STUXNET, OU LE MYTHE DE LA CYBERGUERRE MONDIALE

LE 29 SEPTEMBRE 2010 ***OLIVIER TESQUET***

Largement exposé dans les médias, le virus Stuxnet aurait été conçu par un Etat cherchant à démanteler par la force le programme nucléaire iranien. Ah bon? Pas si sûr.

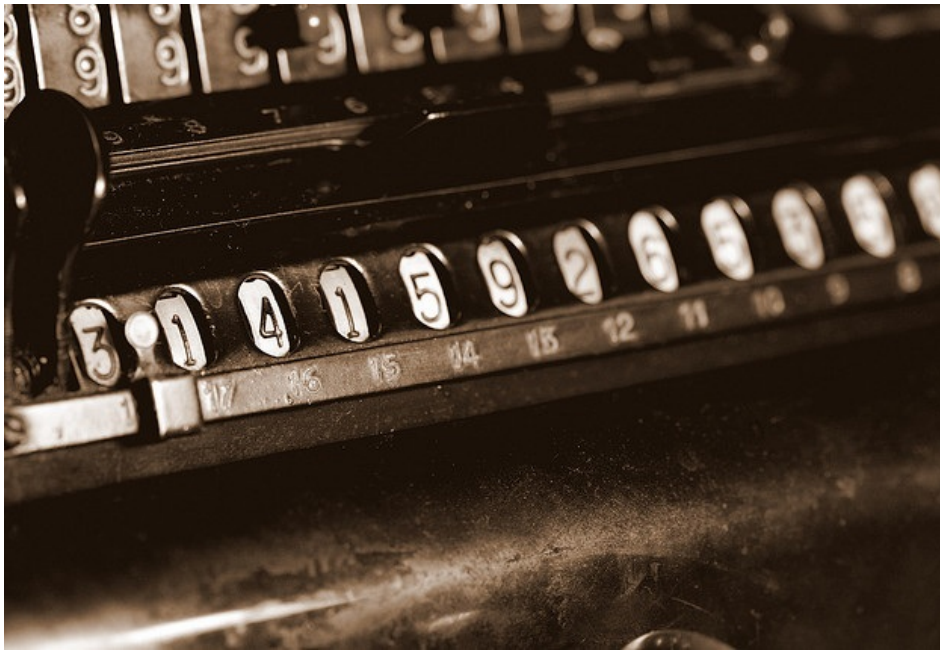
Mise à jour du 30 septembre: *A en croire* ***Jeffrey Carr*** *, spécialiste américain de la cyberguerre et auteur de 'Inside Cyberwarfare', Stuxnet pourrait en réalité avoir été* ***lancé par la Chine*** *contre un satellite indien, dans la course à la Lune qui oppose les deux pays. L'information, postée sur un blog de Forbes, serait le fruit d'un travail de recherche en amont de la* ***conférence Black Hat*** *d'Abu Dhabi, qui se tiendra du 8 au 11 novembre. Voilà une preuve de plus de la faillibilité des hypothèses hâtives au sujet du virus.*

***

"Le piratage du siècle" . C'est en ces termes que Ralph Langner, un expert allemand de la sécurité informatique, a décrit le virus Stuxnet **sur son site web**. Il y a même adjoint la mention, *"Hambourg, 13 septembre 2010"* , ainsi qu'une ligne de code acquise de haute lutte, comme pour économiser une datation au carbone 14 aux archéologues qui découvriraient son avertissement dans quelques dizaines d'années. Depuis plusieurs jours, la presse mondiale s'ébroue dans la bile de ce ver particulièrement complexe. Et pour cause: il saboterait le programme nucléaire iranien en neutralisant ses systèmes de gestion **SCADA** de l'entreprise Siemens, qui administrent notamment la centrale de Bushehr, dans le sud-ouest du pays. Pourtant, à y regarder de plus loin (mieux vaut se prémunir contre les explosions soudaines), il semblerait que l'agitation autour de cette histoire séduisante ne relève que de la fission induite: un dégagement de chaleur qui divise les expertises en de tout petits nucléides légers comme l'air.

