Mikko Hypponen : « Le hacking des élections américaines ? Oui, ce sont bien les Russes »

Silicon.fr : **Concernant les hacking en marge des élections américaines, êtes-vous convaincu par les arguments de l'administration Obama pointant la responsabilité des Russes ?**

Mikko Hypponen : Oui. Et pour ce faire, je ne m'appuie pas seulement sur les éléments produits par les services de renseignement américains, même s'il faut remarquer que toutes les agences convergent pour pointer la responsabilité des Russes. Je me repose aussi sur les informations que j'ai échangées avec la société en charge de l'enquête au sein du comité démocrate (Crowdstrike, NDLR), que je connais très bien. Sur la base d'investigations passées que nous avons menées, nous avons pu mettre en évidence des détails techniques montrant l'implication des Russes. En réalité, il s'agit de deux opérations différentes, l'une du GRU (les services de renseignement militaires russes, NDLR), l'autre du FSB (l'ex KGB), chacun ignorant probablement la présence de l'autre.

Pensez-vous que ces opérations aient eu un impact réel sur le résultat de l'élection ?

M.H. : Je n'en suis pas sûr. Peut-être que le président Trump aurait été élu de toute façon. Mais je pense que là n'est pas le plus important. Le plus important, c'est que les Russes ont essayé d'influencer l'élection présidentielle américaine, soit le scrutin le plus important d'une des deux superpuissances de la planète. C'est un évènement d'une ampleur considérable.

Comme vous le savez, d'importantes élections auront lieu ces prochains mois en France, mais aussi en Allemagne. Peut-on redouter des interférences de même nature ?

M.H. : Je pense que ce qu'on a vu aux Etats-Unis est la nouvelle norme. Il y aura désormais des interférences avec toutes les élections majeures. Et ce ne sera pas forcément l'œuvre des Russes. Ce peut être n'importe qui voulant influencer le résultat des élections. Ce ne sera même pas obligatoirement une opération menée par un pays étranger. J'étais au Mexique il y a deux semaines et ils s'inquiètent de la sécurité de leur élection prévue dans 18 mois. Pas à cause des Russes, ni même des Etats-Unis, mais des narcotrafiquants, qui ont un intérêt à manipuler l'élection et qui disposent de l'argent et des compétences pour mener ce type d'opérations.

Par ailleurs, je hais le vote électronique. C'est réellement une mauvaise idée, parce qu'avec ce système, si vous enregistrez des résultats étranges à tel ou tel endroit, vous ne pouvez pas recompter les bulletins comme avec le vote traditionnel, sur papier. En général, je suis un grand fan de la digitalisation. Mais encore faut-il que cette numérisation résolve un problème. Je ne vois pas le problème que le vote électronique tente de résoudre. En France, quelques heures après le scrutin, le résultat est déjà disponible. Pourquoi dès lors faudrait-il changer les règles du décompte ?

Mikko Hypponen : « *nouvelle course aux armements* »

L'arme cyber n'est-elle pas à vos yeux l'arme parfaite ? Car, après toute cyberattaque, la désignation d'un responsable (l'attribution en jargon) reste toujours discutée…

M.H. : La raison pour laquelle les gouvernements partout dans le monde s'intéressent aux attaques via Internet, c'est que ces opérations sont à la fois efficaces, financièrement abordables et qu'on peut toujours nier en être l'auteur ! C'est une combinaison vraiment redoutable quand on veut espionner, saboter ou atteindre des objectifs militaires. La réfutation des faits en particulier est précieuse pour les militaires, parce que c'est la seule arme à présenter cette caractéristique. Difficile de bombarder un pays et ensuite de nier toute responsabilité ! Alors que si vous fabriquez Stuxnet, vous pouvez réfuter en être l'auteur aussi longtemps que vous le souhaitez. C'est d'ailleurs ce que les Américains font ! Le seul contre-exemple que nous connaissons à ce jour concerne l'implication des Nord-Coréens dans l'attaque contre Sony Pictures. Mais si les Etats-Unis ont été si prompts à pointer le coupable, s'ils en étaient si sûrs, c'est qu'ils avaient infiltré les systèmes nord-coréens et qu'ils ont pu observer l'attaque contre Sony de l'intérieur.

Tous les pays, France y compris, sont actuellement en train de renforcer leurs capacités offensives dans le cyberespace…

M.H. : Et nous n'en sommes qu'au début de cette nouvelle course aux armements. La dernière course aux armements – celle aux armes nucléaires – a duré 60 ans. Il est fort probable que celle qui s'amorce durera aussi des décennies. Il faudra beaucoup de temps avant que n'aient lieu des discussions sur un désarmement dans le cyberespace. Paradoxalement, une des raisons pour lesquelles ce phénomène se produit en ce moment réside dans les révélations d'Edward Snowden. Quand il a rendu public le niveau des armes cyber dont disposent les Etats-Unis, les autres gouvernements ont pris conscience qu'ils devaient se doter d'un arsenal comparable. C'est un des facteurs qui explique le démarrage de la course aux armements cyber, même si Edward Snowden nous a permis de prendre conscience d'un grand nombre de problèmes et a rendu, globalement, un grand service à la société.

Le gouvernement français vient d'annoncer un événement en avril prochain visant à réfléchir à ce que pourrait être les conditions et les termes d'une 'cyberpaix'. Comment accueillez-vous cette initiative ?

M.H. : Il faut effectivement commencer à réfléchir à ces sujets, parce que ce sont des problèmes complexes qui vont demander du temps. Qu'est-ce que signifie la cyberpaix ? Quelles sont les règles d'engagement dans la cyberguerre ? Depuis la Première guerre mondiale, et les atrocités qui se sont déroulées ici en France, les belligérants s'accordent à proscrire les armes chimiques. Peut-être devrions-nous imaginer des règles aussi pour la cyberguerre. Par exemple, associer une date d'expiration aux armes cyber ; elles devraient cesser de fonctionner après 2 ou 3 ans. C'était d'ailleurs le cas de Stuxnet, inopérant aujourd'hui. Sur le champ de bataille, les soldats sont censés arborer des signes distinctifs, comme un drapeau permettant de les identifier. Pourquoi les malwares utilisés comme armes ne comporteraient-ils pas un bloc d'identification, via une signature avec une clef d'identification publique ?

A lire aussi :

Plateforme de signalement Acyma : le premier pas vers un CERT grand public

Chiffrement : pour l'Anssi, la tentation des backdoors a disparu