Brutal Kangaroo : quand la CIA cible les réseaux les plus sensibles

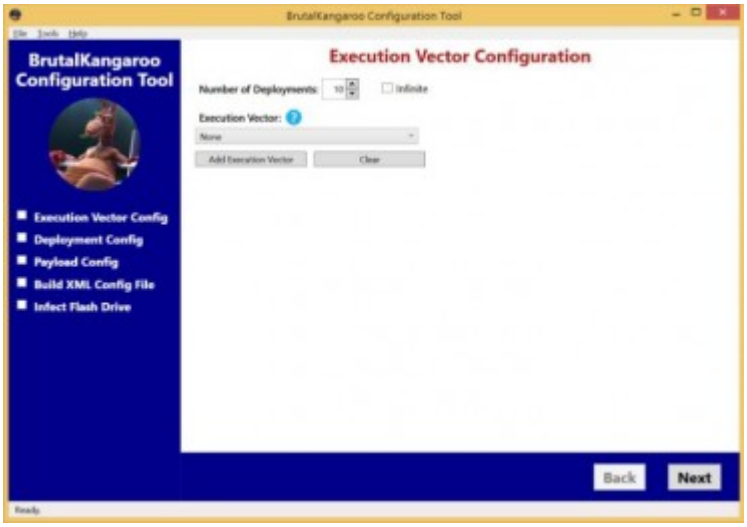
Wikileaks a dévoilé hier la documentation d'une nouvelle série d'utilitaires de hacking provenant, selon le site de Julian Assange, de la CIA. Ce kit, nommé Brutal Kangaroo et renfermant divers logiciels, cible en particulier les réseaux dit 'air-gapped', autrement dit non reliés à Internet. Une technique employée dans des organisations sensibles afin de placer hors de portée des pirates des systèmes manipulant des informations très confidentielles.

Pas de quoi décourager la CIA qui, avec Brutal Kangaroo, déploie un processus d'attaque complexe. Schématiquement, en utilisant d'autres outils faisant partie de son arsenal, l'agence de renseignement commence par infecter au minimum un système accessible par Internet au sein de l'organisation cible, avant de tenter de franchir le 'air-gap' en infectant un maximum de clefs USB que l'agence espère voir connectées au réseau protégé. Dès qu'un support de stockage amovible est connecté au patient zéro, les composants de Brutal Kangaroo vont infecter directement ce support avec un malware différent de celui ayant compromis le poste sur le réseau ouvert. Cette seconde souche est spécialement configurée pour la cible au sein d'un outil appelé Drifting Deadline.

Miser sur l'imprudence des utilisateurs

Si la clef USB est ensuite connectée à un autre poste, ce second malware se déploie, en s'appuyant sur des fichiers Windows LNK (l'extension pour les raccourcis dans l'OS) qui vont lancer la charge utile à chaque fois qu'ils sont vus dans l'explorateur de fichiers. Une mécanique qui a déjà été exploitée par… Stuxnet, le malware qui a infecté les centrifugeuses du programme d'enrichissement d'uranium de l'Iran. Rappelons que la presse américaine a affirmé que cette attaque était l'œuvre de la CIA et d'Israël, ce que les deux intéressés n'ont évidemment jamais confirmé.

Notons que le kit Brutal Kangaroo renferme aussi un outil (Shadow) permettant de coordonner de multiples hôtes compromis au sein d'un réseau protégé et d'envoyer de nouvelles commandes. Bien entendu, tant l'infection du réseau protégé que l'exfiltration de données reposent sur une part de chance, et plus précisément sur l'imprudence de certains utilisateurs (la connexion de clefs USB sur un réseau protégé étant normalement proscrite).



LNK : les patchs de Microsoft

Au cœur de Brutal Kangaroo se trouvent deux exploits (Giraffe et Okabi), des vecteurs d'attaque se basant sur LNK. Notons que, depuis février 2016, Microsoft a publié plusieurs correctifs relatifs à la façon dont ses systèmes gèrent ces fichiers. Dont un en ce mois de juin. Même si Wikileaks a indiqué au début de ses révélations sur les techniques de hacking de la CIA (une campagne appelée Vault 7) qu'il allait travailler avec les éditeurs concernés pour leur permettre de corriger leurs logiciels en amont de ses publications, rien ne permet de confirmer que les récents correctifs de Redmond sont bien liés à Brutal Kangaroo.

A lire aussi :

Vault 7 « Dark Matter » : comment la CIA pirate les Mac et iPhone

Marble Framework : le double jeu perfide des hackers de la CIA

Vault 7 : Wikileaks lève le voile sur les méthodes d'écoute de la CIA