Darkside et Defray : des ransomwares sur ESXi

Quel est le point commun entre Darkside et Defray ? Ces deux *ransomwares* ont chacun une version spécifique à ESXi. C'est en tout cas sur ce trait que CrowdStrike a choisi d'insister.

Darkside avait émergé en août 2020. À la baguette, un groupe cybercriminel qui visait initialement les terminaux point de vente. Il avait commencé à élargir son périmètre d'action au printemps, possiblement en réponse à la réduction d'activité dans le *retail* avec la pandémie.

La version ESXi du *ransomware* s'en prend à une dizaine de types de fichiers associés à des VM. Elle emploie un chiffrement en enveloppe qui implique l'algorithme ChaCha20 et une clé maîtresse RSA-4096. L'attaquant peut contrôler le processus pour gagner du temps en ne chiffrant que partiellement les fichiers – juste assez pour empêcher leur restauration.

vCenter, SSH… Les *ransomwares* ont les clés

Pour accéder aux serveurs ESXi, les attaquants utilisent la console vCenter, mais aussi SSH. Ils ont récupéré au préalable des identifiants, généralement à travers un contrôleur de domaine. Darkside vient alors se loger dans le dossier /tmp/, sous un nom générique. Il exploite les scripts VMware pour éteindre les VM et ainsi « libérer » les fichiers à chiffrer.
Plusieurs entreprises françaises figurent sur sa liste de victimes revendiquées. Les dernières en date son OMV System France (usinage de précision), Pénélope (agence d'hôte(sse)s d'accueil) et Wonderbox.

Defray, qu'on connaît aussi sous le nom de RansomEXX, prend lui aussi place dans /tmp/. Alors que sa version Windows s'exécute en mémoire. L'intrusion passe également par l'obtention préalable d'identifiants pour se connecter au serveur. Deux leviers : un module pour les récupérer dans les navigateurs et un autre pour les chercher dans la mémoire de l'hôte.

Une fois déposé, le *ransomware* s'assure un accès persistant en activant SSH. Il lui arrive de modifier le mot de passe root ou les clés SSH. Il est conçu pour accepter une commande qui lui dicte le chemin du dossier par lequel il doit commencer son chiffrement. Parmi ses capacités figure la désinstallation de l'utilitaire VMware Fault Domain Manager, destiné à relancer les VM qui crashent.

Photo d'illustration © Nmedia – Fotolia