



## Piratage d'Areva: des hackers complotistes ou des espions industriels?

Des pirates ont réussi à s'introduire pendant deux ans dans le système informatique du groupe nucléaire français. Après l'Iran et Stuxnet, la France va-t-elle avoir droit à son méga virus nucléaire?

La nouvelle n'a pas fait tellement de vagues. Le quotidien l'Expansion la révèle pourtant en exclusivité le 29 septembre: [le groupe nucléaire français Areva a été la cible d'une attaque informatique](#) de très grande ampleur probablement perpétrée par des hackers «asiatiques».

Pire encore, les intrusions, découvertes dix jours avant cette annonce, dureraient en réalité depuis plus de deux ans.

Alors que l'info du piratage a eu peu d'écho dans la presse généraliste, elle a été largement relayée dans la presse informatique et les sites spécialisés. Entre indignation et thèses à tendance parano, ceux-ci soulèvent quelques questions qui dérangent. Comment un groupe de l'envergure d'Areva a-t-il pu laisser sa sécurité être violée? Quelle(s) information(s) les pirates pouvaient-ils chercher pour squatter le réseau du groupe nucléaire pendant deux ans?

Stuxnet le retour?

Sur [reflets.info](#), le blogueur Bluetouff, très suivi dans les milieux numériques, écrit:

*«Aucun doute, les pirates ont vraiment dû se goinfrer, et pire, peut-être sont-ils en mesure de reproduire une attaque comparable à celle de Stuxnet sur des infrastructures SCADA (interfaces permettant de piloter à distance des infrastructures sensibles comme les centrales) équipant les centrales nucléaires d'Areva.»*

On le rappelle, Stuxnet, c'est ce formidable virus qui a paralysé le programme nucléaire iranien pendant deux ans. Apparu sur la Toile mondiale en 2010 sans que l'on en connaisse le but, il avait finalement été introduit dans une des centrales via clé USB et avait mis hors service les réacteurs nucléaires.

Alors serait-on dans le cas d'un complot visant le programme nucléaire français? Ce piratage de longue durée a-t-il été pensé pour recueillir les informations nécessaires à la création d'un virus tel que Stuxnet?

Du côté du service presse d'Areva, on n'aime pas beaucoup parler de technique, mais on sait dédramatiser.

*«Areva a bien fait l'objet d'attaques informatiques, mais aucune information critique sensible ou confidentielle n'a pu être visée.»*

Ce que dit une attachée de presse du groupe suffit-il à nous voir rassurés? Pas vraiment. La théorie du retour de Stuxnet a tout de même réussi à insuffler un peu de parano à l'histoire.

Eric Delbecque, chef du département de sécurité économique de l'[INHESI](#) (institut de conseil auprès du Premier ministre), préfère, lui, relativiser la situation:

*«Il ne faut pas tomber dans le catastrophisme, ces attaques sont devenues ordinaires, il y a eu le piratage de Sony, de Bercy, c'est malheureusement devenu banal. L'effet post 11-Septembre a donné l'illusion aux gens que l'ont pouvait créer sa propre bombe dans le secret. Mais une bombe n'est pas livrable en trois clics. Il faut penser aussi que des informations commerciales ont pu aussi intéresser les pirates.»*



La théorie de l'espionnage industriel pour contrer celle d'un complot nucléaire. Une autre piste est lancée, Stuxnet mis sur la touche. Enfin pas pour tout le monde, Bluetouff, sans être formel, se veut plus prudent avec la thèse de l'espionnage industriel.

*«Je ne saurais dire s'il s'agit d'un sabotage de la concurrence, mais cette thèse me paraît peu plausible. Un sabotage est un acte ponctuel. Pour moi, la durée de l'intrusion signifie plutôt qu'une personne ou plusieurs ont cherché à gagner des accès dans le SI d'Areva.»*

### Les méchants Chinois

Il est sûr que voir le système informatique de l'élite du nucléaire français visité aussi librement que le cabinet d'un ministre pendant les journées du patrimoine, ça fait mauvais genre. Surtout quand la visite s'éternise pendant deux ans.

Qui sont donc ces mystérieux squatteurs? Selon certaines sources, il s'agirait des méchants Chinois, adeptes reconnus du hacking. Une thèse à prendre avec des pincettes pour Nicolas Arpagian, directeur scientifique de l'Institut national des hautes études de la sécurité et de la justice, qui souligne que les coupables ne se trouveraient peut-être pas dans l'Empire du Milieu.

*«Sans savoir qui est à l'origine de cette cyberattaque, on peut se douter qu'il se trouve dans un Etat qui se trouve en concurrence avec Areva. Beaucoup de pays souhaitent bénéficier de l'antériorité d'Areva sur le nucléaire. Maintenant, les alliés de la France peuvent aussi s'avérer coupables car ils seront beaucoup moins facilement identifiables et détectables géographiquement que ceux qui viennent d'Iran ou de Chine par exemple.»*

Y aurait-il un loup dans la bergerie d'Areva? Du côté d'Eric Filiol, spécialiste en virologie et sécurité informatique, on penche plus vers la théorie de «l'espionnage commercial» orchestré par des concurrents. Mais pour ce qui est de l'espion chinois, nombreux sont les professionnels de la sécurité à remettre en cause sa culpabilité. Eric Delbecque va même plus loin dans ce sens.

