Expertos en seguridad han descrito una táctica renovada relacionada con el secuestro del orden de búsqueda de bibliotecas dinámicas (DLL), que podría ser empleada por individuos malintencionados para eludir sistemas de seguridad y lograr que se ejecute código dañino en equipos con Microsoft Windows 10 y Windows 11.

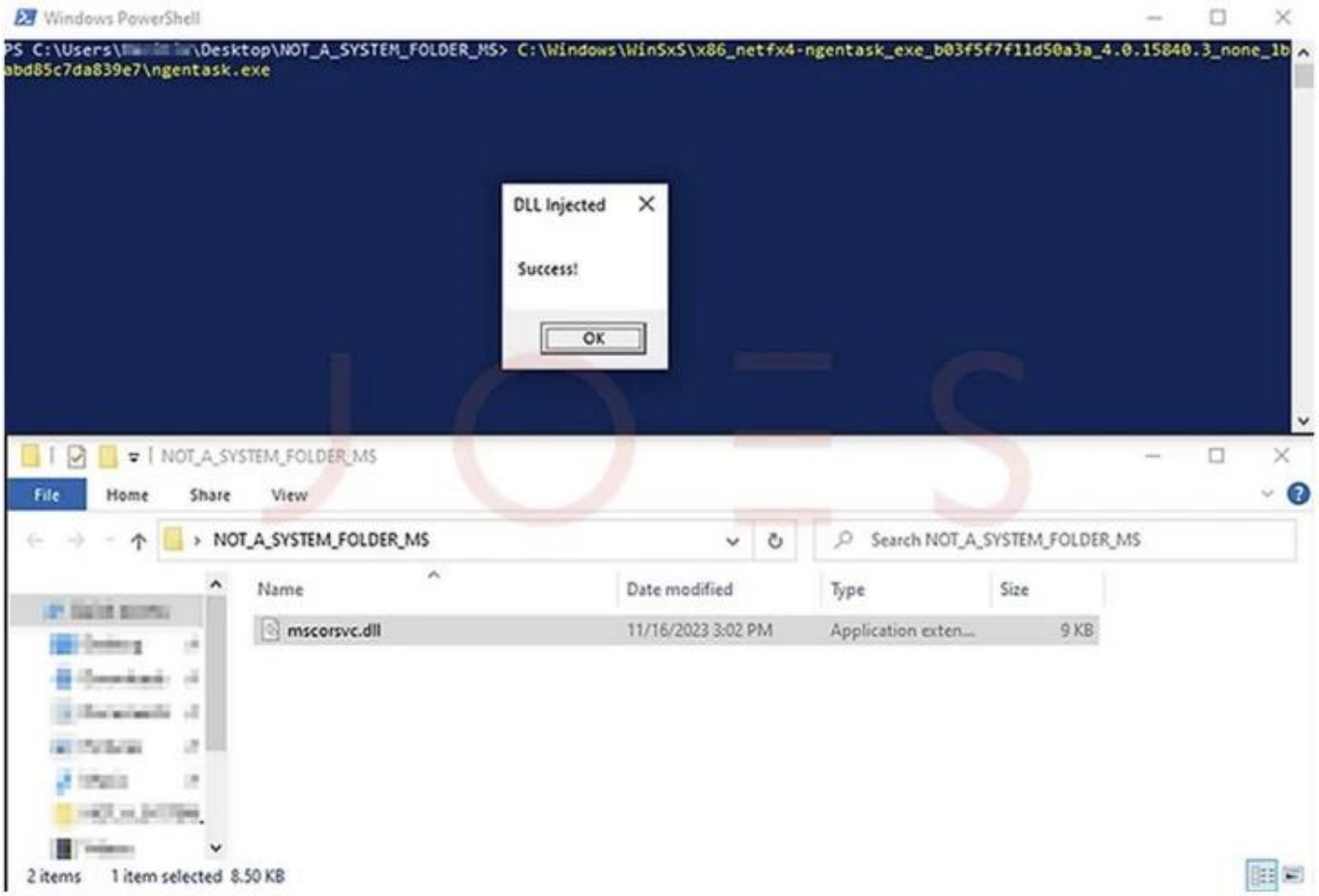
Este método *«utiliza archivos ejecutables que a menudo se encuentran en la conocida carpeta WinSxS, manipulándolos a través de la tradicional técnica de secuestro del orden de búsqueda de DLL»,* mencionó la compañía de seguridad informática Security Joes en un reciente informe.

