DISSECTION D'UNE NOUVELLE CYBERARME

LE 30 NOVEMBRE 2011 ***FÉLIX AIMÉ***

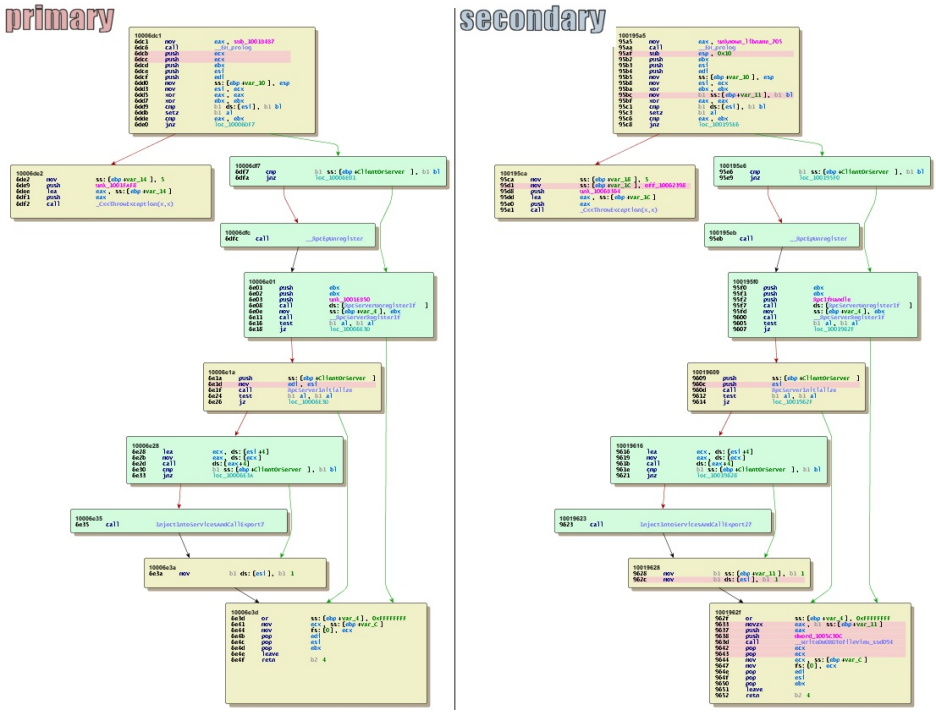
En 2010, la découverte de Stuxnet changeait la donne en matière de cyberarme. Son perfectionnement dépassait les attentes. Aujourd'hui, une nouvelle cyberarme, baptisée Duqu, confirme qu'une étape a bien été franchie. Analyse de Félix Aimé, consultant en sécurité informatique.

Ces deux dernières années, deux malwares[1] se sont illustrés dans le cyberespace par leur complexité, mais aussi par leur utilité stratégique. **Stuxnet** et Duqu visaient tous deux le programme nucléaire iranien. Que peut-on savoir d'eux dans un cyberespace où l'anonymat, le secret défense et l'absence de frontières règnent en maître ? Essai d'analyse.

Plus d'un an après la découverte de Stuxnet, un autre logiciel malveillant fait son apparition dans le cyberespace. Dénommé par les occidentaux *"Duqu"*, en raison des fichiers qu'il laissait sur les systèmes infectés, ce ***Remote Administration Tool*** *(RAT)* a été recensé dans plusieurs pays, principalement l'Iran. Contrairement à Stuxnet, Duqu était cette fois-ci dédié à une campagne d'espionnage, envoyant vers des serveurs distants des informations extraites à partir des ordinateurs infectés. Il n'avait pas de mode de propagation autonome en tant que tel, mais était déployé sur les ordinateurs grâce à une charge utile contenue dans un document Word envoyé par mail aux acteurs ciblés.

Vulnérabilité non connue

Sa méthode de déploiement était triviale, mais son code diffère des autres **trojans** habituellement rencontrés dans ce type de campagne d'espionnage. Tout comme Stuxnet, ce dernier utilisait une vulnérabilité non connue propre à Windows (**CVE-2011-3402**) permettant d'élever ses privilèges pour ensuite se rendre persistant sur le système ciblé ; et donc silencieux auprès des possibles antivirus installés sur la machine. Une autre particularité était frappante chez Duqu : il utilisait des certificats (chose non commune pour ce genre d'attaques) et deux clés de chiffrement identiques au célèbre Stuxnet (0xAE790509 et 0xAE1979DD). Mais les similitudes ne s'arrêtent pas là. Une simple comparaison des deux codes sources à l'aide du logiciel **BinDiff** révèle d'étranges correspondances entre les deux logiciels malveillants :



