

Sécurité : les drones américains victimes d'un virus espion

Les virus informatiques s'infiltrent partout. Y compris dans les centres de contrôles sous haute surveillance. Un virus informatique a infecté la salle de commande à distance des drones militaires américains Predator et Reaper, située dans la base aérienne Creech de l'Air Force (Nevada). Ces drones ont une grande importance stratégique sur les théâtres d'opérations militaires ou anti-terroristes américaines. Ils sont exploités en Irak, Afghanistan et, potentiellement, en Libye.

Le virus a été détecté il y a un peu de plus de deux semaines, ont confirmé trois sources différentes au magazine *Wired*. Le malware est de type *keylogger* et enregistre toutes les entrées clavier effectuées par les pilotes des drones. Il se répand sur le réseau de la base, et aurait contaminés des ordinateurs classifiés. « *Nous n'arrêtons pas de le supprimer, mais il continue de revenir* », constate, fataliste, l'une des sources du magazine américain.

Une transmission accidentelle

A l'origine de la contamination, les soupçons se tournent vers les disques durs externes utilisés pour transférer des données entre les ordinateurs de la base aérienne. Les experts en sécurité du département de la Défense pensent à une transmission accidentelle d'un malware commun : « *Nous pensons qu'il est bénin. Mais nous ne pouvons simplement pas en être sûrs* », confirme l'un d'eux à *Wired*. Malgré la contamination, aucune mission des drones n'aurait été annulée. Cet incident vient confirmer qu'aucun système informatique n'est imperméable aux risques de sécurité, y compris ceux des forces armées.

En 2009, l'US Army s'était ainsi rendue compte que le flux vidéo de leurs drones n'était pas chiffré, et pouvait être lu par les insurgés afghans à l'aide d'un simple logiciel à 26 dollars. Et en 2008, des centaines de milliers d'ordinateurs de la défense américaine avaient été contaminés par le virus Agent.btz. Là encore, il fût introduit par des disques durs et clés USB, rappelle l'Espresso.fr. L'usage de périphériques de stockage avait alors été interdit sur les réseaux sécurisés. La base aérienne de Creech était l'une des rares exceptions...