Dans le Christian Science Monitor, Langner est formel, *"Stuxnet est un cyber-missile à la précision militaire, déployé plus tôt dans l'année pour trouver et détruire une cible physique d'importance mondiale, une cible encore inconnue"*. S'il se garde bien de nommer tous les acteurs de ce **wargame** grandeur nature, d'autres s'en chargent pour lui. **Sur Slate.fr**, Jacques Benillouche affirme qu'*"Israël a lancé une une attaque électronique contre l'Iran "*, avant d'ajouter que *"les infrastructures du programme nucléaire iranien ont été systématiquement piratées depuis deux mois"*. Et **dans le Guardian**, un porte-parole de Symantec, le géant des antivirus, soutient que *"le groupe qui a conçu Stuxnet aurait été très correctement financé, composé de 5 à 10 personnes travaillant sur la conception du virus pendant 6 mois"*.

Problème: tous les termes de cette équation sont inconnus, jusqu'au plus élémentaire. Comme le fait remarquer **Daniel Ventre**, ingénieur d'études au CNRS et spécialiste français de la cyberguerre*, *"Stuxnet est sur le Net depuis plus d'un an. Il a pu être reprogrammé pour s'attaquer aux systèmes SCADA, mais la semaine prochaine, nous découvrirons peut-être qu'il visait une autre cible. Par ailleurs, il n'y a aucune preuve tangible qu'il s'attaque délibérément à l'Iran"*. Jusqu'à maintenant, selon des chiffres du mois d'août fournis par Microsoft, le virus aurait affecté plus de 45 000 ordinateurs dans le monde, du Pakistan à l'Inde, de l'Indonésie à l'Iran, en passant par le Brésil et les États-Unis. Pour justifier leur propos, les experts affirment que 60% des machines infectées se trouvent au cœur de la République islamique. A cela rien d'étonnant. Depuis les années 70, non sans quelques errements diplomatiques, Siemens (et avant elle, sa filiale Kraftwerk Union) a signé des contrats avec l'Iran, ce qui rend les systèmes d'administration de son parc informatique particulièrement perméables au ver.



La main d'un État? Pas forcément

Aux yeux de bon nombre d'experts, Stuxnet ne peut avoir été conçu que par un État, ou sous le haut patronage d'un gouvernement qui aurait délégué auprès de petites mains. Pourquoi? Parce que son objectif à la précision millimétrée ne viserait pas à voler des données, ni à extorquer ses victimes. Ce serait oublier à quel point la culture du hacking érige la performance au rang de finalité. L'attaque pourrait tout aussi bien avoir été menée par un commando d'**Anonymous** particulièrement politisés. L'hypothèse est fantaisiste? Pas plus qu'une autre. *"Il ne faut pas oublier que les attaques de déni de service par botnet, que nous avons pu observer à de nombreuses reprises ces dernières années, ne cherchent qu'à perturber les fonctionnements d'un système"*, estime Daniel Ventre. C'est aussi l'avis de **Bruce Schneier**, éminent cryptologue américain, qui rappelle que *"les programmes informatiques les plus complexes, l'immense majorité d'entre eux, ont été codés par des organisations non-gouvernementales".*

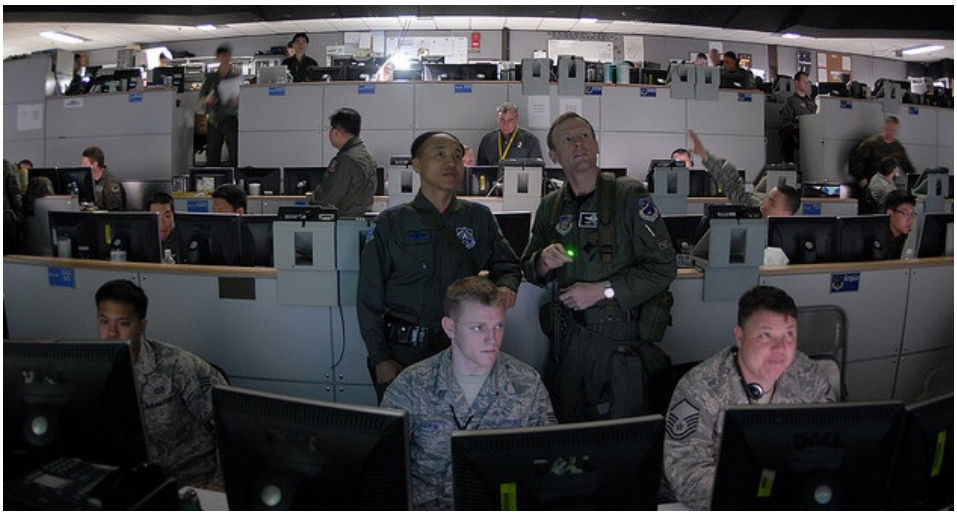
Déjà, on commence à parler de ***"troisième âge du cybercrime"*** , sans qu'on sache vraiment à quelles phases correspondaient les deux premiers. Alors que Stuxnet est à deux doigts d'entrer dans l'Histoire comme *"le premier virus informatique conçu par un État à des fins politiques"* – ce qui permettrait de verbaliser confortablement une cyberguerre "ouverte" – il n'est pas inutile de convoquer quelques précédents. A l'emballement, Daniel Ventre répond par la mise en garde:

