Investigadores de seguridad cibernética brindaron los detalles sobre un cargador malicioso que se ejecuta como un servidor y ejecuta los módulos recibidos en la memoria, dejando al descubierto la estructura de una *«máquina virtual avanzada de varias capas»* utilizada por el malware para pasar desapercibida.

Wslink, como se llama el cargador malicioso, fue documentado por primera vez por la compañía de ciberseguridad eslovaca ESET en octubre de 2021, con muy pocos accesos de telemetría detectados en los últimos dos años en Europa Central, América del Norte y Oriente Medio.

El análisis de las muestras de malware arrojó pocas o ninguna pista sobre el vector de compromiso inicial utilizado, y no se ha descubierto ningún código, funcionalidad o similitudes operativas que sugieran que se trata de una herramienta de un actor de amenazas previamente identificado.

Equipado con una utilidad de compresión de archivos llamada NsPack, Wslink hace uso de lo que se llama máquina virtual de proceso (VM), un mecanismo para ejecutar una aplicación de una forma independiente de la plataforma que abstrae el hardware o el sistema operativo subyacente como un método de ofuscación pero con una diferencia crucial.

> *«Las máquinas virtuales utilizadas como motores de ofuscación no están destinadas a ejecutar aplicaciones multiplataforma y, por lo general, toman código de máquina compilado o ensamblado para una ISA [arquitectura de conjunto de instrucciones] conocida, lo desensamblan y lo traducen a su propia ISA virtual»,* dijo el analista de malware de ESET, Vladislav Hrcka.

> *«La fuerza de esta técnica de ofuscación reside en el hecho de que el ISA de la VM*

> *es desconocido para cualquier posible ingeniero inverso: se requiere un análisis exhaustivo de la VM, que puede llevar mucho tiempo, para comprender el significado de las instrucciones virtuales y otras estructuras de la VM»*, agregó.

Además, el paquete de malware utilizado Wslink viene con un arsenal diverso de tácticas para obstaculizar la ingeniería inversa, incluyendo el código basura, la codificación de operandos virtuales, la combinación de instrucciones virtuales y el uso de una máquina virtual anidada.

> *«Las técnicas de ofuscación son un tipo de protección de software destinada a hacer que el código sea difícil de entender, y por lo tanto, ocultar sus objetivos; las técnicas de ofuscación de máquinas virtuales se han usado ampliamente para fines ilícitos, como la ofuscación de muestras de malware, ya que dificultan tanto el análisis como la detección»,* dijo Hrcka.