Actores malintencionados están aprovechando una técnica de ataque innovadora que utiliza archivos de consola de administración guardados (MSC) especialmente diseñados para obtener ejecución completa de código a través de Microsoft Management Console (MMC) y evadir las defensas de seguridad.

Elastic Security Labs ha llamado a este método GrimResource después de identificar un artefacto («sccm-updater.msc«) que se subió a la plataforma de escaneo de malware VirusTotal el 6 de junio de 2024.

> *«Cuando se importa un archivo de consola malicioso, una vulnerabilidad en una de las bibliotecas de MMC puede permitir la ejecución de código del atacante, incluido malware»*, afirmó la compañía.
>
> *«Los atacantes pueden combinar esta técnica con DotNetToJScript para lograr ejecución de código arbitrario, lo que puede resultar en acceso no autorizado, toma de control del sistema y más.»*

El uso de tipos de archivos poco comunes como vector de distribución de malware se considera un intento alternativo por parte de los adversarios para eludir las barreras de seguridad establecidas por Microsoft en los últimos años, incluida la desactivación de macros por defecto en archivos de Office descargados de internet.

El mes pasado, la firma surcoreana de ciberseguridad Genians detalló el uso de un archivo MSC malicioso por parte del grupo de hackers Kimsuky, vinculado a Corea del Norte, para distribuir malware.

GrimResource, por otro lado, explota una vulnerabilidad de scripting entre sitios (XSS) presente en la biblioteca apds.dll para ejecutar código JavaScript arbitrario en el contexto de MMC. La vulnerabilidad XSS fue reportada originalmente a Microsoft y Adobe a finales de 2018, aunque aún no ha sido parcheada.

Esto se logra añadiendo una referencia al recurso vulnerable APDS en la sección StringTable de un archivo MSC malicioso, que, al abrirse con MMC, desencadena la ejecución del código JavaScript.

La técnica no solo elude las advertencias de ActiveX, sino que también se puede combinar con DotNetToJScript para obtener ejecución de código arbitrario. La muestra analizada utiliza este enfoque para lanzar un componente cargador de .NET llamado PASTALOADER que finalmente abre camino para Cobalt Strike.

> *«Después de que Microsoft desactivara las macros de Office por defecto para documentos descargados de internet, otros vectores de infección como JavaScript, archivos MSI, objetos LNK e ISOs han ganado popularidad»,* dijeron los investigadores de seguridad Joe Desimone y Samir Bousseaden.
>
> *«Sin embargo, estas otras técnicas son revisadas por los defensores y tienen una alta probabilidad de ser detectadas. Los atacantes han desarrollado una nueva técnica para ejecutar código arbitrario en Microsoft Management Console utilizando archivos MSC diseñados.»*