

# Affaire Kaseya : le ransomware REvil attaque sur un air de SolarWinds

A-t-on affaire, avec Kaseya, à un « autre SolarWinds » ? Immanquablement, la question se pose. Mais de quoi parle-t-on vraiment ? D'une attaque que l'éditeur américain a signalée vendredi dernier. La cible : son logiciel de gestion informatique VSA. Celui-ci n'était toutefois qu'un intermédiaire, ouvrant la porte sur les SI de ses utilisateurs. À savoir, essentiellement, des MSP.

L'inquiétude ne porte pas tant sur la version SaaS de VSA – Kaseya a [passé](#) en mode maintenance les serveurs qui l'hébergent – que sur les installations *on-prem*. Le risque : la diffusion, chez les clients des MSP, d'un *ransomware* (REvil).

## Windows Defender détourné

Les privilèges dont VSA dispose sur les systèmes Windows visés facilite l'[infection](#). Dans les grandes lignes, elle se déroule ainsi :

- Compromission de serveurs VSA
- Diffusion d'une fausse mise à jour de l'agent VSA sur les machines connectées à ces serveurs
- Écriture de la charge utile (encodée en Base64 pour éviter l'analyse statique) dans le répertoire de travail de l'agent
- Désactivation de Defender

*Here's how they try to kill Defender telemetry [pic.twitter.com/47ZwK62yil](https://pic.twitter.com/47ZwK62yil)*

— Kevin Beaumont (@GossiTheDog) [July 2, 2021](#)

- Création d'une copie de [certutil](#) et utilisation pour déchiffrer la charge utile ; il en résulte un exécutable (Agent.exe) signé avec un certificat valide, connu pour être employé avec REvil
- Lancement de cet exécutable par l'agent, avec les privilèges associés
- Extraction d'une version expirée de Defender (MsMpEng.exe, signée par Microsoft en mars 2014 et déjà utilisée par le passé à des fins malveillantes)
- Chargement, avec cet exécutable, d'une DLL placée dans le même dossier

*We are monitoring a REvil 'supply chain' attack outbreak, which seems to stem from a malicious Kaseya update. REvil binary C:\Windows\mpsvc.dll is side-loaded into a legit Microsoft Defender copy, copied into C:\Windows\MsMpEng.exe to run the encryption from a legit process.*

— Mark Loman @markloman [July 2, 2021](#)

- Chiffrement du disque local, ainsi que des éventuels supports amovibles et volumes réseau
- Exécution d'une commande NetShell pour modifier les paramètres du pare-feu et permettre la découverte du système par d'autres machines sur le réseau local
- Chiffrement de ces machines ; les fichiers chiffrés se placent sur les mêmes secteurs que les originaux, ce qui complique leur récupération

```
# Command & control domains
"dmn": "boisehosting.net;fotoideaymedia.es;dubnew.com;stallbyggen.se;koken-voor-baby.nl;juneauopioidworkgroup.org;vancouver-print.ca;zewa
# Should system information be sent to C2 server
"net": false,
# Services to stop and delete
"svc": [
  "veeam",
  "memtas",
  "sql",
  "backup",
  "vss",
  "sophos",
  "svc$",
  "mepocs"
],
```

## La piste des injections SQL

Pour suivre l'évolution de la situation, il y a le [fil rouge](#) officiel de Kaseya. Aux dernières nouvelles (postées cette nuit), la version SaaS doit redémarrer aujourd'hui, 5 juillet. Pour les instances sur site, il faut s'attendre à un correctif. Lequel supprimera « quelques fonctionnalités anciennes ».

Kaseya fait état d'une quarantaine de victimes au maximum. On retrouve une estimation similaire [sur](#) le *subreddit* des MSP... mais c'est sans compter leurs clients. En les incluant, on en serait plutôt à au moins un millier.

Sur ce même *subreddit* figurent quelques indicateurs de compromis. Entre autres, une IP AWS qui a envoyé des requêtes GET et POST vers les serveurs VSA. Plus précisément pour détecter l'éventuelle présence – et l'accessibilité par le réseau internet – de certains fichiers. Dont un semblant permettre un contournement d'authentification. Et un autre qui paraît abriter des failles d'injection SQL.

## Kaseya : REvil tente la « rançon globale »

Kaseya a publié un [outil](#) destiné principalement à repérer le deuxième fichier. D'autres ressources sont disponibles pour les administrateurs ; par exemple sur [ce dépôt](#) GitHub. On aura aussi noté les [recommandations](#) des autorités américaines (FBI et CISA). Parmi elles, la systématisation du MFA « sur tout compte que vous contrôlez » et la limitation des communications avec les IP distantes. Ainsi que le placement des interfaces d'administration des outils d'accès distant derrière un VPN ou derrière un *firewall* sur un réseau dédié.

C:\> Administrator: Command Prompt - powershell.exe -ExecutionPolicy ByP

```
==== Kaseya VSA Detection Tool ====  
Parsing IIS Logs. May Take A While...  
PASS: File Reference Not Found  
Searching For Suspicious Certificates...  
PASS: Certificate Not Found  
Searching For Suspicious Executables...  
PASS: Executable Not Found  
Generating Results...  
RESULT: System Does Not Indicate Vulnerability  
Press Enter to exit: _
```

Here's another screenshot highlighting multiple runs of the « Kaseya VSA Agent HotFix » as it deploys the encryptor and Windows Defender disable script to unique agents (computers and servers).  
[pic.twitter.com/colmFY0tLL](https://pic.twitter.com/colmFY0tLL)

— Kyle Hanslovan (@KyleHanslovan) [July 3, 2021](#)

Quelques victimes se sont déclarées, [à l'image](#) de Visma Esscom. L'entreprise suédoise gère notamment des systèmes de paiement en magasin. Soit précisément ce qui a contraint le détaillant Coop (environ 20 % du commerce alimentaire dans le pays) à fermer les portes de centaines de boutiques.

Here's the notice on stores. [pic.twitter.com/FmjlgMZRVl](https://pic.twitter.com/FmjlgMZRVl)

— Kevin Beaumont (@GossiTheDog) [July 3, 2021](#)

La rançon demandée varie selon les cibles. L'attaque est en tout cas revendiquée sur le « site vitrine » de REvil. Avec un court message : contre 70 millions de dollars, nous déchiffrerons tout...



Illustration principale © Rawpixel.com – Adobe Stock