Los piratas informáticos están utilizando una técnica novedosa para encontrar formas de utilizar el Servicio de Transferencia Inteligente en Segundo Plano (BITS) de Microsoft, con el fin de implementar cargas útiles maliciosas en máquinas con Windows de forma sigilosa.

En 2020, los hospitales, las comunidades de jubilados y los centros médicos fueron los más afectados por una campaña de phishing en constante cambio que distribuyó puertas traseras personalizadas como KEGTAP, que finalmente allanó el camino para los ataques del ransomware RYUK.

Sin embargo, una nueva investigación del brazo forense cibernético Mandiante de FireEye, ahora reveló un mecanismo de persistencia previamente desconocido que muestra que los adversarios hicieron uso de BITS para lanzar la puerta trasera.

Introducido en Windows XP, BITS es un componente de Microsoft Windows que hace uso del ancho de banda inactivo de la red para facilitar la transferencia asincrónica de archivos entre máquinas. Esto se logra al crear un trabajo, un contenedor que incluye los archivos para descargar o cargar.

BITS se utiliza comúnmente para entregar actualizaciones del sistema operativo a los clientes, así como también el escáner de antivirus de Windows Defender para buscar actualizaciones de firmas de malware. Además de los productos propios de Microsoft, el servicio también es utilizado por otras aplicaciones como Mozilla Firefox para permitir que las descargas sigan en segundo plano aún cuando el navegador está cerrado.

> *«Cuando las aplicaciones maliciosas crean trabajos BITS, los archivos se descargan o cargan en el contexto del proceso del host de servicio. Esto puede ser útil para evadir firewall que pueden bloquear procesos maliciosos o desconocidos, y ayuda a ocultar qué aplicación solicitó la transferencia»,* dijeron los investigadores de FireEye.

Específicamente, se encontró que los incidentes posteriores al compromiso que involucraron

infecciones de Ryuk aprovecharon el servicio BITS para crear un nuevo trabajo como una *«Actualización del sistema»*, que se configuró para iniciar un ejecutable llamado mail.exe, que a su vez, activó la puerta trasera KEGTAP, luego de intentar descargar una URL no válida.

> *«El trabajo malicioso de BITS se configuró para intentar una transferencia HTTP de un archivo inexistente desde el host local. Como este archivo nunca existiría, BITS desencadenaría el estado de error y lanzaría el comando de notificación, que en este caso era KEGTAP»,* dijeron los investigadores.

El nuevo mecanismo es otro recordatorio de cómo los atacantes pueden reutilizar una herramienta útil como BITS en su propio beneficio. Para ayudar en la respuesta a incidentes y las investigaciones forenses, los investigadores también pusieron a disposición una utilidad de Python llamada BitsParser, que tiene como objetivo analizar archivos de base de datos BITS y extraer información de trabajos y archivos para análisis adicional.