Un subconjunto dentro del conocido Grupo Lazarus ha establecido recientemente una infraestructura nueva que simula ser portales de evaluación de habilidades como parte de sus estrategias de ingeniería social.

Microsoft atribuyó esta actividad a un actor de amenazas al que denomina Sapphire Sleet, describiéndolo como un *«cambio en las tácticas del actor persistente».*

Sapphire Sleet, también conocido como APT38, BlueNoroff, CageyChameleon y CryptoCore, tiene un historial de dirigir robos de criptomonedas mediante la ingeniería social.

En los últimos días, Jamf Threat Labs vinculó al actor de amenazas con una nueva familia de malware para macOS llamada ObjCShellz, la cual se considera una carga útil en una etapa avanzada y se entrega en conexión con otro malware para macOS conocido como RustBucket.

> *«Usualmente, Sapphire Sleet identifica objetivos en plataformas como LinkedIn y utiliza señuelos relacionados con la evaluación de habilidades»*, informó el equipo de inteligencia de amenazas de Microsoft en una serie de publicaciones en X (anteriormente Twitter).

> *«Posteriormente, el actor de amenazas traslada las comunicaciones exitosas con los objetivos a otras plataformas».*

La empresa tecnológica indicó que campañas anteriores realizadas por este grupo de hackers implicaron el envío directo de archivos maliciosos o la inserción de enlaces a páginas alojadas en sitios web legítimos como GitHub.

No obstante, la detección y eliminación rápida de estas cargas útiles podrían haber obligado a Sapphire Sleet a expandir su propia red de sitios web para la distribución de malware.

> *«Varios dominios y subdominios maliciosos hospedan estos sitios web, los cuales atraen a los reclutadores a registrarse para obtener una cuenta. Estos sitios web están protegidos con contraseña para complicar el análisis»,* añadió la empresa.