> ***"Quand l'aspect futuriste de la guerre informatique se double d'une dimension diplomatique, c'est attirant, bien sûr. Mais ce n'est pas parce qu'une attaque touche aux intérêts d'un État qu'elle a été lancée par un autre État. En 2007, on écrivait les mêmes choses qu'aujourd'hui à propos des incidents estoniens, et à l'été 2008, c'était autour des affrontements entre la Russie et la Géorgie ."***

"Don't believe the hype"

A défaut de circonscrire le virus ou de l'analyser par strates comme le ferait un géologue avec ses sédiments, si on désossait la hype? Quand les ballons-sondes n'offrent aucun résultat, il est peut-être temps de dégonfler la baudruche. Au royaume de la supputation, les observateurs pointent la responsabilité d'un acteur étatique. Bien. Mais dans le même temps, ils reconnaissent qu'il est presque impossible d'identifier le commanditaire de l'attaque, encore plus les dividendes qu'il pourrait récolter. Drôle de syllogisme. Pour Daniel Ventre, *"ce phénomène relève plus de l'inculture que de la paranoïa"* , que le jeu d'accusation

et de démenti permanent avec l'Iran alimente. Sans surprise, le régime des mollahs **s'est empressé d'accuser Washington**, tout en laissant planer le doute sur son degré d'infection.



Evgeny Morozov, le blogueur technologique et ombrageux de **Foreign Policy**, estime de son côté que

> ***chacun voit ce qu'il veut dans Stuxnet. C'est le problème avec les débats autour de la cyberguerre: ils sont si difficiles à cerner qu'ils ouvrent la porte à une infinité d'interprétations. A ce stade, n'importe qui peut invoquer la responsabilité de n'importe quoi, qu'elle relève d'un gouvernement, des aliens ou des Roms***

Reste la question du timing. Alors que se tient à Vienne une Conférence Générale de l'Agence Internationale de l'Energie Atomique (AIEA), quelques informateurs fiables, comme le site **Arms Control Wonk**, relèvent les tensions entre l'Iran, les pays non-alignés, les Etats-Unis et Israël, tout en soulignant la volonté américaine d'un consensus. L'administration Obama souhaite en effet organiser une conférence sur le désarmement nucléaire au Moyen-Orient dans le courant de l'année 2012. Alors, dans ce schéma brouillé, à qui profite le crime? Aux Etats-Unis? A Israël? A l'Iran? Dans l'immédiat, Stuxnet sert surtout les intérêts de Symantec, **comme l'explique en creux Le Monde**. Mais pas seulement. Il est un formidable levier pour tous les experts en cybersécurité de la planète, et notamment ceux qui cherchent à monnayer leurs services auprès du Pentagone.

Avant de fantasmer sur la fin du monde 2.0 ou le grand retour en ligne des **cellules stay-behind** de la Guerre Froide, pourquoi ne pas s'asseoir devant nos moniteurs et attendre quelques mois? Il ne sert à rien de guetter les codes binaires façon Matrix. Devant le rythme accélérateur du web, la cyberguerre impose une contrainte: prendre son temps.

