



Des actions militaires américaines utilisées comme arme pour la propagation des malwares

Les chercheurs BitDefender ont identifié une nouvelle vague de spams annonçant une attaque présumée de l'armée américaine sur l'Iran, ayant pour but d'abuser l'utilisateur en le poussant à télécharger et à installer des logiciels malveillants sur son ordinateur personnel.

La page Internet hébergeant le malware – dailydotnews.com – est conçue de manière particulièrement efficace, avec une bannière en haut, une image ressemblant à une vidéo Youtube et trois lignes de textes détaillant l'opération américaine en Iran. Cette approche a ensuite été utilisée de manière plus large, car les spammeurs misent sur un titre accrocheur et un lien vers un malware, de manière à susciter la curiosité de l'utilisateur et à le prendre au piège en l'amenant à télécharger le malware."

"La nouvelle vague de spam repose essentiellement sur la curiosité des utilisateurs suscitée par le conflit entre les Etats-Unis et l'Iran. Ils sont apparemment redirigés vers un faux site Internet d'actualités, avec une description plus approfondie du conflit et accompagnée d'un lecteur vidéo" constate Andra Miloiu, analyste de la cellule Antispam de BitDefender. "Cependant, le présumé film en flash est en fait une image représentant un lecteur vidéo; quand l'utilisateur clique dessus, l'option - Sauvegarder en tant que - s'affiche".

Si l'utilisateur clique sur la "video" ou sur la bannière, il démarre le processus de téléchargement d'un malware binaire, appelé « [iran_occupation.exe](#) ». Le fichier contient le même code malicieux utilisé pour infecter l'utilisateur avec Storm Worm. Les auteurs du malware profitent d'une période idéale, au moment même où les tensions entre le Moyen Orient et les États-Unis s'intensifient.

D'un point de vue social, la vague de spam s'adresse aux citoyens américains de plus en plus inquiets et à la recherche d'actualités sur les menaces de représailles de l'Iran sur Tel Aviv en cas d'attaques américaines sur leurs installations nucléaires.

Actuellement, l'antivirus BitDefender filtre et détecte à la fois le spam et le code malicieux infectant le binaire « [iran_occupation.exe](#) » (Trojan.Peed.PM). Pour vous assurer un Internet sécurisé, BitDefender vous recommande d'installer une solution de protection anti-malware complète.





À propos de BitDefender®

BitDefender est la société créatrice de l'une des gammes de [solutions de sécurité](#) la plus complète et la plus certifiée au niveau international reconnues comme étant parmi les plus rapides et les plus efficaces du marché. Depuis sa création en 2001, BitDefender n'a cessé d'élever le niveau et d'établir de nouveaux standards en matière de protection proactive des menaces. Chaque jour, BitDefender protège des dizaines de millions de particuliers et de professionnels à travers le monde – en leur garantissant une utilisation sereine et sécurisée de l'univers informatique. Les [solutions de sécurité](#) BitDefender sont distribuées dans plus de 100 pays via des partenaires revendeurs et distributeurs hautement qualifiés. Dans les pays francophones, BitDefender est édité en exclusivité par Éditions Profil. Pour plus d'informations, visitez : www.bitdefender.fr

À propos des Editions Profil

Éditions Profil, société indépendante créée en 1989, développe, édite et diffuse des logiciels sur différents secteurs d'activités, professionnel et grand public. L'éditeur a constitué un large catalogue de solutions dans de nombreux domaines, par exemple sur les segments de la bureautique et de la productivité. Éditions Profil s'est plus particulièrement spécialisée ces dernières années dans l'édition et la distribution d'outils de sécurité informatique et la protection des données en général. Éditions Profil édite notamment les solutions de sécurité BitDefender et Parental Filter, ainsi que les solutions Farstone et diffuse les solutions de récupération de données et de gestion de serveurs MS Exchange de Kroll-Ontrack.