28.04.2023

MacOS dans le viseur des rançongiciels

Le groupe de ransomware « Lockbit » serait en train de développer des logiciels de cryptage spécialement conçus pour s'en prendre aux systèmes d'exploitation d'Apple. Une première, si la nouvelle se confirme.

Une archive récemment découverte par Virustotal contenait, entre autres, une variante du ransomware LockBit ciblant le système d'exploitation macOS. La première analyse du fichier laisse à penser qu'il ne s'agit encore que d'une version test. En l'absence de certains certificats de confiance, macOS empêche en effet pour le moment l'exécution du programme malveillant. Qui plus est, un certain nombre d'erreurs de programmation empêchent encore LockBit de déployer toute sa puissance destructrice sur les systèmes macOS.

Actuellement, le risque pour les produits Apple est considéré comme faible. LockBit n'aurait en effet pas encore implémenté les fonctions nécessaires pour assurer un cryptage efficace des données.

Mais les utilisateurs d'Apple auraient tort de se croire en sécurité. Le porte-parole officiel du groupe de cybercriminels a en effet confirmé qu'une variante pour macOS de LockBit est en phase active de développement. LockBit est considéré comme le « leader de marché » des groupes de rançongiciels.

Comment les utilisateurs de produits macOS peuvent-ils se protéger ? En général, il convient d'appliquer les « 5 règles pour votre sécurité numérique » que vous pouvez retrouver [ici \(https://www.ebas.ch/5-schritte-fuer-ihre-digitale-sicherheit/\)](https://www.ebas.ch/5-schritte-fuer-ihre-digitale-sicherheit/). La particularité de macOS réside dans le fait que le pare-feu n'est pas activé par défaut. Il peut néanmoins être activé dans Préférences Système/Réseau/Coupe-feu.