* Auteur de ***Cyberguerre et guerre de l'information. Stratégie, règles, enjeux*** (Hermès-Lavoisier, septembre 2010)

–

Crédits photo: Capture Google Earth de la centrale nucléaire de Bushehr / Flickr CC ***Ian's Shutter Habit***, ***UNC – CFC – USFK***

MOKTARAMA
le 29 septembre 2010 - 13:58 • SIGNALER UN ABUS - PERMALINK

Se servir de Stuxnet pour infirmer l'idée de cyberguerres me semble aller un peu vite : il me semble que Russie et surtout Chine ont développé de réelles capacités offensives en la matière, comme on a pu le voir depuis quelques années avec des pays ou des organisations attaquées ou qui se sont fait voler de gros paquets de données.

Après, pour Stuxnet et l'Iran, les réserves sont effectivement de mise, même si plusieurs faits peuvent expliquer un rapprochement peut-être trop hâtif : on sait qu'Israëliens et américains pratiquent à grande échelle le sabotage en amont des installations nucléaires iraniennes, notamment avec les centrifugeuses (et l'ont déjà fait par le passé avec divers pays) . Hors, de ce que j'en ai lu, Stuxnet permet de perturber le fonctionnement des valves des systêmes industriels contrôlés par des systêmes Siemens (ce qui peut entraîner de graves dysfonctionnements) . Bref, c'est un trop beau scénario pour qu'il ne soit pas repris médiatiquement. Même si, comme votre conclusion le pointe, le tout est tellement nébuleux et techniques que très peu d'intervenants peuvent en saisir une quelconque esquisse de fidélité… les modalités précises des cyber attaques restent donc effectivement sujettes à caution, toutefois l'existence de ces dernières ne me semble pas réfutable. Ceci étant, l'article est nettement plus circonspect que le titre choisi ;-)

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

JEFUNET
le 29 septembre 2010 - 20:22 • SIGNALER UN ABUS - PERMALINK

Existe-t'il une centrale nucléaire connectée à Internet ? J'espère bien que non !

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

OLIVIER TESQUET
le 30 septembre 2010 - 11:03 • SIGNALER UN ABUS - PERMALINK

@Moktarama: je pense qu'il faut se méfier du sophisme "cum hoc ergo propter hoc". Ce n'est ni parce que les Etats-Unis ou Israël ont déjà eu recours à des attaques informatiques pour servir leur stratégie, ni parce que l'Iran constitue un noeud de tension régional, que ces deux éléments doivent absolument être corrélés. Après tout, la cyberguerre existe depuis des années, sous l'appellation "guerre de l'information".

@Jefunet: Bien évidemment, aucune centrale nucléaire n'est connectée au réseau. En revanche, les systèmes d'administration peuvent être corrompus si le virus est importé via une clé USB par exemple.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

MOKTARAMA
le 30 septembre 2010 - 12:13 • SIGNALER UN ABUS - PERMALINK

@Olivier Tesquet :

Je ne crois pas avoir dit le contraire dans mon commentaire, je pointais surtout le fait qu'une telle corrélation était trop belle pour ne pas provoquer sa reprise médiatique (la forme ultra-simplifiée de l'approche iranienne du cas Stuxnet n'aura mis que 10 jours pour arriver aux JT) . Bref, si votre analyse est intéressante, on est à mon sens ici en dehors du rationnel et de l'analyse technique (ou corrélation n'est pas causalité) et dans la sociologie des champs médiatiques (où un tel faisceau d'éléments croustillants justifiera des approximations au doigt mouillé dans le récit de l'info) , et si votre article est intéressant, il passe pour moi quelque peu à côté de sa cible.

