RegretLocker : ce ransomware s'en prend aussi aux disques virtuels

Évasion par utilisation d'une instance virtuelle : c'est l'une des techniques cybercriminelles « défensives » répertoriée dans le *framework* ATT@CK de MITRE. On a vu des *ransomwares* en faire usage. En particulier Ragnar Locker.

L'alerte à ce sujet avait été donnée au printemps dernier. Levier d'attaque : les GPO (objets de stratégie de groupe), destinés à appliquer des politiques de sécurité sur des systèmes Windows en environnement Active Directory.

Détournés, ils ont servi à exécuter le moteur d'installation MSI pour télécharger un paquet malveillant. Celui-ci comportait deux éléments majeurs. D'une part, un installeur de Sun xVM VirtualBox (version 3.0.4, datée d'août 2009). De l'autre, une image disque (.vdi) basée sur MicroXP 0.82, version « légère » de Windows XP SP3.

Ragnar Locker se cachait dans cette VM. Son exécution se faisait par l'intermédiaire d'un script lancé automatiquement au démarrage. Ledit script avait monté, au préalable, les volumes détectés sur le système hôte. Ne restait plus qu'à les chiffrer, à l'abri des logiciels de sécurité. Lesquels ne voyaient que le processus VirtualBox, exécuté en mode *headless*.

Au cours de l'été, on a vu Maze adopter la même technique. Mais avec une VM plus volumineuse, fondée sur Windows 7 SP1.

RegretLocker : une autre approche de la virtualisation

La semaine passée a émergé un autre type de *ransomware*, qui fait également usage de la virtualisation, mais à des fins purement offensives. On lui a donné le nom de RegretLocker. Simple en apparence, il a une particularité : la capacité à chiffrer des fichiers sur des disques virtuels ; plus précisément ceux au format Hyper-V (VHD/VHDX).

Pour y parvenir, il exploite trois fonctionnalités de l'API Windows Virtual Storage : OpenVirtualDisk, AttachVirtualDisk et GetVirtualDiskPhysicalPath. Une clé de chiffrement est codée en dur au cas où RegretLocker ne parviendrait pas à joindre son serveur de contrôle (en .ru).

> *RegretLocker ransomware: a188e147ba147455ce5e3a6eb8ac1a46bdd58588de7af53d4ad542c6986491f4*
> *Extension: .mouse*
> *Note: HOW TO RESTORE FILES.TXT*
> *Mutex: svchost*
> *Interesting one...*
> *Can work w/ & w/o internet connection.*
> *Full of logging.*

> *Checks « WIN-295748OMAKG » – dev's PC?@demonslay335 pic.twitter.com/Avzp263ozz*
>
> *— MalwareHunterTeam (@malwrhunterteam) October 28, 2020*

Le *ransomware* semble s'inspirer d'une publication récente de la communauté vx-underground. Intitulée « Weaponizing Windows Virtualization », elle traite de l'exploitation d'ISO (images de disques optiques) à des fins malveillantes. Et laisse entendre que la même technique peut s'appliquer aux fichiers VHD.

> *Oh, that is the name of the paper by @smelly__vx . That also is the exact same code structure.*
>
> *Paper: https://t.co/wPl6RxWnrb https://t.co/bMYKnqSQUD*
>
> *— vx-underground (@vxunderground) November 3, 2020*

> *2020-11-03: □□□#RegretLocker #Ransomware □*
>
> *Weaponizes Windows Virtualization for Ransomware□*
> *1□open_virtual_drive*
> */**
> *OpenVirtualDisk□□AttachVirtualDisk□□ GetVirtualDiskPhysicalPath□□.□□*
> **/*
> *2□smb_scanner*
> *3□crypted_callback*
> *4□get_process_opened_file (Rm*)*
>
> *h/t @malwrhunterteam pic.twitter.com/uCRNahJbqP*
>
> *— Vitali Kremez (@VK_Intel) November 3, 2020*

*Photo d'illustration © newfilm.dk*via*Visualhunt / CC BY-NC-SA*