



#Lactu CYBERGUERRE L'ETRANGE AFFAIRE

Fin 2010, l'Iran révèle que l'une de ses usines nucléaires a été la cible d'une cyberattaque. Aujourd'hui, on en sait un peu plus sur Stuxnet, le ver informatique responsable de cet incroyable piratage. **OLIVIER LASCAR**

Le 29 novembre 2010, Mahmoud Ahmadinejad, le président iranien, apparaît devant les journalistes. À son air crispé, on devine que l'heure est grave : il confie à la presse médusée que son pays vient de subir une « cyberattaque ». Elle a frappé l'usine nucléaire de Natanz, au centre du pays. Le président explique que « des ennemis de l'Iran » sont parvenus à s'introduire dans les ordinateurs de l'usine afin de saboter des dispositifs-clés de son fonctionnement : les centrifugeuses qui traitent l'uranium. C'est le début de l'affaire Stuxnet, du nom du ver informatique dont on sait, aujourd'hui, qu'il est responsable de ce piratage.

L'œuvre d'un bataillon de programmeurs

Ce n'est pas la première fois qu'une cyberarme est utilisée dans un conflit entre deux pays. Déjà, en 2007, par le truchement d'un virus informatique, les Israéliens avaient réussi à bloquer les radars syriens et avaient pu ainsi bombarder tranquillement des entrepôts d'armements sur le territoire ennemi. Mais ce qui est frappant, cette fois, avec Stuxnet, c'est qu'il ne s'agit pas d'une opération coup-de-poing. Au contraire, le ver informatique a agi lentement et discrètement, ce qui lui a permis de fonctionner longtemps sans être repéré, et donc de retarder de manière significative le programme nucléaire iranien.

Une tactique sophistiquée qui a bluffé les meilleurs spécialistes de sécurité informatique. Ils sont des centaines dans le monde à avoir décortiqué le programme malveillant après sa découverte. Les experts de Microsoft estiment ainsi que sa mise au point a nécessité un investissement d'environ 10000 jours-homme. Autrement dit, si un pirate l'avait conçu tout seul, il y aurait passé 10000 jours ;

Sa mise au point a nécessité environ **10000** jours-homme



deux pirates, 5000 jours, etc. « Ce ver, c'est certain, est l'œuvre d'une équipe de nombreux spécialistes en tous genres, affirme le lieutenant-colonel Éric Filiol, directeur du centre de recherche de l'ESIEA (École supérieure d'informatique, électronique, automatique), dont le labo a également analysé une version de Stuxnet. Il représente des dizaines de milliers de lignes de code, portant de multiples informations qui font appel à toutes sortes de connaissances, notamment en matière d'industrie nucléaire. Cela n'a pas pu être fait par un pirate seul dans son coin. »

