Descubrimientos recientes muestran que actores maliciosos podrían aprovechar una astuta técnica de evasión de detección de malware y superar las soluciones de seguridad de puntos finales al manipular el Marco de Aislamiento de Contenedores de Windows.

Estos hallazgos fueron presentados por el investigador en seguridad de Deep Instinct, Daniel Avinoam, durante la conferencia de seguridad DEF CON celebrada a principios de este mes.

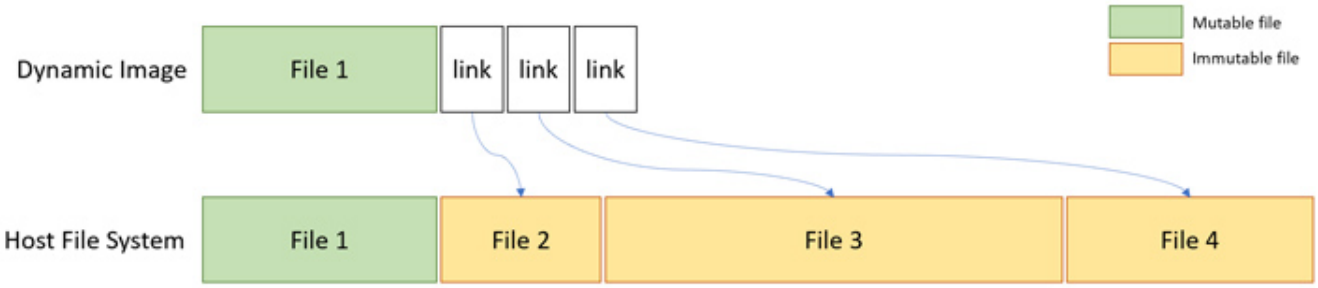
La arquitectura de contenedores de Microsoft (y, por extensión, Windows Sandbox) utiliza lo que se conoce como una imagen generada dinámicamente para separar el sistema de archivos de cada contenedor del sistema anfitrión y, al mismo tiempo, evitar la duplicación de archivos del sistema.

En resumen, se trata de una *«imagen del sistema operativo que contiene copias limpias de archivos que pueden cambiar, pero que enlazan con archivos que no pueden cambiar y que ya existen en la imagen de Windows en el sistema anfitrión»,* lo que reduce el tamaño general de un sistema operativo completo.

> *«El resultado son imágenes que contienen 'archivos fantasmas', que no almacenan datos reales, pero que señalan hacia un volumen diferente en el sistema. Fue en este punto cuando se me ocurrió la idea: ¿y si podemos utilizar este mecanismo de redirección para oscurecer nuestras operaciones en el sistema de archivos y confundir a los productos de seguridad?»*, explicó Avinoam en un informe

Aquí es donde entra en juego el controlador del minifiltro de Aislamiento de Contenedores de Windows (wcifs.sys). La principal función de este controlador es encargarse de la separación del sistema de archivos entre los contenedores de Windows y su sistema anfitrión.

En otras palabras, la idea es tener el proceso actual funcionando dentro de un contenedor fabricado y aprovechar el controlador del minifiltro para gestionar las solicitudes de E/S de manera que pueda crear, leer, escribir y eliminar archivos en el sistema de archivos sin despertar sospechas en el software de seguridad.



Es importante destacar en este punto que un minifiltro se conecta a la pila del sistema de archivos de manera indirecta, registrándose en el administrador de filtros para las operaciones de E/S que elige filtrar. A cada minifiltro se le asigna un valor de «altitud» asignado por Microsoft en función de los requisitos del filtro y el grupo de orden de carga.

El controlador wcifs tiene un rango de altitud de 180,000-189,999 (específicamente 189,900), mientras que los filtros antivirus, incluidos los de terceros, funcionan en un rango de altitud de 320,000-329,999. Como resultado, varias operaciones de archivos pueden llevarse a cabo sin activar sus devoluciones de llamada.

> *«Debido a que podemos anular archivos utilizando la etiqueta de redirección IO_REPARSE_TAG_WCI_1 sin que los controladores antivirus lo detecten, su algoritmo de detección no captará el panorama completo y, por lo tanto, no se activará»,* explicó Avinoam.

Dicho esto, llevar a cabo el ataque requiere permisos administrativos para comunicarse con el controlador wcifs y no se puede utilizar para anular archivos en el sistema anfitrión.

Esta revelación se produce mientras que la empresa de ciberseguridad demostraba una técnica sigilosa llamada NoFilter que abusa de la Plataforma de Filtrado de Windows (WFP)

para elevar los privilegios de un usuario al nivel de SYSTEM y potencialmente ejecutar código malicioso.

Estos ataques permiten utilizar WFP para duplicar tokens de acceso para otro proceso, iniciar una conexión IPSec y aprovechar el servicio de Cola de Impresión para insertar un token de SYSTEM en la tabla, lo que hace posible obtener el token de otro usuario que haya iniciado sesión en el sistema comprometido y así realizar movimientos laterales.