Publicado en Madrid el 20/02/2019

Rusia se convierte en el objetivo del grupo de cibercriminales Lazarus

Este grupo de cibercriminales está detrás de algunas de las mayores violaciones de seguridad de la última década, como el ataque a Sony Pictures Entertainment, el atraco al banco de Bangladesh o el robo de millones de dólares en criptomonedas de al menos cinco casas de cambio diferentes en todo el mundo

En las últimas semanas, el equipo de investigadores de Check Point ha estado vigilando actividades sospechosas dirigidas contra empresas privadas con sede en Rusia que revelan una nueva relación. Por primera vez, detectaron lo que parecía ser un ataque coordinado por Corea del Norte contra entidades rusas. 'A pesar de las dificultades para poder atribuir la autoría de los ciberataques, el análisis que hemos llevado a cabo revela una conexión intrínseca de las tácticas, técnicas y herramientas con el grupo norcoreano de la APT - Lazarus', informan desde Check Point.

Este descubrimiento se produjo al rastrear múltiples documentos Office maliciosos que fueron diseñados y elaborados específicamente para las víctimas rusas. Al examinar más de cerca estos archivos, el equipo US-CERT descubrió que pertenecían a las primeras etapas de una cadena de infección que finalmente condujo a una variante actualizada de KEYMARBLE, una versátil puerta trasera de Lazarus.

Lazarus, también conocido como la Cobra Oculta, es uno de los grupos de APT más activos en la actualidad. Se cree que este grupo de cibercriminales, conocido por ser un actor de ciberamenazas patrocinado por Corea del Norte, está detrás de algunas de las mayores violaciones de seguridad de la última década. Esto incluye el ataque a Sony Pictures Entertainment, el atraco al banco de Bangladesh y muchas otras operaciones de alto riesgo, como el robo de millones de dólares en criptomonedas de al menos cinco casas de cambio diferentes en todo el mundo.

Este incidente, sin embargo, representa una elección inusual de víctima por parte del actor amenazador norcoreano. Por lo general, estos ataques reflejan las tensiones geopolíticas entre la República Popular Democrática de Corea y países como Estados Unidos, Japón y Corea del Sur. En este caso, sin embargo, son las organizaciones rusas las que están en el punto de mira.

La comunidad de seguridad cree desde hace mucho tiempo que Lazarus se compone de dos subdivisiones: la primera se llama Andariel y se centra principalmente en atacar al gobierno y las organizaciones de Corea del Sur, y la segunda es Bluenoroff, cuyo enfoque principal es la monetización y las campañas mundiales de espionaje.

Las diferencias entre las dos campañas, que se llevaron a cabo al mismo tiempo, refuerzan una vez más la teoría de que existen múltiples divisiones.

Este incidente, llevado a cabo por parte del actor norcoreano, supone un cambio en la elección de las víctimas, ya que nunca antes sus objetivos habían sido entidades rusas. Estos ataques solían reflejar la tensión geopolítica entre la República Popular Democrática de Corea y otras naciones como los Estados Unidos, Japón y Corea del Sur.

Cadena de infección
Según los investigadores de Check Point, el flujo principal de infección en este tipo de ataques se basa en 3 pasos principalmente:

1. Un archivo ZIP que contiene dos documentos: un documento PDF benigno y un documento de Word malicioso con macros.

2. Las macros maliciosas descargan un script VBS desde una URL de Dropbox, seguido de la ejecución del script VBS.

3. El script VBS descarga un archivo CAB del servidor de la dropzone, extrae el archivo EXE incrustado (backdoor) usando la utilidad 'expandir.exe' de Windows, y finalmente lo ejecuta.

Al principio, la cadena de infección seguía todos los pasos, pero en un momento dado, los ciberdelincuentes decidieron saltarse la segunda etapa, y las macros maliciosas de Word fueron modificadas para 'descargar y ejecutar' directamente la puerta trasera de Lazarus en la tercera etapa.

Datos de contacto:
Jorge Aguado

Nota de prensa publicada en: Madrid

Categorías: Internacional Nacional Sociedad Programación Ciberseguridad