*«Les sources "asiatiques", pour moi, c'est une extrapolation. Vous savez bien que les serveurs marchent par système de rebond. On pense avoir affaire à un serveur basé en Chine, mais en réalité celui-ci nous renvoie ailleurs. Le petit espion chinois est un mythe à la mode.»*

Dans cette affaire, les Asiatiques auraient donc bon dos. Leurs faits d'armes antérieurs en feraient même les coupables idéals. «On a bien sûr pris le prétexte de cas avérés, mais ce n'est pas aussi simple. Il suffit de prendre le contrôle d'un serveur chinois et on croira que c'est la Chine qui est derrière tout ça», observe Eric Filiol.

Si l'on ignore encore leur identité, on sait néanmoins que ces pirates ont fait preuve d'une importante organisation et d'une grande technicité. Il ne s'agirait pas d'un petit hacker à peine pubère, désireux de faire tomber la grande machine Areva, ni même d'une quelconque stratégie de sabotage pensée par l'ONG Greenpeace.

*«Ici, il s'agit d'un véritable espionnage. N'oubliez pas que c'est l'agressé qui a parlé et non l'agresseur. Pour ces pirates informatiques, la discrétion prime. Avant, vous aviez les mouchards, maintenant, vous avez les cyberattaques.»*

Ce piratage a de quoi faire frémir Areva. Il faut dire que rester deux ans dans le système informatique du fleuron du nucléaire français relève d'un grand professionnalisme et peut rendre l'entreprise un brin fébrile. Mais comment ces pirates ont pu jouer les intrus pendant si longtemps sans se faire détecter? Selon Nicolas Arpagian, «ces pirates sont particulièrement structurés pour être restés deux dans le système informatique d'Areva. Ils doivent se déplacer régulièrement en essayant de ne pas déranger l'infrastructure existante. Ils doivent se fondre à l'intérieur».



### Stuxnet ou pas Stuxnet?

L'adresse et la précaution des pirates ne relanceraient-elles pas la théorie du complot nucléaire? Si l'on se souvient du cas Stuxnet, on ne peut pas vraiment dire que la discrétion avait été de mise. Le virus découvert par une agence de sécurité informatique biélorusse était apparu sur le réseau mondial des mois avant de frapper.

Pour Eric Filiol, le cas du piratage d'Areva ne ressemble en rien à l'affaire du «malware» qui a sévi en Iran.

*«A ce jour, pour Areva, personne n'aurait dit qu'il s'agissait un code malveillant. On n'est pas dans le même cas. Il s'agirait d'une attaque véritablement ciblée, d'une collecte organisée mais pas systématique.»*

Même son de cloche chez Nicolas Arpagian.

*«Dans la situation d'Areva, on est dans un vol d'informations, pas dans une prise de contrôle. Stuxnet avait une mission précise: stopper les bobines et arrêter la production. C'est un cas de figure très différent.»*

Reste que chez les professionnels de la sécurité comme chez Areva, qui a pourtant tout de suite réagi en contactant l'Anssi pour mesurer l'impact de l'attaque, on manque encore de recul pour définir les véritables motifs de ce hack. Aussi, comme l'explique le spécialiste de la cyberguerre Daniel Ventre, *«rien ne s'oppose à ce qu'un nouveau Stuxnet, plus élaboré même, se reproduise dans les semaines/mois à venir. Stuxnet a marqué les esprits: il a démontré que des actions contre les systèmes SCADA, les processus industriels, sont possibles. Tous les secteurs industriels sont potentiellement des cibles de telles opérations. Il en est de plus sensible que d'autres, qui font (ou devraient faire) l'objet de programmes de sécurisation spécifiques».*

### Vigilance humaine vs progrès technologique

A un moindre niveau, et sans parler de virus, cette intrusion laisse en effet redouter le pire quant aux systèmes de sécurité informatiques de grands groupes internationaux. L'expert en sécurité Eric Filiol va même jusqu'à parler de *«faiblesse de la victime»*.

*«Ce qui est consternant, c'est qu'encore une fois, le mythe du super pirate n'a rien à voir avec cela, il s'agit plutôt d'une certaine incurie et de lacunes cruelles de sécurité.»*

Selon des sources internes, l'origine de l'intrusion trouverait ses causes dans des mots de passe trop faibles qui auraient été cassés. La preuve que *«même si le système informatique est sécurisé, il peut toujours y avoir une défaillance humaine»*, selon Nicolas Arpagian. Pour Eric Delbecque, *«la formation est nécessaire. On doit comprendre certains gestes élémentaires de prudence. La principale réponse à donner est humaine, d'ordre organisationnelle, et pas technique. La technique n'est qu'une réponse provisoire. Elle progresse en permanence».*

Une vigilance sérieuse couplée à une dose confortable de suspicion: le seul moyen encore pour l'être humain de ne pas se faire mettre à terre par la technique. On ne pourra plus reprocher aux geeks leur paranoïa.

**Laura Guien et Stéphanie Plasse**