Investigadores de seguridad cibernética revelaron un nuevo ataque de manipulación de imágenes ejecutables denominado «Process Ghosting», que podría ser abusado por hackers para eludir las protecciones y ejecutar de forma sigilosa código malicioso en un sistema Windows.

> *«Con esta técnica, un atacante puede escribir una pieza de malware en el disco de tal forma que sea difícil de escanear o eliminar, y donde luego ejecuta el malware eliminado como si fuera un archivo normal en el disco. Esta técnica no implica la inyección de código, Process Hollowing o Transactional NTFS (TxF)»,* dijo Gabriel Landau, investigador de Elastic Security.

Process Ghosting amplía los métodos de omisión de endpoints previamente documentados, como Process Doppelgänging y Process Herpaderping, lo que permite la ejecución velada de código malicioso que puede evadir las defensas y la detección antimalware.

Process Doppelgänging, análogo a Process Hollowing, implica la inyección de código arbitrario en el espacio de direcciones del proceso en vivo de una aplicación legítima que luego se puede ejecutar desde el servicio confiable.

Process Herpaderping, detallado por primera vez en octubre pasado, describe un método para ocultar el comportamiento de un proceso en ejecución mediante la modificación del ejecutable en el disco después de que la imagen se haya mapeado en la memoria.

La evasión funciona debido a una *«brecha entre el momento en que se crea un proceso y cuando se notifica a los productos de seguridad de su creación»,* lo que brinda a los desarrolladores de malware una ventana para manipular el ejecutable antes de que los productos de seguridad puedan escanearlo.

Process Ghosting va un paso más allá de Doppelgänging y Herpaderping, al permitir ejecutar binarios que ya han sido eliminados. Aprovecha el hecho de que los intentos de Windows de evitar que los ejecutables asignados se modifiquen o eliminen solo entra en vigencia después

de que el binario se asigna a una sección de imagen.

> *«Esto significa que es posible crear un archivo, marcarlo para eliminarlo, asignarlo a una sección de imagen, cerrar el identificador del archivo para completar la eliminación y luego crear un proceso desde la sección ahora sin archivos. Esto es Process Ghosting»,* dijo Landau.

En una demostración de prueba de concepto (PoC), los investigadores detallaron un escenario en el que Windows Defender intenta abrir un ejecutable de carga útil malicioso para escanearlo, pero no lo hace porque el archivo está en un estado independiente de eliminación y luego falla nuevamente, ya que el archivo ya está eliminado, lo que permite que se ejecute sin obstáculos.

Elastic Security dijo que informó del problema al Centro de Respuesta de Seguridad de Microsoft (MSRC) en mayo de 2021, luego de lo cual el fabricante de Windows declaró que el problema *«no cumple con su estándar de servicio«,* haciéndose eco de una respuesta similar cuando Process Herpaderping se reveló de forma responsable a MSRC en julio de 2020.

Microsoft, por su parte, lanzó desde entonces una versión actualizada de Sysinternals Suite a inicios de enero con una utilidad mejorada del Monitor del Sistema (también conocido como Sysmon) para ayudar a detectar los ataques de Process Herpaderping y Process Hollowing.

Como resultado de esto, las versiones 13.00 y posteriores de Sysmon, ahora pueden generar y registrar *«ID de evento 25» cuando una pieza de malware manipula un proceso legítimo y si se cambia una imagen de proceso de un proceso diferente, con Microsoft notando que el evento se activa «cuando la imagen mapeada de un proceso no coincide con el archivo de imagen en el disco, o el archivo de imagen está bloqueado para acceso exclusivo».*