

Extrait du Spyworld Actu

<http://spyworld.spyworld-actu.com/spip.php?article12722>

# La simulation d'une cyberattaque révèle les failles des Etats-Unis

- Informatique - Sécurité Informatique -



Date de mise en ligne : jeudi 18 février 2010

---

Spyworld Actu

---

### **Mardi 16 février, les autorités américaines ont simulé une cyberattaque mettant à mal les systèmes de télécommunications et le réseau électrique du pays.**

Plus de 60 millions de téléphones mobiles hors d'usage, le réseau Internet en panne, la fermeture de Wall Street pendant une semaine, le réseau électrique hors service dans une partie du pays... Les conséquences de l'opération Shockwave laissent songeur.

Ce mardi 16 février, les Etats-Unis ont simulé à Washington une cyberattaque. L'opération s'est déroulée de 10 heures à 22 heures. Dans le scénario imaginé par les services de sécurité américains et le Bipartisan Policy Center, la paralysie d'une partie du pays est causée par une simple application pour smartphones conçue pour les fans d'une équipe scolaire de basket-ball.

Ce spyware a permis le vol de mots de passe et l'interception d'e-mails grâce auxquels les pirates ont pu infecter Internet, entraînant la perturbation de nombreux services et administrations. L'enjeu de cette simulation était de voir quels moyens les autorités peuvent mettre en oeuvre pour enrayer la crise.

#### **Un ancien fonctionnaire dans le rôle du président**

D'anciens hauts fonctionnaires issus des partis républicain et démocrate participaient à ce jeu grandeur nature. La Situation Room, la pièce ultrasécurisée de la Maison Blanche où le président gère les crises, avait été reconstituée pour l'occasion. Une fausse chaîne d'information en continu couvrait même l'événement pour plus de réalisme.

La simulation a révélé le manque de préparation de la plus grande puissance mondiale face à une guerre de ce type. En outre, des problèmes constitutionnels ont été soulevés. Alors que les joueurs voulaient mettre en quarantaine tous les téléphones mobiles du pays pour éviter la propagation du spyware, ils ont réalisé que la Maison Blanche n'avait pas ce pouvoir légalement.

Plus inquiétant : durant toute la simulation, les services secrets et la sécurité intérieure ont été incapables d'identifier l'origine de l'attaque. Dans ce jeu grandeur nature, l'infection est partie d'un serveur hébergé en Russie. Le programme à l'origine de tous ces maux a quant à lui été développé au Soudan.

A l'issue de l'opération, certaines questions sont encore sans réponse. Dans cette simulation, des maisons ont été détruites par l'explosion de stations électriques et de gazoducs. Jusqu'à présent, aucun lien de cause à effet n'a pu être mis en évidence avec l'infection du réseau Internet.

#### **Une simulation publique**

Les Etats-Unis ont l'habitude de procéder à ce genre de simulation. Mais, pour la première fois, la presse était invitée à suivre l'opération, dont le déroulé devrait être disponible prochainement sur CNN.

« Les gens ont du mal à appréhender les menaces », a déclaré au Washington Post John McLaughlin, ancien membre de la CIA qui a joué ici le rôle du directeur de l'intelligence service. « C'est seulement après le 11 Septembre que les gens ont pu s'apercevoir que cela était possible. L'utilité de la simulation sera d'aider les gens à

visualiser [la menace] ».

*Post-scriptum :*

<http://www.01net.com/editorial/5127...>