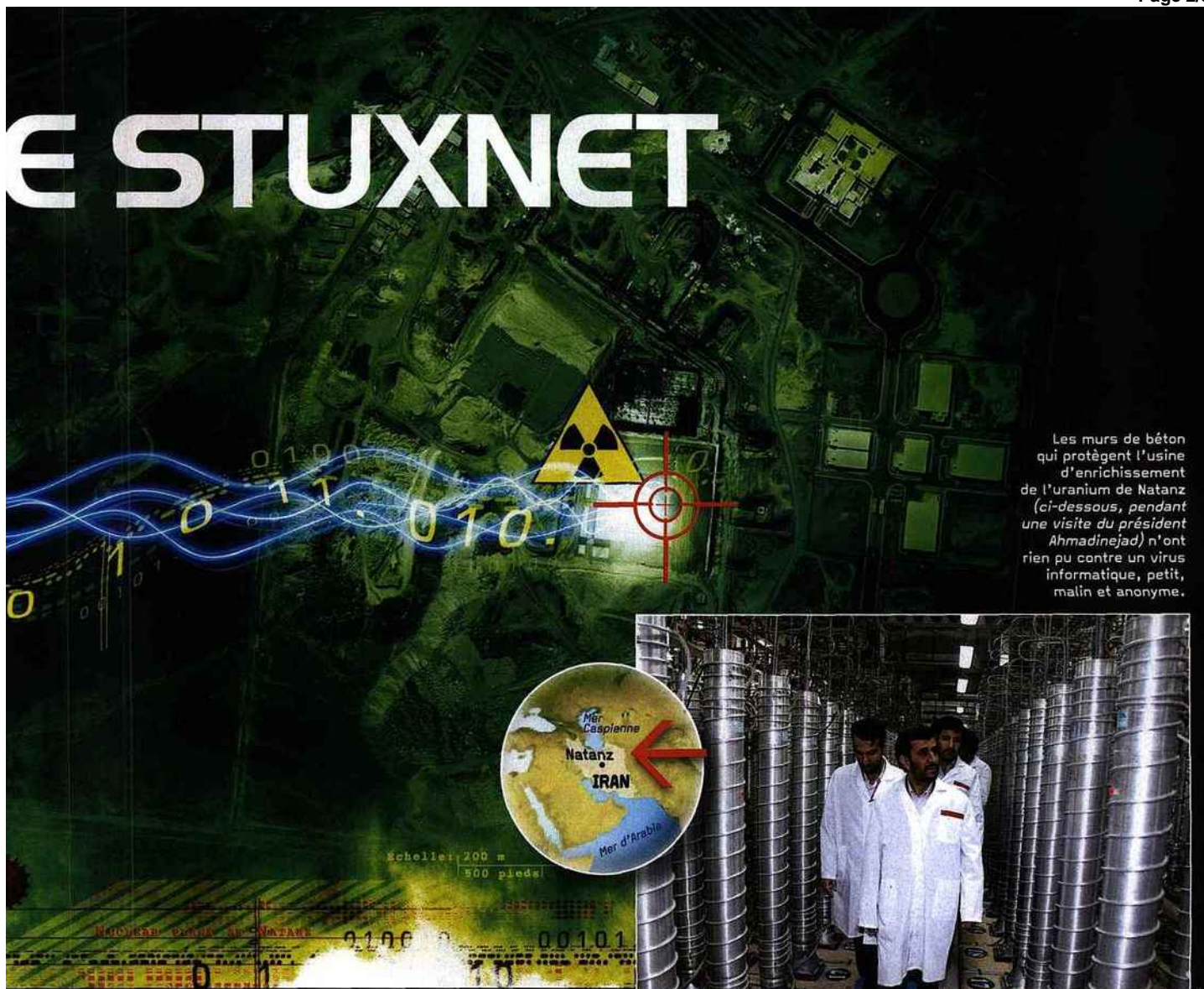
Une attaque lente mais destructive

Ainsi, le premier objectif visé par Stuxnet était de s'infiltrer dans le système d'exploitation le plus courant du monde, Windows 7. Oui, celui-là même qui tourne

sur les PC des ingénieurs iraniens comme sur votre ordi. Pour y parvenir, le ver tire profit de quatre failles dans le code de Windows, dont trois *zero day*, autrement dit des erreurs non identifiées jusqu'alors. Une fois niché dans Windows, le ver devait ensuite cibler un logiciel industriel utilisé à Natanz. « Il s'agit de Scada, explique Daniel Martin, ancien commissaire divisionnaire de la DST (Direction de la surveillance du territoire). Ce programme permet de commander des dispositifs comme on en trouve dans quantité d'usines et pas spécifiquement dans des sites nucléaires : pour ouvrir des vannes, contrôler la vitesse d'une turbine, etc. »

À Natanz, Scada pilote un automate qui commande les centrifugeuses, le matériel-clé du traitement de l'uranium. Stuxnet avait pour mission, non pas de les arrêter, mais de les dérégler. « Le moteur des centrifugeuses doit tourner dans une gamme de fréquences bien précise, entre 807 et 1210 hertz, précise Éric Filiol. Stuxnet dérègle les machines