Duqu a été repéré la première fois en octobre 2011 par un laboratoire hongrois de sécurité informatique dénommé Crysys. Nous ne savons pas d'où vient l'exemplaire qu'ils ont eu entre les mains. L'existence de Duqu serait antérieure à octobre 2011. En effet, en début d'année, l'Iran se disait, **par l'intermédiaire de son agence de presse nationale**, victime d'un malware appelé "Stars". Cela devient intéressant quand on est au courant que Duqu utilise une image **représentant deux galaxies** comme vecteur de communication entre les ordinateurs infectés et les serveurs de contrôle… Duqu serait-il donc le malware Stars ? Cette hypothèse est plus que probable.

Mais alors, depuis combien de temps Duqu est présent dans les réseaux informatiques iraniens ? Personne ne le sait vraiment. La politique en la matière, que ce soit en Iran, en France ou dans d'autres pays, est de disséminer le moins d'informations possibles concernant une attaque. Ainsi, après la découverte tardive du malware Stars, l'Iran a préféré garder le malware bien au chaud dans ses laboratoires de recherche afin d'en étudier la complexité et prévoir une désinfection de son parc informatique gouvernemental. Il pourrait alors faire partie d'une attaque antérieure à Stuxnet ou parallèle à ce dernier, même si sa découverte officielle demeure récente.

Stuxnet, la première cyberarme

Juin 2010, un nouveau ver pour Windows fait son apparition dans les laboratoires de recherche de la société biélorusse VirusBlokAda spécialisée en sécurité informatique. Utilisant quatre failles non connues de Windows et profitant d'une mauvaise configuration dans le système de gestion (PLC) Siemens des centrifugeuses, ce ver, dénommé rapidement Stuxnet, allait devenir aux yeux des experts du monde entier la première cyberarme, car sans doute réalisée uniquement dans le but de détruire ou paralyser tout ou partie du système industriel d'un pays.

Outre les multiples craintes qu'ont fait naître Stuxnet, ce logiciel malveillant avait une cible précise : les centrifugeuses permettant la réalisation d'un uranium hautement enrichi, et donc à visées militaires. Ce n'est qu'à la rentrée 2010 que l'Iran, pris dans la tourmente médiatique, a du avouer son impuissance concernant l'attaque dont il a fait l'objet, ayant selon certains experts, reculé de cinq ans le programme de la bombe iranienne. Stuxnet était bel et bien une arme, composée comme telle, avec un système de propulsion : des vulnérabilités permettant sa diffusion dans les réseaux informatiques, mais également une charge utile, c'est à dire un code d'exploitation permettant de saboter le système de contrôle (PLC) des centrifugeuses d'enrichissement.

Le petit monde des experts en sécurité n'avait jamais rien vu de tel, quatre vulnérabilités non connues affectant uniquement le système Windows présentes dans un seul et même ver informatique. Ce dernier utilisait de plus des certificats permettant de signer son code source devenant à terme un logiciel légitime aux yeux du système ciblé. Cela devenait une évidence pour tous, du fait de son ingéniosité et de ces nombreux codes d'exploitation embarqués, Stuxnet était l'œuvre d'un État, indéniablement en possession de capacités avancées en Lutte Informatique Offensive (LIO).

L'Iran en ligne de mire

Un faible nombre de pays est actuellement en mesure de déployer des projets de LIO et de réaliser des programmes informatiques malveillants d'une grande complexité (les attaques dites "chinoises" (APT) utilisant le plus souvent des versions modifiées de programmes connus du grand public, telles que le célèbre **Poison Ivy**). Ainsi, on retrouve principalement sur le banc des suspects liés à Duqu deux pays ayant fait parler d'eux avec l'affaire Stuxnet, les États-Unis et Israël, ayant tous deux des programmes de LIO développés.

Il est plus que probable que ces attaques soient le fruit des mêmes auteurs, le tout avec une coopération forte entre des services secrets de différents pays, alimentant le renseignement sur les cibles. Toutefois, rien ne fait pencher la balance en faveur d'un pays particulier, **même si certaines pistes, présentes dans le code peuvent laisser présager une implication réelle d'Israël**. Cette piste demeure à prendre avec des pincettes, cependant. En effet, dans le cyberespace il est toujours possible de mener des attaques informatiques lançant de fausses pistes, inscrites dans le code même du logiciel malveillant (**compilation** avec une version chinoise de compilateur, par exemple) ou dans la prétendue origine d'une attaque. A ce jour, connaître les auteurs de ces attaques s'avère impossible car le secret défense est de mise, tant chez l'attaquant que chez la cible. Cependant, des fuites d'informations ou des attaques à venir pourraient nous permettre d'y voir plus clair.

