Se ha descubierto una nueva backdoor asociada con un descargador de malware llamado Wslink, y la herramienta probablemente sea utilizada por Lazarus Group, alineado con Corea del Norte, según los nuevos hallazgos.

La carga útil, denominada WinorDLL64 por ESET, es un implante con todas las funciones que puede filtrar, sobrescribir y eliminar archivos; ejecutar comandos de PowerShell y obtener información completa sobre la máquina subyacente.

Otras de sus características son la enumeración de sesiones activas, creación y finalización de procesos, enumeración de unidades y compresión de directorios.

Wslink fue documentado por primera vez por la compañía de seguridad cibernética ESET en octubre de 2021, describiéndolo como un cargador de malware *«simple pero notable»* que es capaz de ejecutar módulos recibidos en la memoria.

> *«La carga útil de Wslink se puede aprovechar más tarde para el movimiento lateral, debido a su interés específico en las sesiones de red. El cargador Wslink escucha en un puerto especificado en la configuración y puede servir a clientes de conexión adicionales e incluso cargar varias cargas útiles»*, dijo el investigador de ESET, Vladislav Hrčka.

Se cree que las instrucciones que aprovechan el malware están muy dirigidas debido al hecho de que hasta ahora solo se han observado unas pocas detecciones en Europa Central, América del Norte y Oriente Medio.

En marzo de 2022, ESET elaboró sobre el uso del malware de un ofuscador de *«máquina virtual avanzada de múltiples capas»* para evadir la detección y resistir la ingeniería inversa.

Los enlaces a Lazarus Group se derivan de superposiciones en el comportamiento y el código de las campañas anteriores, Operation GhostSecret y Bankshot, que se han atribuido a la amenaza persistente avanzada.

Esto incluye similitudes con las muestras de GhostSecret detalladas por McAfee en 2018, que vienen con un «*componente de instalación de implantes y recopilación de datos*» que se ejecuta como un servicio, reflejando el mismo comportamiento de Wslink.

ESET dijo que la carga útil se cargó en la base de datos de malware VirusTotal desde Corea del Sur, donde se encuentran algunas de las víctimas, lo que agrega credibilidad a la participación de Lazarus.

Los hallazgos demuestran una vez más el conjunto de herramientas de hacking empleadas por Lazarus Group para infiltrarse en sus objetivos.

> *«La carga útil de Wslink está dedicada a proporcionar medios para la manipulación de archivos, la ejecución de código adicional y la obtención de información extensa sobre el sistema subyacente que posiblemente se pueda aprovechar más tarde para el movimiento lateral»*, dijo ESET.