ESTUXNET



Les murs de béton qui protègent l'usine d'enrichissement de l'uranium de Natanz (ci-dessous, pendant une visite du président Ahmadinejad) n'ont rien pu contre un virus informatique, petit, malin et anonyme.



en leur faisant dépasser brutalement ces limites : elles montent d'un coup de 200 à 1400 hertz, par exemple...» Une tactique qui permet de rendre les centrifugeuses parfaitement inefficaces, sans trop attirer l'attention. Et qui, à force d'accélération/décélération intempestives, casse le mécanisme, comme lorsqu'on fait passer plusieurs fois de suite la boîte de vitesse d'une voiture de la cinquième à la marche arrière.

Il détourne la signature de Microsoft!

Rien de révolutionnaire cependant, dans ce ver, selon Éric Filiol : «Du point de vue du "code opérationnel", j'ai vu beaucoup plus subtil que Stuxnet. Il fonctionne un peu à la manière des virus des années 1980 qui, sous le système d'exploitation DOS, provoquaient purement et simplement une

destruction des disques durs des ordinateurs.» La véritable innovation de ce ver, selon lui, est d'un tout autre ordre. C'est la première fois qu'on voit un programme malveillant équipé de «codes cryptographiques» qui le font passer auprès des systèmes informatiques pour un programme licite. «Sous Windows, on ne peut charger en mémoire que les programmes dont les signatures cryptographiques ont été validées par Microsoft, explique Éric Filiol. Sans ces codes, on ne peut pas installer un programme, il n'est tout simplement pas accepté en mémoire.» Les pirates ont donc volé des certificats de cryptographie qui appartenaient à des logiciels légaux pour les greffer dans le code de Stuxnet. Le ver a ainsi pu montrer patte blanche et faire son nid dans les ordinateurs de Natanz. «C'est une nouveauté inquiétante : si les

codes cryptographiques sont à présent détournés par les pirates, c'est un nouveau talon d'Achille, dans les ordinateurs, et il va falloir rapidement le sécuriser», s'alarme le spécialiste.

Le début d'une cyberguerre globale?

Plus inquiétant encore, c'est le choix de sa cible : un site industriel semblable à ceux qui gèrent nos ressources vitales. «Toutes nos infrastructures, qu'elles soient liées à l'eau, à l'électricité, aux transports, sont automatisées et fonctionnent de la même façon, explique Daniel Martin. Si des virus peuvent les mettre en danger, le fonctionnement de nos sociétés s'en trouve singulièrement fragilisé...» Quelques attaques avant-gardistes donnent la mesure du danger. Ainsi, en Australie, un pirate

#L'actu

CYBERGUERRE

LE SCÉNARIO DE L'ATTAQUE

1 LE VER EST INTRODUIT SUR LE SITE

D'habitude, les vers informatiques se transmettent via Internet, dans les pièces jointes d'un e-mail, par exemple. Or, le réseau informatique de l'usine de Natanz n'est évidemment pas connecté à la Toile. Il a fallu que Stuxnet soit introduit directement sur l'un des ordinateurs connectés au centre de recherche. Autrement dit, il a fallu qu'un pirate glisse une clé USB porteuse de Stuxnet directement sur l'ordi d'un ingénieur iranien. Cela a dû se passer en 2009. Était-ce une agente secrète déguisée en femme de ménage ? Qui sait...



