# Asus : la mise à jour logicielle infectée par un malware

Jusqu'à un million d'ordinateurs de la marque Asus auraient été infectés par un logiciel malveillant de type porte dérobée (backdoor).

C'est ce qu'affirment des chercheurs de Kaspersky Lab selon lesquels l'attaque aurait été propagée depuis un serveur Asus officiel hébergeant le système de mise à jour logicielle LiveUpdate qui dessert les utilisateurs finaux.

## Operation ShadowHammer

Le malware était signé par un certificat Asus légitime afin de tromper la vigilance des logiciels antivirus et des clients. L'attaque, baptisée "Operation ShadowHammer", se serait produite entre juin et octobre 2018.

Une fois installé, le backdoor relevait l'adresse MAC de la carte réseau qu'il comparait avec une base de données de 600 adresses intégré à son code. Si une correspondance était établie, un second malware était alors installé sur la machine.

On ignore pour le moment le rôle de cette deuxième partie de l'attaque.

## Symantec confirme l'information de Kaspersky

Selon le site Motherboard qui a rapporté l'information, l'éditeur Symantec a confirmé les affirmations de Kaspersky.

Asus en revanche n'a pas encore réagi officiellement.

Ce type d'attaque n'est pas inédit. En 2017, les serveurs de Piriform, l'éditeur du logiciel CCleaner avaient été compromis pour diffuser une porte dérobée. 2,3 millions d'utilisateurs avaient été touchés.