Una nueva herramienta de malware que permite a los atacantes crear archivos maliciosos de acceso directo de Windows (.LNK) ha sido descubierta a la venta en foros de hacking.

Nombrado como *Quantum Lnk Builder,* el software permite suplantar cualquier extensión y elegir entre más de 300 iconos, además de ser compatible con UAC y omitir Windows SmartScreen, así como *«múltiples cargas útiles por archivo .LNK».* También se ofrecen capacidades para generar cargas útiles .HTA e imagen de disco (.ISO).

Quantum Builder está disponible para arrendamiento a distintos precios: €189 al mes, €355 por dos meses, €899 por seis meses o como una compra única de por vida por €1500.

> *«Los archivos .LNK son archivos de acceso directo que hacen referencia a otros archivos, carpetas o aplicaciones para abrirlos. El atacante aprovecha los .LNK y lanza cargas útiles maliciosas usando LOLBins»,* dijeron los investigadores de Cyble en un informe.

Se cree que las primeras pruebas de muestra de malware que usan Quantum Builder en la naturaleza datan del 24 de mayo, y se hacen pasar por archivos de texto de apariencia inofensiva («test.txt.lnk»).

> *«De forma predeterminada, Windows oculta la extensión .LNK, por lo que si un archivo tiene el nombre file_name.txt.lnk, el usuario solo verá file_name.txt, incluso si la opción Mostrar extensión de archivo está habilitada. Por tales razones, esta podría ser una opción atractiva para los TA, utilizando los archivos .LNK como disfraz o cortina de humo»*, dijeron los investigadores.

Al iniciar el archivo .LNK, se ejecuta el código de PowerShell que, a su vez, ejecuta un archivo de aplicación HTML («bdg.hta») alojado en el sitio web de Quantum («quantum-software[.]online») mediante MSHTA, una utilidad legítima de Windows que se utiliza para

ejecutar los archivos HTA.

Al parecer, Quantum Builder comparte vínculos con Lazarus Group, con sede en Corea del Norte, en función a las superposiciones de nivel de código fuente en la herramienta y el modus operandi de este último para aprovechar los archivos .LNK con el fin de entregar más cargas útiles en el escenario, lo que indica su uso potencial por parte de los actores de APT en sus ataques.

Este desarrollo se produce cuando los operadores detrás de Bumblebee y Emotet están cambiando a archivos .LNK como conducto para desencadenar las cadenas de infección después de la decisión de Microsoft de deshabilitar las macros de Visual Basic para aplicaciones (VBA) de forma predeterminada en todos sus productos a inicios del año.

Bulmblebee, un reemplazo del malware BazarLoader, descubierto por primera vez en marzo, funciona como puerta trasera diseñada para dar a los atacantes acceso persistente a los sistemas comprometidos y un descargador de otro malware, incluyendo Cobalt Strike y Sliver.

Las capacidades del malware también lo convierten en una herramienta elegida por los hackers, con 413 incidentes de infección de Bumblebee en mayo de 2022, frente a los 41 de abril, según Cyble.

> *«Bumblebee es un cargador de malware nuevo y altamente sofisticado, que emplea maniobras evasivas extensas y trucos antianálisis, incluyendo técnicas complejas antivirtualización. Es posible que se convierta en una herramienta popular para que los grupos de ransomware entreguen su carga útil»*, dijeron los investigadores.