Se ha observado que tres distintos actores de amenazas patrocinados por el estado, alineados con China, India y Rusia, están adoptando un nuevo método llamado inyección de plantilla RTF (también conocido como formato de texto enriquecido), como parte de sus campañas de phishing para enviar malware a sistemas específicos.

> *«La inyección de plantillas RTF es una técnica novedosa que es ideal para archivos adjuntos de phishing maliciosos porque es simple y permite a los actores de amenazas recuperar contenido malicioso de una URL remota usando un archivo RTF»,* dijeron los investigadores de Proofpoint en un informe.

En el centro del ataque se encuentra un archivo RTF que tiene contenido de señuelo que puede manipularse para permitir la recuperación de contenido, incluyendo cargas útiles maliciosas, alojado en una URL externa al abrir un archivo RTF.

Específicamente, aprovecha la funcionalidad de plantilla RTF para alterar las propiedades de formato de un documento utilizando un editor hexadecimal al especificar un recurso de URL en lugar de un destino de recurso de archivo accesible desde el cual se puede recuperar una carga útil remota.

En otras palabras, la idea es que los atacantes puedan enviar documentos maliciosos de Microsoft Word a víctimas específicas que parecen completamente inocuas, pero que están diseñadas para cargar código malicioso por medio de la función de plantilla remotamente. Esto hace que el mecanismo sea un método duradero y eficaz cuando se combina con el phishing como vector de entrega inicial.

Por lo tanto, cuando se abre un archivo RTF alterado a través de Microsoft Word, la aplicación procederá a descargar el recurso desde la URL especificada antes de mostrar el contenido atractivo del archivo. Por lo tanto, no es sorprendente que los atacantes estén armando cada vez más la técnica para distribuir malware.

Proofpoint dijo que observó archivos RTF de inyección de plantillas vinculados a los grupos de APT DoNot Team, Gamaredon y un actor de APT relacionado con China apodado TA423 en febrero de 2021, y que los adversarios utilizaron los archivos para apuntar a entidades en Pakistán, Sri Lanka, Ucrania y aquellos que operan en el sector de exploración de energía en aguas profundas en Malasia a través de señuelos con temas de defensa y otros señuelos específicos de cada país.

Aunque se sospecha que el equipo DoNot Team lleva a cabo ataques cibernéticos alineados con los intereses del estado indio, Gamaredon fue recientemente denunciado por la policía ucraniana como un equipo conectado al Servicio Federal de Seguridad de Rusia (FSB), con una propensión a atacar a organizaciones del sector público y privado en el país para recolectar información clasificada de sistemas Windows comprometidos para obtener ganancias geopolíticas.

> *«La innovación de los actores de amenazas para llevar a este método a un nuevo tipo de archivo en RTF representa una superficie de amenaza en expansión para las organizaciones de todo el mundo. Si bien este método es utilizado actualmente por un número limitado de actores de APT con un rango de sofisticación, la efectividad de la técnica combinada con su facilidad de uso probablemente impulse su adopción en todo el panorama de amenazas»,* dijeron los investigadores.