Les deux cyberarmes, Duqu et Stuxnet ont étonné une grande partie des chercheurs dans ce domaine. Au-delà de la simple question de la complexité de la réalisation de ces cyberarmes, l'existence même des deux malwares pose la question de la difficulté d'attribution des attaques dans le cyberespace.

Article initialement publié sur **Intelligence-Strategique.eu** sous le titre : "**Duqu, Stuxnet : deux cyber-armes, un maître d'oeuvre ?**"
Photos et illustrations via les galeries Flickr de **Julia Manzerova [cc-byncsa]** ; **Campra [cc-byncnd]** ; **Dynamosquito [cc-bysa]** ;

1. logiciels malveillants [↩]

WORTI
le 30 novembre 2011 - 15:58 • SIGNALER UN ABUS - PERMALINK

En attendant, le vecteur de la cyberguerre, c'est quand même les failles de windows…

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

7 pings

Lectures by redisdead - Pearltrees le 5 décembre 2011 - 13:20

[...] Dissection d'une nouvelle cyberarme » OWNI, News, Augmented société 9 Culture numérique Open Data société PENSÉES [+] Propriété intellectuelle michel société 7 levaï société 5 occupy vidéosurveillance confirmation open data gouvernement gouvernementale lieux News in French tsunami friday Open Data software Programme Nucleaire Iranien nucléaire Novembre partie HAKIM BEY pirates surveillance espionné libération Internet Illimité mouël devront Open-Data juridique thematic bibliothèques Société démontage alain désobéissance Data nicolas company Les liens de la semaine (5 novembre) médias indignés lieux libre librologie unhosted designs loppsi vente divers pratiques filmer O, grand rêve de l'impossible… spectateur MEDIAS ET WEB SOCIAL veracruz réseaux kinect News jamais destruction israël eEducation ligne ottami mapping Données ouvertes leaked moteurs government DataViz tilemill public When the

web looks at his bellybottom explorateurs internet OPEN DATA opendata Histoire marqué village image DOCS #OWS street decryptages Livres encore HADOPI encore alors wireless Loppsi extrêmement police liberticide France consommation collaborative capitalistique Pearltree du 30 octobre au 10 novembre lieux jenny webzé Numérique solution nouveau Numerique neutralité Applis trois Polémique sur les Grandes Ecoles classes ingénieur un peu de tout économie prices L'enseignement collège classe libre / hacking monnaie home • contact • blog • fb • twitter to experience pearltrees activate javascript. [...]

Les Etats-Unis s'autorisent les cyberattaques » revue du web, Just another weblog le 12 janvier 2012 - 14:19

[...] opérations ont déjà été conduites, dans une relative clandestinité : les virus Stuxnet et Duqu, l'opération Orchard lancée par Israël contre la Syrie en 2007. Les cyberattaques sont [...]

La cybermenace iranienne inquiète Washington » revue du web, Just another weblog le 1 février 2012 - 12:51

[...] suspicions sur la guerre de l'ombre que se livrent les deux Etats (Stuxnet et plus récemment Duqu), aucune information nouvelle n'est venue étayer cette décision des autorités [...]

Israël en guerre (de moins en moins) froide contre l'Iran l ActuHighTech le 28 mars 2012 - 3:37

[...] destinées à enrichir l'uranium auraient été arrêtées. Le site d'information Owni a disséqué le virus et signalait en juin une vidéo (en anglais) publiée par la chaîne [...]

Nouvelle cyberattaque contre l'Iran » revue du web, Just another weblog le 25 avril 2012 - 13:43

[...] spectre de précédentes attaques plane sur ces nouveaux dysfonctionnements (Stuxnet, Duqu, Stars) dont les objectifs étaient tant de retarder le programme nucléaire – pour le [...]

Un malware plus puissant que Stuxnet » revue du web, Just another weblog le 29 mai 2012 - 11:01

[...] des cibles : principalement des pays au Moyen-Orient, avec une préférence pour l'Iran, déjà la cible de précédentes attaques de ce [...]

Diplômés en cyberguerre par l'US Air Force » revue du web, Just another weblog le 12 juillet 2012 - 13:25

[...] moins tabou, d'autant moins après les révélations du New York Times sur la fabrication de Stuxnet et Flame, les virus destinés à saboter le programme nucléaire iranien. Un programme resté [...]