Expertos en seguridad digital han identificado una reciente vulnerabilidad en Apple macOS denominada SpectralBlur que coincide con un tipo de software malicioso ya conocido y atribuido a actores cibernéticos de Corea del Norte.

> *«SpectralBlur es una puerta trasera con capacidades intermedias que permite la subida y bajada de archivos, la ejecución de comandos, la actualización de su configuración, la eliminación de archivos y la capacidad de entrar en modo hibernación o reposo, todo basado en instrucciones recibidas desde el servidor de mando y control»,* comentó el investigador en seguridad Greg Lesnewich.

El comportamiento del software malicioso presenta similitudes con KANDYKORN (también conocido como SockRacket), un programa avanzado que actúa como un troyano de acceso remoto con capacidad para dominar un equipo comprometido.

Es importante mencionar que las acciones relacionadas con KANDYKORN también coinciden con otra serie de actividades lideradas por el subgrupo Lazarus, denominado BlueNoroff (conocido también como TA444), que se centra en la implementación de una puerta trasera llamada RustBucket y una funcionalidad avanzada llamada ObjCShellz.

Recientemente, se ha observado que los responsables del software malicioso combinan elementos de ambas cadenas de infección, utilizando herramientas como RustBucket para distribuir KANDYKORN.

Estos hallazgos indican que los actores cibernéticos de Corea del Norte están ampliando sus objetivos hacia los sistemas macOS, enfocándose especialmente en sectores como el de las criptomonedas y tecnologías blockchain.

> *«TA444 sigue evolucionando rápidamente con estas nuevas variantes de software malicioso para macOS»*, destacó Lesnewich.

Patrick Wardle, otro experto en seguridad, proporcionó detalles adicionales sobre SpectralBlur, mencionando que este programa malicioso fue analizado por primera vez en el servicio de escaneo de malware VirusTotal en agosto de 2023 desde una ubicación en Colombia.

Las características compartidas entre KANDYKORN y SpectralBlur sugieren la posibilidad de que ambos programas hayan sido desarrollados por diferentes equipos con objetivos similares.

Lo que diferencia a SpectralBlur es su capacidad para dificultar el análisis y evitar ser detectado, utilizando grantpt para establecer un terminal simulado y ejecutar comandos remotos desde el servidor C2.

Estos descubrimientos llegan en un contexto en el que se identificaron un total de 21 nuevas variantes de software malicioso diseñadas para atacar sistemas macOS, incluyendo software de rescate, programas para robar información, troyanos de acceso remoto y software malicioso respaldado por estados en 2023, un aumento con respecto a las 13 variantes identificadas en 2022.

> *«Con la creciente popularidad de macOS, especialmente en el ámbito corporativo, es probable que 2024 vea un aumento en el número de variantes de software malicioso dirigidas a esta plataforma»*, señaló Wardle.