Un grupo de hackers norcoreanos fue detectado desplegando el troyano RokRat en una nueva campaña de phishing dirigida al gobierno de Corea del Sur.

Al atribuir el ataque cibernético a APT37, también conocido como Starcruft, Ricochet Chollima o Reaper, Malwarebytes afirmó que identificó un documento malicioso en diciembre pasado que, al abrirse, ejecuta una macro en la memoria para instalar la mencionada herramienta de acceso remoto (RAT).

> *«El archivo contiene una macro incrustada que utiliza una técnica de autodescodificación de VBA para descodificarse a sí mismo dentro de los espacios de memoria de Microsoft Office sin escribir en el disco. Luego incrusta una variante de RokRat en el bloc de notas»,* dijeron los investigadores este miércoles.

El grupo está activo al parecer desde 2012, conocido por sus enfoques en entidades públicas y privadas principalmente en Corea del Sur, como entidades químicas, electrónicas, manufactureras, aeroespaciales, automotrices y de salud. Desde entonces, su victimología se ha expandido más allá de la península de Corea para incluir a Japón, Vietnam, Rusia, Nepal, China, India, Rumania, Kuwuait y otras partes del Medio Oriente.

Aunque los ataques anteriores aprovecharon los documentos del procesador de texto Hangul (HWP) con malware, el uso de archivos de Office VBA de autodescodificación para entregar RokRat sugiere un cambio en las tácticas para APT37, según los investigadores.

El documento de Microsoft VBA subido a VirusTotal en diciembre, pretendía ser una convocatoria de reunión fechada el 23 de enero de 2020, lo que implica que los ataques tuvieron lugar hace casi un año.

La principal de las responsabilidades de la macro incrustada en el archivo es inyectar

shellcode a un proceso Notepad.exe, que descarga la carga útil de RokRat en formato cifrado desde una URL de Google Drive.

RokRat, documentado públicamente por Cisco Talos en 2017, es una RAT de elección para APT37, y el grupo la utiliza para varias campañas desde 2016. Una puerta trasera basada en Windows distribuida a través de documentos troyanizados, es capaz de realizar capturas de pantalla, registrar pulsaciones de teclas, evadir el análisis con detecciones de máquinas virtuales y aprovechar las API de almacenamiento en la nube como Box, Dropbox y Yandex.

En 2019, la RAT basada en el servicio en la nube obtuvo funciones adicionales para robar información de dispositivos Bluetooth como parte de un esfuerzo de recopilación de inteligencia dirigido contra empresas de inversión y comercio en Vietnam y Rusia, y una agencia diplomática en Hong Kong.

> *«El caso que analizamos es uno de los pocos en los que no utilizaron archivos HWP como sus documentos de phish y en su lugar utilizaron documentos de Microsoft Office armados con una macro de autodescodificación. Esa técnica es una elección inteligente que puede eludir varios mecanismos de detección estática y ocultar la intención principal de un documento malicioso»,* agregaron los investigadores.