[France] Retour d’expérience suite à une attaque par rançongiciel contre une structure de santé

cyberveille-sante.gouv.fr/cyberveille-sante/1821-france-retour-dexperience-suite-une-attaque-par-rancongiciel-contre-une

CERT Santé

Une structure de santé française a récemment été victime d’une attaque utilisant le rançongiciel Ncov. Les conséquences de cette attaque furent minimes car l’activité malveillante a rapidement été détectée et stoppée. Les fichiers chiffrés ont pu être restaurés, les sauvegardes n’ayant pas été impactées.

Le rançongiciel Ncov est une variante de Dharma, un ransomware présent depuis 2016. Il est nommé Ncov à cause de l'extension de fichier ajoutée lors du chiffrement de données. L’attaquant a accédé au réseau de la structure par RDP avec le compte ILS_ANONYMOUS_USER, un compte générique utilisé par le service ILS (Internet Locator Server) qui était autrefois utilisé pour Microsoft NetMeeting (dernière MàJ en 2007). Le chiffrement des données a eu lieu suite au dépôt d’exécutables dans le profil utilisateur.

La structure a pris plusieurs mesures correctives pour prévenir le risque d’une nouvelle attaque :

- Blocage du compte ILS_ANONYMOUS_USER ;
- Revue et restriction des accès aux serveurs RDP exposés sur Internet ;
- Mise en place d’une passerelle d’accès RDS limitant le nombre de serveurs visibles ;
- Revue et restriction des accès aux partages réseau ;
- Achat et distribution de PC portables pour tous les télétravailleurs avec accès sécurisé en VPN.

Pour plus de conseils concernant la sécurisation d’un réseau, nous vous suggérons de vous reporter aux guides de l’ANSSI tel que le guide d’hygiène informatique, le guide de sécurité de RDP ou la fiche sur la sécurisation de son exposition sur Internet.

Liens

Comment désinstaller le rançongiciel Ncov d'un ordinateur ?