Ragnar : le ransomware s'habille en VM

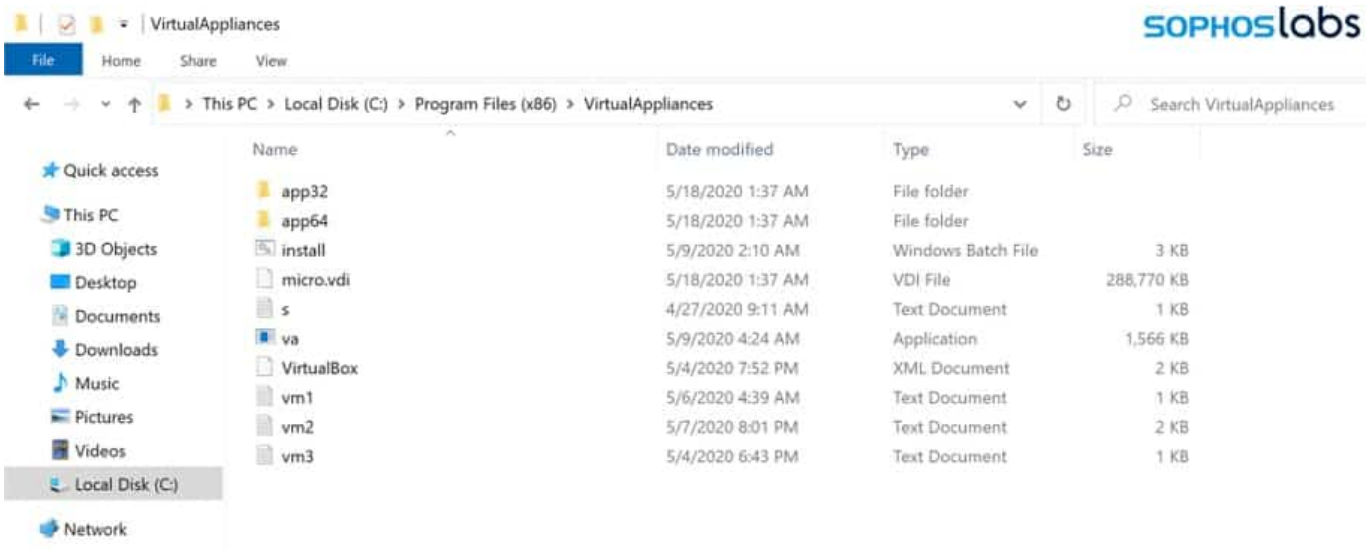
Comment se protéger des antivirus ? En se cachant dans une machine virtuelle. Des chercheurs de Sophos se sont intéressés à un *ransomware* qui exploite cette technique : Ragnar Locker.

On en a connaissance depuis fin 2019. Parmi ses victimes récentes figure le groupe Energias de Portugal. Les auteurs de l'attaque disent avoir pu récupérer puis chiffrer plus de 10 To de données.

La méthode « traditionnelle » pour exploiter Ragnar Locker consiste à exploiter des failles dans des logiciels d'infogérance. La latéralisation peut se faire à travers les objets de stratégie de groupe (GPO), destinés à appliquer des politiques de sécurité sur des systèmes Windows en environnement Active Directory.

La version que présente Sophos utilise les GPO pour exécuter le moteur d'installation MSI et télécharger un fichier à ce format (.msi).

Ce paquet comprend un installeur de Sun xVM VirtualBox (version 3.0.4, datée d'août 2009) et une image disque (.vdi) basée sur MicroXP 0.82, version « légère » de Windows XP SP3.
Le tout est copié dans C:\Program Files\[x86] \VirtualAppliances.



Inception

Ce sont les deux principales composantes de l'attaque, mais il y en a d'autres. Notamment un exécutable va.exe qui lance un script install.bat. Lequel :

- installe les DLL et les pilotes nécessaires pour VirtualBox ;
- désactive ensuite le service Windows Shell Hardware Detection, afin d'éviter l'affichage d'une fenêtre de lecture automatique ;
- supprime les éventuelles sauvegardes réalisées avec Shadow Copy, pour empêcher la restauration des fichiers qui seront chiffrés ;
- inscrit, dans un fichier de configuration (.xml), les disques locaux, les lecteurs réseau et les supports amovibles ;

- tue certains processus répertoriés dans deux listes (antivirus, applications métier, outils de *backup*, administration à distance…).

La VM se lance alors, en mode *headless*, avec 256 Mo de RAM, un vCPU et un disque virtuel de 299 Mo. Ragnar (vrun.exe) y est exécuté par l'intermédiaire d'un script (vrun.bat) lancé automatiquement au démarrage et qui monte, au préalable, les volumes détectés sur le système hôte. Il ne lui reste plus qu'à les chiffrer, à l'abri des logiciels de sécurité, qui ne voient que le processus VBoxHeadless.exe.

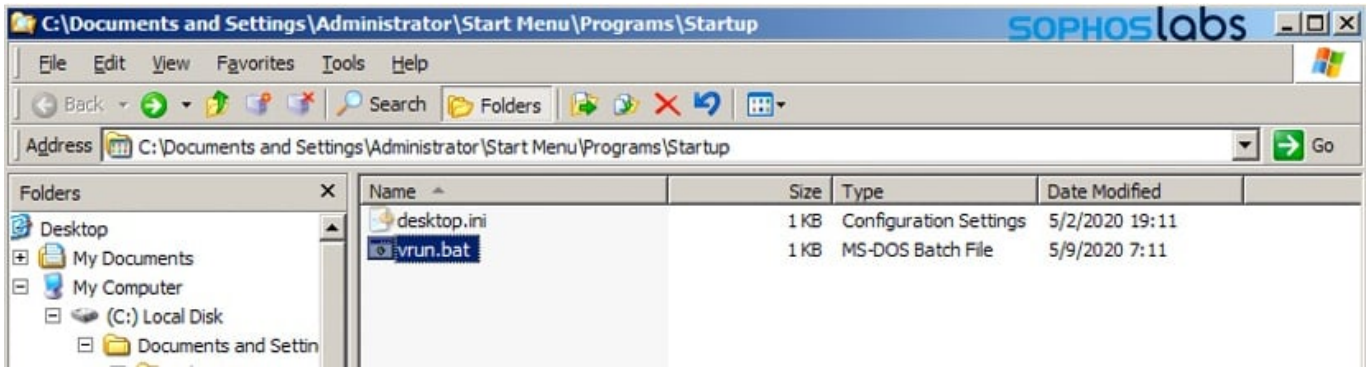


Illustration principale © Nmedia – Fotolia.com