

# Le virus Conficker touche la Marine française et ses Rafales

## Le ver

**Downadup**, aussi appelé **Conficker**, continue de faire des ravages. Pire, il est en passe de devenir le vecteur de la plus grosse attaque contre les [PC Windows](#) depuis des années. Avec plus de 10 millions de postes impactés selon les éditeurs de sécurité, il faut dire que la propagation de ce malware se poursuit à grande vitesse alors que la **faille qu'il exploite est corrigée depuis octobre...**

[Downadup continue de s'attaquer aux postes](#) en **passant par les ports USB** mais aussi en utilisant divers moyens de propagation. Il devine les mots de passe réseau et infecte les supports externes. Un motif contre lequel il est **nécessaire de désactiver les fonctions Autorun ou Autoplay des clés USB**, histoire de ne pas encourager la propagation du virus.

De même, [Conficker/Downadup](#) exploite une vulnérabilité dans le service Serveur de Windows qui permet l'exécution de code à distance **si un système affecté recevait une requête RPC (Remote Procedure Call)** spécialement conçue.

Cette fois, ce sont les réseaux informatiques de **l'Armée française**, et notamment de la Marine, qui seraient touchés. Une infection qui contribue à rendre inopérants certains chasseurs. A en croire le site *Intelligence Online*, la menace est grave : « *depuis deux semaines, les réseaux informatiques du ministère de la Défense sont infectés par un virus qui a immobilisé certains systèmes d'armes, à l'instar des Rafale de l'Aéronavale* ».

L'infection pourrait provenir du réseau interne de la Marine baptisé **Intramar**. Ce réseau infecté le 12 janvier sert à transmettre la majeure partie des données numériques. Par contre, les services de l'Armée expliquent : « *Le réseau Sicmar (Systèmes d'Information et de Commandement Marine), q **ui est confidentiel défense n'est pas touché*** » .

Toujours selon *Intelligence Online*, des ordinateurs de la base aérienne de Villacoublay (Yvelines) et du 8ème régiment de transmissions ont également été touchés par le ver informatique.

On assiste donc à une internationalisation de cette menace puisque même la **Marine britannique** aurait coupé l'accès de ses ordinateurs à Internet et **interdit momentanément l'usage des clés USB**.

L'infection du réseau de l'Armée française a de quoi inquiéter sur les mesures **mises en œuvre pour la sécurité de leurs terminaux** mais aussi quant à la politique de sécurité en place. Dans tous les cas, ce cas montre que l'Armée n'avait **pas mis à jour ses ordinateurs sous Windows**.

Cette propagation « *pose de sérieuses questions sur la sécurité des réseaux militaires français et leur capacité à faire face à une cyber-attaque d'envergure* », commente *Intelligence Online*.