Un grupo de investigadores de seguridad descubrieron un nuevo virus informático asociado con el grupo de espionaje cibernético Stealth Falcon, patrocinado por el estado, que abusa de un componente integrado del sistema operativo Microsoft Windows para filtrar de forma sigilosa los datos robados al servidor controlado por el atacante.

Activo desde 2012, Stealth Falcon es un grupo de piratería sofisticado conocido por atacantes a periodistas, activistas y disidentes con spyware en el Medio Oriente, principalmente en los Emiratos Árabes Unidos (EAU).

Nombrado como Win32/StealthFalcon, llamado así por el grupo de piratería, el malware se comunica y envía los datos recopilados a sus servidores remotos de comando y control (C&C) utilizando el Servicio de Transferencia Inteligente en segundo plano de Windows (BITS).

BITS es un protocolo de comunicación en Windows que utiliza el ancho de banda de red no utilizado para facilitar la transferencia asíncrona, priorizada y acelerada de archivos entre máquinas en primer plano o en segundo plano, sin afectar la experiencia de la red.

Es muy utilizado por los actualizaciones de software, incluida la descarga de archivos de los servidores o pares de Microsoft para instalar actualizaciones en Windows 10, mensajeros y otras aplicaciones diseñadas para operar en segundo plano.

Según los investigadores de seguridad de la compañía de seguridad cibernética ESET, ya que las tareas BITS son más probables permitidas por los firewalls basados en host y la funcionalidad ajusta de forma automática la velocidad de transferencia de datos, permite que el malware opere sigilosamente en segundo plano sin levantar ninguna señal de alerta.

> *«En comparación con la comunicación tradicional por medio de funciones API, el mecanismo BITS está expuesto a travées de una interfaz COM, y por lo tanto, es más difícil de detectar para un producto de seguridad. La transferencia se reanuda automáticamente luego de ser interrumpida por razones como una interrupción de la red, el cierre de sesión del usuario o un reinicio del sistema»,* dijeron los

> investigadores.

Además, en lugar de filtrar los datos recopilados en texto plano, el malware primero crea una copia encriptada y luego carga la copia al servidor de comando y control por medio del protocolo BITS.

Después de extraer con éxito los datos robados, el malware elimina de forma automática todos los archivos de registro y recopilados luego de reescribirlos con datos aleatorios para evitar el análisis forense y la recuperación de los datos eliminados.

Como se explica en el informe, la puerta trasera Win32/StealthFalcon no solo ha sido diseñada para robar datos de los sistemas comprometidos, sino que también puede ser utilizada por los atacantes para desplegar más herramientas maliciosas y actualizar su configuración enviando comandos por medio del servidor C&C.

> *«La puerta trasera Win32/StealthFalcon, que parece haber sido creada en 2015, permite al atacante controlar la computadora comprometida de forma remota. Hemos visto un pequeño número de objetivos en EAU, Arabia Saudita, Tailandia y los Países Bajos, en este último caso, el objetivo era una misión diplomática de un país del Medio Oriente»,* dijeron los investigadores.

Según los investigadores, el malware recientemente descubierto comparte sus servidores C&C y su base de código con una puerta trasera basada en PowerShell atribuida al grupo Stealth Falcon y rastreada por Citizen Lab en 2016.