La técnica de inyección de código sin archivo denominada como Process Doppelgänging, está siendo utilizada activamente por un gran número de familias de malware en el medio, según reveló The Hacker News.

Descubierto a finales de 2017, Process Doppelgänging es una variación sin archivos de la técnica de inyección de procesos que aprovecha la función integrada de Windows para evadir la detección y funciona en todas las versiones modernas del sistema operativo Microsoft Windows.

El ataque de proceso Doppelgänging funciona mediante el uso de la función de Windows llamada Transactional NTFS (TxF) para iniciar un proceso malintencionado al reemplazar la memoria de un proceso legítimo, engañar a las herramientas de monitoreo de procesos y al antivirus para que crean que se está ejecutando el proceso legítimo.

Pocos meses después de la divulgación de esta técnica, una variante del ransomware *SynAck* se convirtió en el primer malware que explota la técnica Process Doppelgänging, dirigida a usuarios en Estados Unidos, Kuwuait, Alemania e Irán.

Poco tiempo después, los investigadores descubrieron un cargador para el troyano bancario Osiris, que también estaba utilizando esta técnica en combinación con una técnica similar de evasión de malware previamente descubierta llamada Process Hollowing.

Ahora se supo que no solo fue SynAck y Osiris, sino que más de 20 familias de malware diferentes, incluyendo FormBook, LokiBot, SmokeLoader, AZORult, NetWire, njRat, Pony stealer y GrandCrab han estado usando cargadores de malware que aprovechan este híbrido al implementar el proceso Doppelgänging para evadir la detección.

Después de analizar cientos de muestras de malware, los investigadores de seguridad de enSilo descubrieron al menos siete versiones distintas del cargador, que denominaron «TxHollowe», utilizado por varios autores de malware.

> *«Se sabe que los atacantes reutilizan recursos y herramientas en sus cadenas de ataque, los más notables son descargadores, empacadores y cargadores. Se destaca que los componentes compartidos y el código hacen que el seguimiento y la atribución de varios grupos sean aún más complicados»,* dijeron los investigadores.

Los investigadores creen que los cargadores TxHollower están disponibles para los piratas informáticos por medio de un marco ofensivo o un kit de explotación, lo que eventualmente aumenta el uso de técnicas de proceso Doppelgänging en el medio.

La muestra más temprana del cargador con la función TxHollower se utilizó en marzo de 2018 para distribuir Netwire RAT, y luego se encontró con varias versiones de GrandCrab, comenzando con v5 y llegando a v5.2.

Además, los investigadores de enSilo también encontraron algunas muestras envueltas en una capa adicional como los archivos MSI, y en algunos casos, los cargadores se anidaron entre sí.

> *«Si bien no observamos las infecciones reales, pudimos encontrar algunas muestras que sospechamos que están relacionadas con la cadena de infección, como los descargadores y los cargadores de TxHollower. El tipo de archivos incluye ejecutables de PE, JavaScript y documentos»,* dijeron los investigadores.