Rapport menaces et incidents - CERT-FR

Une gestion de version détaillée se trouve à la fin de ce document.

Ces dernières semaines, l'ANSSI a observé plusieurs attaques impliquant le déploiement du rançongiciel Clop sur des systèmes d'information en France. Ce code malveillant chiffre les documents présents sur les SI et leur ajoute, suivant les versions, l'extension « .CIop » ou « .Clop ». Les analyses réalisées par l'ANSSI et ses partenaires montrent que le chiffrement des postes est précédé par des actions de propagation manuelle réalisées par l'attaquant au sein du réseau victime. Cette phase en amont du chiffrement dure plusieurs jours et signifie qu'il est possible de détecter certains signes de l'attaque avant le déclenchement du rançongiciel sur une grande partie du SI.

Ces attaques semblent être le résultat d'une vaste campagne d'hameçonnage ayant eu lieu autour du 16 octobre 2019 et liée au groupe cybercriminel TA505.

TÉLÉCHARGER LE RAPPORT

Gestion détaillée du document

le 22 novembre 2019
Version initiale