Votre remarque sur les batailles de l'info est ainsi tout à fait justifiée et je pensais à voir votre titre que ce serait le coeur de l'article ;-)

Après, pour les cyberguerres proprement dites, on a quand même depuis 2006 pas mal d'exemples d'attaques (Estonie pour la plus visible) et de vol de données (US en 2009 notamment) dirigées ou approuvées en sous-main par des Etats souverains…

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

OLIVIER TESQUET
le 30 septembre 2010 - 13:52 • SIGNALER UN ABUS - PERMALINK

@Moktarama: Daniel Ventre cite justement ces exemples dans l'exergue en fin

d'article ;-)

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

NANOJV
le 30 septembre 2010 - 13:54 • SIGNALER UN ABUS - PERMALINK

Stuxnet met Pékin en état d'alerte. Menaces sans précédent sur la sécurité intérieure et l'industrie.

http://nanojv.wordpress.com/2010/09/30/stuxnet-chine-infrastructures-critiques-30septembre2010/

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

FREAKO
le 30 octobre 2010 - 13:54 • SIGNALER UN ABUS - PERMALINK

Tout à fait d'accord pour l'analyse de ce mythe – votre article est vraiment bien sur le thème et sort un peu de l'analyse classique. Nous avons essayé d'en faire autant sans sombrer dans un délire d'hypothèses ici:

http://freakosophy.over-blog.com/article-stuxnet-le-ver-est-dans-le-fruit-59682643.html

Enjoy

F.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

7 pings

Un média turc soulève l'ambiguité de Stuxnet. Et si le ver n'était qu'un leurre ? « NANOJV le 29 septembre 2010 - 14:41

[...] Aux yeux de bon nombre d'experts, Stuxnet ne peut avoir été conçu que par un État, ou sous le haut patronage d'un gouvernement qui aurait délégué auprès de petites mains. Pourquoi? Parce que son objectif à la précision millimétrée ne viserait pas à voler des données, ni à extorquer ses victimes. Ce serait oublier à quel point la culture du hacking érige la performance au rang de finalité. L'attaque pourrait tout aussi bien avoir été menée par un commando d'Anonymous particulièrement politisés. "Il ne faut pas oublier que les attaques de déni de service par botnet, que nous avons pu observer à de nombreuses reprises ces dernières années, ne cherchent qu'à perturber les fonctionnements d'un système", estime Daniel Ventre. C'est aussi l'avis de Bruce Schneier, éminent cryptologue américain, qui rappelle que "les programmes informatiques les plus complexes, l'immense majorité d'entre eux, ont été codés par des organisations non-gouvernementales". Lire la suite sur owni.fr [...]

Stuxnet, le mythe de la cyberguerre mondiale | Actualité Internationale le 30 septembre 2010 - 14:11

[...] Cet article de notre collaborateur Olivier Tesquet a été publié sur Owni.fr. [...]

Quand la technologie fait peur | Karizmatic le 1 octobre 2010 - 21:03

[...] d'anti-virus en font leurs fonds de commerce et les journaux boost leurs ventes avec Stuxnet en annonçant le début d'une cyber- guerre mondiale de façon quelque peu prématurée. Les dangers réels sont sûrement bien plus cachés que ce qu'on nous [...]

Quand les gouvernements se feront prendre par derrière » Article » OWNI, Digital Journalism le 16 novembre 2010 - 18:10

[...] De telles “portes de derrière” (qui existent sûrement déjà, d’ailleurs) sont une irrésistible invitation aux hackers, aux pirates et aux employés des centres de cyberguerre d’autres gouvernements (comme ceux qui ont conçu le virus Stuxnet). [...]

La guerre de l’information n’est pas la cyberguerre (+ vidéo) « MecanoBlog le 11 décembre 2010 - 18:42

[...] à des fins géopolitiques. Et quand on soupçonne Israël ou les États-Unis d’avoir créé le ver Stuxnet pour perturber le programme nucléaire iranien, il s’agit encore d’une nouvelle arme de [...]

De la cyberguerre à la surveillance » Article » OWNI, Digital Journalism le 3 janvier 2011 - 10:37

[...] Européens veulent légaliser le partage de fichierLa surveillance du Web monte d’un Echelon !Stuxnet, ou le mythe de la cyberguerre mondialeLes va-t-en-cyberguerre débarquent[MAJ] La guerre de l’information n’est pas la [...]

De l’intermédiaire vers le contrôle de l’infrastructure globale | Adam le 6 octobre 2012 - 10:34

[...] les américains et les israéliens afin de compromettre le programme nucléaire iranien (voir l’article d’Olivier Tesquet à ce sujet). Loin d’un soit disant « choc des civilisations » prédit par Huntington, des mythes de [...]