ILLUSTRATIONS NICOLAS RYSER POUR SVJ

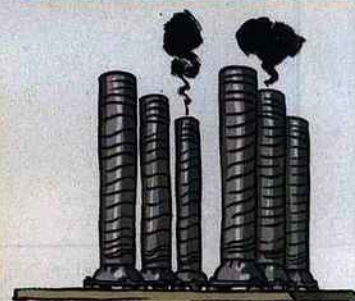
2 STUXNET SE PROPAGE JUSQUE DANS LES AUTOMATES INDUSTRIELS

Les postes informatiques de la centrale sont puissamment verrouillés. Mots de passe, pare-feu, cryptage des données... De nombreux obstacles empêchent l'introduction d'un fichier pirate. Pourtant, grâce aux failles de Windows 7 qu'exploite le ver, Stuxnet se fraye un chemin à travers le réseau interne des PC des ingénieurs. Reste à contaminer les circuits électroniques des processus industriels qui, eux, ne sont pas reliés à ce réseau. C'est sans doute par le truchement d'un notebook infecté que la transmission s'est effectuée. Un ingénieur, venu configurer l'automate industriel S7-300, branche son ordi au poste de contrôle, et le tour est joué !



3 LES CHAÎNES DE CENTRIFUGEUSES SONT ENDOMMAGÉES ET LE PROGRAMME NUCLÉAIRE IRANIEN EST COMPROMIS

L'automate industriel S7-300 assure le bon fonctionnement d'une des étapes indispensables au programme nucléaire : l'enrichissement de l'uranium. Sans cette opération, le minéral radioactif est inutilisable. Il contient en effet à l'état brut deux types d'atomes : plus de 99 % d'uranium 238 ; et moins de 1 % d'uranium 235. Or, c'est ce dernier qui intéresse les ingénieurs, car ses atomes sont instables et ont tendance à se briser en dégageant une forte énergie : ce que l'on appelle la fission nucléaire. L'uranium est donc injecté, sous forme gazeuse, dans des centrifugeuses qui vont séparer les molécules d'uranium 235 de celles d'uranium 238. Les premières, légères, remontent vers le haut de la centrifugeuse, tandis que les secondes, lourdes, s'accumulent en bas. Reproduit en cascade, le processus permet d'accumuler le fameux uranium 235 en concentration suffisante pour qu'il devienne utilisable. Stuxnet va faire dérailler les moteurs des centrifugeuses en les faisant tourner trop vite ou trop lentement, ce qui perturbe le processus d'enrichissement.



QUI A CRÉÉ STUXNET ?

La presse iranienne tient déjà son coupable : Israël. Il est vrai que les Israéliens ne manquent pas de raisons pour mettre un terme au programme nucléaire iranien. Ahmadinejad n'a-t-il pas maintes fois appelé à la destruction de leur pays ? De plus, les analystes ont trouvé dans les entrailles du ver une référence à Esther, la reine juive ayant empêché un génocide... Éric Filiol trouve que c'est un signe vraiment trop voyant : « Il est courant que des pirates laissent des traces dans le code, un mot, une phrase, une signature. Mais là, c'est vraiment trop gros pour être vrai ! » D'ailleurs, de nombreux autres États, dont les pays occidentaux, ne sont-ils pas, autant qu'Israël, de bons suspects ? En effet, le programme nucléaire iranien inquiète. On sait que ce pays, dirigé par des fanatiques religieux, cherche à fabriquer la bombe atomique. L'usine de Natanz pourrait servir à ça, même si les autorités iraniennes le nient. Alors qui ? Il se peut qu'on ne le sache jamais...

s'est récemment immiscé dans le système de gestion des eaux usées, et les a détournées pour polluer des champs et des nappes souterraines. À Łódź, en Pologne, un adolescent qui avait pris le contrôle des tramways a provoqué un accident où un homme est mort, écrasé.

Ne coupez pas !

Avec Stuxnet, on monte un cran plus haut. « On découvre ainsi qu'il est possible d'attaquer des

infrastructures vitales, comme les centres de gestion de l'énergie, les banques, le système médical, etc. », commente Daniel Martin. Et, comme pour confirmer ces craintes, Keith Alexander, le directeur de l'Agence de la sécurité nationale américaine, déclarait récemment qu'il redoutait une attaque du réseau électrique à l'intérieur du pays. On imagine la panique que provoquerait un black-out sur tout le territoire des États-Unis. Un scénario catastrophe qui, avec Stuxnet, ne semble pas irréaliste... ●