Los expertos en ciberseguridad han identificado una nueva versión, más sofisticada y difícil de detectar, de un malware diseñado específicamente para macOS, conocido como Banshee Stealer.

> *«Después de que su código fuente se filtrara a finales de 2024, lo que llevó a pensar que estaba inactivo, esta nueva variante ha implementado un avanzado sistema de cifrado de cadenas inspirado en XProtect de Apple. Este avance le permite eludir la detección por parte de los antivirus, representando una amenaza considerable para más de 100 millones de usuarios de macOS en todo el mundo»*, señaló Check Point Research en un informe.

La empresa descubrió esta nueva variante en septiembre de 2024. El malware se distribuye mediante sitios web de phishing y repositorios falsos en GitHub que simulan ofrecer programas legítimos como Google Chrome, Telegram y TradingView.

Banshee Stealer fue documentado inicialmente en agosto de 2024 por Elastic Security Labs. Este malware se comercializaba bajo un modelo de *«malware como servicio»* (MaaS) a ciberdelincuentes, con un costo mensual de $3,000. Su funcionalidad incluye la recolección de datos de navegadores, monederos de criptomonedas y archivos con extensiones específicas.

En noviembre de 2024, el malware enfrentó un revés significativo cuando su código fuente fue filtrado en línea, lo que provocó el cierre de sus operaciones originales. Sin embargo, Check Point ha detectado varias campañas que continúan distribuyendo el malware a través de sitios fraudulentos, aunque no se ha confirmado si estas están relacionadas con clientes anteriores.

Entre los cambios más notables de esta nueva versión está la eliminación de una función que verificaba si el idioma del sistema era ruso, diseñada originalmente para evitar infectar dispositivos configurados con este idioma. Este cambio indica que los actores detrás del malware podrían estar buscando expandir su alcance a una base de víctimas más amplia.

Otra actualización clave es la adopción de un algoritmo de cifrado de cadenas basado en el motor antivirus XProtect de Apple, lo que permite ocultar las cadenas de texto que en la versión anterior estaban expuestas.

> *«Las campañas de malware actuales aprovechan vulnerabilidades humanas más que fallos técnicos específicos de una plataforma. macOS, al igual que otros sistemas operativos, no está exento de estas amenazas, especialmente cuando los atacantes emplean estrategias avanzadas como la ingeniería social o falsas actualizaciones de software»,* explicó Eli Smadja, líder del grupo de investigación de seguridad en Check Point Research.

Este descubrimiento coincide con un aumento en el uso de mensajes no deseados en Discord para propagar diferentes tipos de malware de robo de información, como Nova Stealer, Ageo Stealer y Hexon Stealer, disfrazados como pruebas de nuevos videojuegos.

> *«Un objetivo clave de estos stealers parece ser las credenciales de Discord, las cuales se utilizan para ampliar la red de cuentas comprometidas. Esto se ve reforzado porque la información robada a menudo incluye cuentas de amigos de las víctimas»*, indicó Malwarebytes.