



Investigadores de seguridad cibernética descubrieron hoy una nueva versión avanzada de ComRAT, una de las backdoors conocidas más antiguas utilizadas por el grupo Turla APT, que aprovecha la interfaz web de Gmail para recibir comandos de forma encubierta y filtrar datos confidenciales.

«ComRAT v4 se vio por primera vez en 2017 y se sabe que sigue en uso desde enero de 2020. Identificamos al menos tres objetivos: dos Ministerios de Relaciones Exteriores en Europa del Este y un parlamento nacional en la región del Cáucaso», dijo [ESET](#) en un informe.

[Turla](#), también conocida como Snake, ha estado activa por más de diez años con un largo historial y campañas de phishing contra embajadas y organizaciones militares desde al menos 2004.

La plataforma de espionaje del grupo comenzó como Agent.BTZ, en 2007, antes de evolucionar a [ComRAT](#), además de obtener capacidades adicionales para lograr persistencia y robar datos de una red local.

Ahora se sabe que las versiones anteriores de Agent.BTZ fueron responsables de infectar las redes militares de Estados Unidos en el Medio Oriente en 2008. En los últimos años, se dice que Turla estuvo detrás del compromiso de las Fuerzas Armadas francesas en 2018 y el Ministerio de Relaciones Exteriores de Austria a inicios de 2020.

Las versiones más recientes de la puerta trasera ComRAT abandonaron el Agente, el mecanismo de infección de memoria USB de BTZ a favor de inyectarse en cada proceso de la máquina infectada y ejecutar su carga principal en explorer.exe.

Lo nuevo en ComRAT v4

El ComRAT v4 (o «Chinch», por los autores del malware), utiliza una base de código



completamente nueva y es mucho más complejo que sus variantes anteriores, según ESET. La compañía dijo que la primera muestra conocida del malware fue detectada en abril de 2017.

Por lo general, ComRAT se instala por medio de [PowerStallion](#), una puerta trasera PowerShell liviana utilizada por Turla para instalar otras puertas traseras. Además, el cargador PowerShell inyecta el módulo ComRAT Orchestrator en el navegador web, que emplea dos canales diferentes, un modo heredado y un modo de correo electrónico, para recibir comandos de un servidor C2 y filtrar información de los operadores.



«El uso principal de ComRAT es descubrir, robar y filtrar documentos confidenciales. En un caso, sus operadores incluso desplegaron un ejecutable .NET para interactuar con la base de datos MS SQL Server central de la víctima que contiene los documentos de la organización», dijeron los investigadores.

Además, todos los archivos relacionados con ComRAT, con la excepción de la DLL del orquestador y la tarea programada para la persistencia, se almacenan en un sistema de archivos virtual (VFS).

El modo «mail» funciona al leer la dirección de correo electrónico y las cookies de autenticación ubicadas en el VFS, conectándose a la vista HTML básica de Gmail y analizando la página HTML de la bandeja de entrada (usando el [analizador HTML Gumbo](#)), para obtener la lista de correos electrónicos con líneas de asunto que coinciden con los de un archivo «subject.str» en el VFS.

Para cada correo electrónico que cumpla con los criterios anteriores, el ComRAT procede descargando los archivos adjuntos (por ejemplo, «documento.docx») y eliminando los correos electrónicos para evitar procesarlos por segunda vez.



A pesar del formato «.docx» y «.xlsx» en los nombres de archivo, los archivos adjuntos no son documentos en sí, sino bloques de datos cifrados que incluyen un comando específico para ejecutar: leer/escribir archivos, ejecutar procesos adicionales y recopilar registros.

En la etapa final, los resultados de la ejecución del comando se cifran y almacenan en un archivo adjunto (con la doble extensión «.jpg.bfe»), que luego se envía como un correo electrónico a una dirección de destino especificada en «answer_add.str».

Por otro lado, el modo «heredado» utiliza la infraestructura C2 ya existente (ComRAT v3.x) para emitir comandos remotos, cuyos resultados se comprimen y transmiten a un servicio en la nube como Microsoft OneDrive o 4Shared.

Los datos filtrados comprenden detalles del usuario y archivos de registro relacionados con la seguridad para verificar si sus muestras de malware se detectaron durante un análisis de los sistemas infectados.

Basado en los patrones de distribución de correo electrónico de Gmail durante un período de un mes, ESET dijo que los operadores detrás de la campaña están trabajando en las zonas horarias UTC +3 o UTC +4.

«La versión cuatro de ComRAT es una familia de malware totalmente renovada lanzada en 2017. Sus características más interesantes son el Sistema de Archivos Virtual en formato FAT16 y la capacidad de usar la interfaz de usuario web de Gmail para recibir comandos y filtrar datos. Por lo tanto, puede eludir algunos controles de seguridad porque no depende de ningún dominio malicioso», dijo Matthieu Faou, investigador de ESET.