Al implementar este método, los atacantes pueden prescindir de requerir permisos elevados al intentar desplegar código malicioso en un dispositivo comprometido. Además, pueden integrar binarios con posibles fallos de seguridad en la cadena de ataque, tal como se ha visto anteriormente.

El concepto de secuestro del orden de búsqueda de DLL consiste en alterar el proceso de búsqueda empleado para cargar DLLs, con el propósito de ejecutar acciones maliciosas para evadir defensas, mantenerse en el sistema y obtener privilegios adicionales.

Más específicamente, las tácticas basadas en esta técnica identifican programas que no indican la ubicación exacta de las bibliotecas que necesitan. En su lugar, confían en un esquema de búsqueda determinado para hallar las DLLs requeridas en el almacenamiento.

Los delincuentes cibernéticos se aprovechan de esta vulnerabilidad traslocando archivos legítimos del sistema a directorios fuera de lo común, incorporando DLLs dañinas con nombres que se asemejan a las auténticas. Esto causa que el sistema cargue la biblioteca con código dañino en lugar de la original.



Example of a successful DLL Search Order Hijacking abusing a binary in the WinSxS folder.

Esto se debe a que el proceso que invoca la DLL primero revisará el directorio en el que se ejecuta antes de recorrer sistemáticamente otras ubicaciones en un esquema específico para descubrir e integrar el recurso deseado. Para ser más preciso, el esquema de búsqueda se configura así:

1. El sitio desde donde se arrancó la aplicación.
2. La ruta «C:\Windows\System32».
3. La ruta «C:\Windows\System».
4. La ruta «C:\Windows».
5. La ubicación de trabajo actual.

6. Las rutas especificadas en la variable de entorno PATH del sistema.
7. Las rutas especificadas en la variable de entorno PATH del usuario.

El enfoque innovador presentado por Security Joes se enfoca en ficheros situados en la confiable carpeta «C:\Windows\WinSxS». Denominada como Windows side-by-side, WinSxS es un elemento esencial de Windows que sirve para adaptar y actualizar el sistema operativo, garantizando así su compatibilidad y consistencia.

> *«Este método introduce una perspectiva inédita en el campo de la ciberseguridad: hasta ahora, los atacantes se han inclinado por técnicas reconocidas como el desvío del orden de búsqueda de DLL, una táctica que altera la forma en que las aplicaciones de Windows incorporan bibliotecas y programas externos»,* expresó Ido Naor, uno de los fundadores y director ejecutivo de Security Joes.
>
> - *«Nuestro hallazgo representa un desvío de las tácticas habituales, mostrando un procedimiento de manipulación más matizado y discreto».*

El concepto fundamental es identificar archivos susceptibles en la carpeta WinSxS (como ngentask.exe y aspnet_wp.exe) y entrelazarlo con las técnicas convencionales de alteración del orden de búsqueda de DLL, situando estratégicamente una DLL adaptada con el nombre de la DLL legítima en una carpeta bajo control del atacante, logrando así la activación de código.

Por ende, con solo ejecutar un archivo con vulnerabilidades en WinSxS, estableciendo la carpeta con la DLL fraudulenta como directorio activo, se desencadena la activación del contenido de dicha DLL sin requerir trasladar el archivo desde WinSxS.

Security Joes subrayó que existen posiblemente otros archivos en WinSxS propensos a este tipo de manipulación del orden de búsqueda de DLL, instando a las entidades a adoptar medidas preventivas en sus sistemas.

> *«Analice las interacciones entre procesos, especialmente en binarios confiables. Supervise meticulosamente todas las operaciones efectuadas por los binarios en WinSxS, poniendo atención tanto en las interacciones en red como en las operaciones de ficheros»,* recomendó la firma.