Investigadores de seguridad cibernética descubrieron un nuevo troyano de acceso remoto (RAT), que parece ser obra de un grupo de amenaza especializado en ataques contra objetivos gubernamentales y diplomáticos.

El jueves, investigadores de Cisco Talos, dijeron que el malware denominado como ObliqueRAT, se está implementando en una nueva campaña centrada en objetivos del sudeste asiático.

La última campaña comenzó en enero de 2020 y sigue. Los ciberdelincuentes detrás del esquema usan correos electrónicos de phishing como el principal vector de ataque, con documentos maliciosos de Microsoft Office adjuntos a los correos electrónicos fraudulentos diseñados para implementar la RAT.

Los archivos adjuntos tienen nombres que parecen inofensivos, como Company_Terms.doc o DT_JD_GM.doc, puede puede significar *«Departamento de Telecomunicaciones_Descripción del Trabajo_Gerente General».*

La protección con contraseña está implementada, una técnica que puede diseñarse para tratar de hacer que los documentos parezcan legítimos y seguros en entornos corporativos. Las credenciales necesarias para abrir el archivo probablemente estén contenidas en el cuerpo principal del correo electrónico de phishing.

Si la víctima ingresa la contraseña y abre el documento, un script VB malicioso se ejecutará, extrayendo un binario malicioso y soltando un ejecutable que actúa como gotero para ObliqueRAT.

La persistencia se mantiene mediante la creación de un proceso de inicio para el ejecutable cada vez que se reinicia el sistema comprometido.

Talos considera que el RAT es *«simple»* y contiene la funcionalidad principal de un troyano típico, incluida la capacidad de extraer archivos y datos del sistema para transferirlos a un servidor de comando y control (C2), funcionalidad para descargar y ejecutar cargas útiles

adicionales, y la capacidad de terminar procesos existentes.

Sin embargo, una característica interesante es que el malware busca un directorio particular para capturar los archivos que residen dentro. El nombre del directorio C:\ProgramData\System\Dump, está codificado.

> *«El RAT asegura que solo una instancia de su proceso se ejecute en el punto final infectado en cualquier momento dado al crear y verificar un mutex llamado Oblique. Si el mutex nombrado ya existe en el punto final, el RAT dejará de ejecutarse hasta el siguiente inicio de sesión de la cuenta de usuario infectada»,* dijeron los investigadores.

Para evitar la detección y los esfuerzos de ingeniería inversa, el malware también verificará el nombre del sistema y la información en busca de indicios de que la PC esté protegida, como el uso de la *«prueba»* de nombre de usuario.

Según Talos, las similitudes entre cómo se está extrayendo el RAT y dentro de las variables de script VBA utilizadas en los documentos maliciosos sugieren un posible vínculo con CrimsonRAT, un grupo previamente conectado a ataques contra organizaciones dimplomáticas y políticas en la misma región.

> *«Esta campaña muestra a un actor de amenazas que realiza una distribución dirigida de maldocs similares a los utilizados en la distribución de CrimsonRAT. Sin embargo, lo que destaca aquí es que el actor ahora está distribuyendo una nueva familia de RATS. Aunque no es técnicamente sofisticado, ObliqueRAT consiste en una gran cantidad de capacidades que se pueden usar para llevar a cabo diversas actividades maliciosas en el punto final infectado»*, dijo Talos.