

Du choix risqué du logiciel propriétaire et étranger pour sa défense nationale

Le blog de Libération, animé par le spécialiste maison des questions militaires Jean-Dominique Merchet, nous informe aujourd'hui que nos armées ont été attaquées par un virus informatique.



En effet la Marine nationale, ayant son réseau sous Windows, a récemment été infectée par le ver informatique *Conflicker* (qui exploite une faille du serveur de ce système d'exploitation), jusqu'à, semble-t-il, empêcher certains avions Rafales de décoller^[1].

Sachant que Microsoft avait identifié le problème et averti dès le mois d'octobre ses clients de la nécessité d'effectuer des mises à jour pour s'en prémunir, Jean-Dominique Merchet a raison de pointer là l'inquiétante négligence des services informatiques du Ministère.

Par contre il est passé complètement à côté de la question bien plus fondamentale de confier son informatique à un éditeur étranger de logiciels propriétaires. Qui plus est quand il s'agit de Windows dont on connaît les problèmes de sécurité, qui plus est quand on travaille dans le domaine hautement sensible de la Défense nationale.

Heureusement certains commentaires sous son billet ne se sont pas privés de le lui rappeler, commentaires qui se trouvent être comme synthétisés par cette intervention lue sur LinuxFr et que je me suis permis de recopier ci-dessous :

Un ver s'attaque à la Marine française

URL d'origine

Conficker est le nom d'un ver qui infecte les machines sous Microsoft Windows. Il s'attaque au processus SVCHOST.EXE et il permet d'exécuter du code à distance. Un truc sérieux donc mais, hélas, pas inhabituel dans le monde merveilleux de Windows.

Ce qui est plus inhabituel en revanche c'est qu'il semble que ce ver ait réussi à se propager au sein du réseau informatique de la Marine Nationale (Intramar). L'isolation du réseau a été décidée mais elle a été trop tardive et des ordinateurs de la base aérienne de Villacoublay et du 8ème régiment de transmissions ont été infectés par la bestiole.

Sur ce lien on peut même lire que le 15 et le 16 janvier les chasseurs Rafale de la Marine Nationale qui devaient exécuter une mission n'ont pas pu décoller car ils étaient dans l'incapacité de télécharger les données de leur vol !

A priori Microsoft n'est pas coupable de négligence car un correctif pour la faille de SVCHOST.EXE avait été mis à disposition le 23 octobre 2008. Cette infection est donc entièrement la faute des administrateurs du réseau Intramar qui n'ont pas appliqué les correctifs et qui ont donc indirectement provoqué un gros "couac" dans la capacité de défense du pays.

Les questions qui se posent à la suite de cet épisode sont bien entendu les suivantes :

- Comment est-il possible qu'une fonction aussi critique que le réseau informatique de la Marine nationale dépende d'un système d'exploitation propriétaire fourni par une firme étrangère ?
- Comment est-il possible de choisir un système d'exploitation à la réputation sécuritaire plus que douteuse et dont il est impossible de relire le code source pour le vérifier ou l'améliorer ?
- Comment les administrateurs d'un réseau militaire sensible peuvent-ils laisser leurs serveurs non patchés pendant des mois alors que le danger a été signalé et le que le correctif a été mis à disposition ?

Il y a quelque chose de pourri au royaume de la Royale...

Notes

[1] Crédit photo : Army.mil (Creative Commons By)