http://www.developpez.com/actu/52226/Les-gouvernements-de-23-pays-victimes-des-cyberattaques-inhabituelles-MiniDuke-exploite-une-faille-dans-Adobe-Reader/

Les gouvernements de 23 pays victimes des cyberattaques inhabituelles

MiniDuke exploite une faille dans Adobe Reader

Le 28/02/2013, par Hinault Romaric, Responsable Actualités

Une nouvelle variante de malware, permettant d'espionner des gouvernements et des institutions à travers le monde, vient d'être découverte par le cabinet de sécurité Kaspersky en partenariat avec les chercheurs du Crysys Lab de Budapest.

Le malware, baptisé MiniDuke, aurait exploité une faille de sécurité découverte récemment dans le lecteur PDF Adobe Reader pour compromettre les systèmes de plusieurs organisations.

La faille dans Adobe Reader avait été découverte par FireEye et pouvait être utilisée pour contourner la sécurité du Sandbox (bac à sable) implémenté dans le logiciel et prendre le contrôle d'un poste affecté via un PDF piégé.

Les pirates utilisent comme vecteur d'infection un fichier PDF corrompu traitant de la politique étrangère, d'un séminaire sur les droits de l'Homme ou des plans d'adhésion à l'OTAN qui, après ouverture, permet l'installation de MiniDuke.

Le malware génère par la suite une signature unique pour chaque poste affecté, qui sera utilisée pour chiffrer les échanges avec ses créateurs. MiniDuke aurait la capacité de suivre discrètement des comptes Twitter prédéfinis pour déchiffrer des tweets contenant des marqueurs spécifiques signalant des URL chiffrées comportant les adresses des serveurs de Command and Control qui permettront au malware de rester connecté en cas d'arrêt du premier.

D'une taille de 20 Kb seulement et écrit en assembleur, ce malware d'un type très différent serait, pour le CEO de Kaspersky, écrit par des programmeurs de la vieille école.

« *Il s'agit là d'une cyberattaque très inhabituelle* », souligne Eugene Kaspersky, fondateur et CEO de Kaspersky Lab. « *Cela me rappelle une typologie de programmes malveillants de la fin des années 1990 ou du début des années 2000. C'est à se demander si leurs auteurs ne se seraient pas soudainement réveillés après une période d'hibernation de plus de dix ans, afin de faire leur entrée sur la scène des cybermenaces évoluées. Ces programmeurs d'élite "de la vieille école" ont fait preuve par le passé d'une extrême efficacité dans la création de virus très complexes et allient aujourd'hui ces compétences avec les dernières techniques d'évasion de sandbox, afin de cibler des entités gouvernementales ou des établissements de recherche dans plusieurs pays*. »

Environ 59 ordinateurs d'organisations gouvernementales, d'instituts de recherche et de « Think Tanks » de près de 23 pays ont été affectés ces 10 derniers jours, y compris les dispositifs de l'OTAN.

Il faut noter que la faille dans Adobe Reader avait été patchée la semaine dernière par un correctif d'urgence publié par Adobe.

Source : SECURELIST