

# [Vault 7 « Dark Matter » : comment la CIA pirate les Mac et iPhone](#)

Début mars, **Wikileaks** levait le voile sur les méthodes utilisées par la **CIA** pour espionner les internautes. Des documents rassemblés sous le nom de **Vault 7**.

Wikileaks dévoile aujourd'hui un nouveau volet de l'affaire Vault 7 : [Dark Matter](#). Un ensemble de documents expliquant comment la CIA peut prendre le contrôle des machines **Apple**. Qu'elles fonctionnent sous OS X ou iOS.

Côté iPhone, **NightSkies** est un malware conçu pour être installé sur des iPhone neufs. Les personnes visées n'ont ainsi aucun moyen de savoir qu'elles sont sous écoute. Wikileaks évoque une version 1.2 de cet outil, datant de 2008. Une version qui serait inopérante sur les iPhones actuels.

## **Des outils qui ne seraient plus fonctionnels. Vraiment ?**

Pour les machines classiques, deux solutions sont présentées. **DarkSeaSkies** peut infecter des MacBook Air. Il se compose de trois outils (DarkMatter, SeaPea et NightSkies) dédiés respectivement au firmware EFI, au kernel et à l'espace utilisateur.

**Triton** est un autre malware, qui se compose du logiciel Dark Mallet, chargé d'infecter les firmwares EFI avec le l'outil DerStarke. Une solution dont la version 1.4 date de 2013. Mais qui aurait encore été utilisée **en 2016**... en version 2.0.

Dernier outil présenté aujourd'hui, **Sonic Screwdriver**, un outil permettant d'infecter un Mac via un adaptateur Thunderbolt vers Ethernet compromis.

Apple indique que tous les **iPhone** proposés à partir de **2009** et tous les **Mac** conçus après **2013** seraient protégés contre les actions de ces outils.

### **À lire aussi :**

[Vault 7 : Wikileaks lève le voile sur les méthodes d'écoute de la CIA](#)

[Vault 7 : Android serait \(en partie\) protégé explique Google](#)

[iOS serait protégé des écoutes de la CIA, rassure Apple](#)

**Crédit photo : © CIA**