Investigadores de seguridad cibernética publicaron los detalles de una puerta trasera y un ladrón de documentos previamente indocumentados que se han implementado contra objetivos específicos desde 2015 hasta principios de 2020.

Con el nombre clave de «Crutch» por los investigadores de ESET, el malware se ha atribuido a Turla (también conocido como Venomous Bear o Snake), un grupo de hackers avanzados con sede en Rusia conocido por sus extensos ataques contra gobiernos, embajadas y organizaciones militares a través de distintos abrevaderos y campañas de phishing.

> *«Estas herramientas fueron diseñadas para filtrar documentos confidenciales y otros archivos a cuentas de Dropbox controladas por los operadores de Turla»,* dijo la compañía en un análisis.

Los implantes de la backdoor se instalaron en secreto en varias máquinas pertenecientes al Ministerio de Relaciones Exteriores en un país anónimo de la Unión Europea.

Además de identificar fuertes vínculos entre una muestra de Crutch de 2016 y otra puerta trasera de segunda etapa de Turla llamada Gazer, el último malware en su conjunto de herramientas diverso apunta al enfoque continuo del grupo en el espionaje y el reconocimiento contra objetivos de alto perfil.

Crutch se entrega por medio de la suite Skipper, un implante de primera etapa previamente atribuido a Turla, o un agente de post-explotación llamado PowerShell Empire, con dos versiones distintas del malware detectadas antes y después de mediados de 2019.

Mientras que el primero incluía una puerta trasera que se comunica con una cuenta de Dropbox codificada mediante la API HTTP oficial para recibir comando y cargar los resultados, la variante más nueva («Crutch v4») evita la configuración de una nueva función que puede cargar de forma automática los archivos encontrados en unidades locales y extraíbles a Dropbox mediante la utilidad Wget de Windows.

> *«La sofisticación de los ataques y los detalles técnicos del descubrimiento fortalecen aún más la percepción de que el grupo Turla tiene recursos considerables para operar un arsenal tan grande y diverso»*, dijo Matthieu Faou, investigador de ESET.

> *«Además, Crutch puede eludir algunas capas de seguridad al abusar de la infraestructura legítima, en este caso, Dropbox, para integrarse en el tráfico normal de la red mientras filtra los documentos robados y escribe comandos de sus operadores»*, agregó.