EFS : le chiffrement Windows victime d'un ransomware

Attention aux rançongiciels qui tireraient parti des outils de chiffrement intégrés à Windows.

SafeBreach vient d'émettre une alerte dans ce sens.

L'entreprise américaine a développé un *malware* de ce type. Et mis à l'épreuve trois solutions de sécurité, sur des machines virtuelles équipées de Windows 10 :

- ESET Internet Security 12.1.34.0
- Kaspersky Anti-Ransomware Tool for Business 4.0.0.861(a)
- Microsoft Windows 10 Controlled Folder Access

Au « premier jet », aucun de ces produits n'avait détecté le rançongiciel.

La situation s'est améliorée depuis lors, à en croire les éditeurs concernés.

SafeBreach avait pris contact avec eux à la mi-2019. Tout en sollicitant une quinzaine d'autres fournisseurs de solutions de sécurité.

Les leaders du marché (d'après le classement d'OPSWAT) ont tous livré une forme de correctif :

- Dans un e-mail du 7 octobre 2019, Symantec a déclaré avoir intégré des signatures à son offre Endpoint Protection.
- McAfee a signalé avoir intégré, en date du 10 janvier 2020, les protections adéquates dans ses produits grand public et entreprises.
- ESET a publié, le 21 janvier 2020, un bulletin annonçant que tous ses produits embarquant la technologie Ransomware Shield sont mis à jour.
- Bitdefender affirme, dans un e-mail du 10 janvier 2020, avoir amorcé le déploiement d'un correctif sur la version24.0.14.85 de ses produits Antivirus, Internet Security et Total Security.
- Avast a implémenté une « méthode de contournement » à partir de la version 19.8 de son antivirus (mail du 26 septembre 2019).

Discret… avec modération

EFS (Encrypting File System) est proposé depuis Windows 2000 sur les éditions du système d'exploitation destinées à un usage professionnel.
Il permet de chiffrer des fichiers et des dossiers à la demande – par opposition à Bitlocker, qui chiffre des volumes entiers.

Les opérations se font au niveau du pilote NTFS. Elles sont inivisibles pour l'utilisateur, qui n'a pas d'action à réaliser (la clé dépend en partie du mot de passe de la session Windows).

En exploitant les API cryptographiques de Windows, le rançongiciel de Safebreach :

- Génère une clé et mémorise le nom que la CryptoAPI donne à cette clé
- Génère un certificat et le stocke dans l'un des magasins de certificats de Windows
- Associe la clé EFS à ce certificat et peut alors chiffrer fichiers et dossiers
- Place la clé en RAM et la supprime du disque
- Vide le cache EFS, rendant les données inaccessibles par l'utilisateur et par l'OS
- Réalise éventuellement des opérations d'écriture sur le disque pour empêcher toute récupération de la clé EFS
- Récupère la clé en RAM… et la chiffre avec une clé tierce (celle de l'attaquant)

Le *malware* présente l'avantage de travailler à bas niveau, sans avoir besoin de privilèges particuliers (au contraire des rançongiciels qui s'en prennent à Bitlocker).

Son action est toutefois trahie par le cadenas jaune qui s'affiche en haut à droite sur l'icône des fichiers et dossiers chiffrés.

On peut par ailleurs le désactiver en coupant EFS (mettre la valeur 1 pour la clé de registre HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EFS\EfsConfiguration).

Autre solution : les agents de restauration, actifs par défaut sur les machines Windows reliées à des domaines.

Photo d'illustration © Infosec Images via *Visual hunt / CC BY*