privilegio.
- Configurar Firewalls y filtros de red.
- Ejecutar soluciones con antivirus oficialmente aceptados.
- Segmentar la red aislando los activos críticos.

Fuente de Información:	• hxxps://devel.group/blog/nofilter-attack-el-metodo-de-escalada-de-privilegios-furtivos-omite-la-seguridad-de-windows/ • hxxps://es.linkedin.com/pulse/nofilter-un-novedoso-ataque-que-otorga-los-atacantes