Vous avez Duqu ?  Pas de bol !

L'industrie avait tremblé en 2010 avec Stuxnet. Cette année, c'est le Virus Duqu qui est entré en scène en octobre. Un petit frère en termes de structure, mais pas en termes d'objectif.

Tous aux abris, les virus visant les systèmes industriels reviennent ! Le premier, tout le monde s'en rappelle, s'appelait Stuxnet et avait attaqué les fameuses centrifugeuses iraniennes. Désormais, c'est une bestiole répondant au doux nom de Duqu – prononcez s'il vous plaît Diu-Qiu, ce n'est pas parce nous sommes en danger que cela nous autorise à être incorrects ! – qui menace les industriels du monde entier. Et malgré son nom, il ne fait rire personne.

L'alerte a été donnée le 14 octobre dernier par le Laboratoire de cryptographie et de sécurité systèmes (Crysys) de Budapest. C'est d'ailleurs ce laboratoire qui a baptisé ce ver, en référence aux fichiers qu'il engendre, qui se terminent par un .DQ. Très rapidement, les spécialistes de la lutte contre les virus, toujours attentifs à l'activité cybercriminelle dans le monde, ont réagi. A l'image de Symantec, qui est allé jusqu'à éditer un livre blanc sur ce nouveau virus. Les industriels, eux, se veulent rassurant, à commencer par Siemens, directement visé (du moins les machines alors touchées étaient équipées de certaines de ses solutions) par la dernière attaque qui assure que Duqu ne causera pas de problème sur ses produits et ne contiendrait pas de code pouvant affecter un système de contrôle industriel. L'occasion pour le géant allemand de rappeler que seuls 24 de ses clients ont déclaré avoir été touchés par Stuxnet et que le maliciel a été éliminé dans tous les cas.

UN LIEN AVEC STUXNET

C'est certain, ce Duqu présente une parenté évidente avec Stuxnet. « *Nous avons une équipe qui a travaillé sur Stuxnet pendant des mois. Ce sont les mêmes personnes qui ont étudié Duqu chez nous et elles ont repéré des parties copiées-collées de Stuxnet vers ce nouveau maliciel* », déclare Laurent Heslault, directeur des stratégies de sécurité pour l'Europe de l'Ouest chez Symantec. Effectivement, inutile d'être un grand manitou de l'informatique pour se rendre compte, à la lecture de leurs codes, que leur presque intégralité est identique…

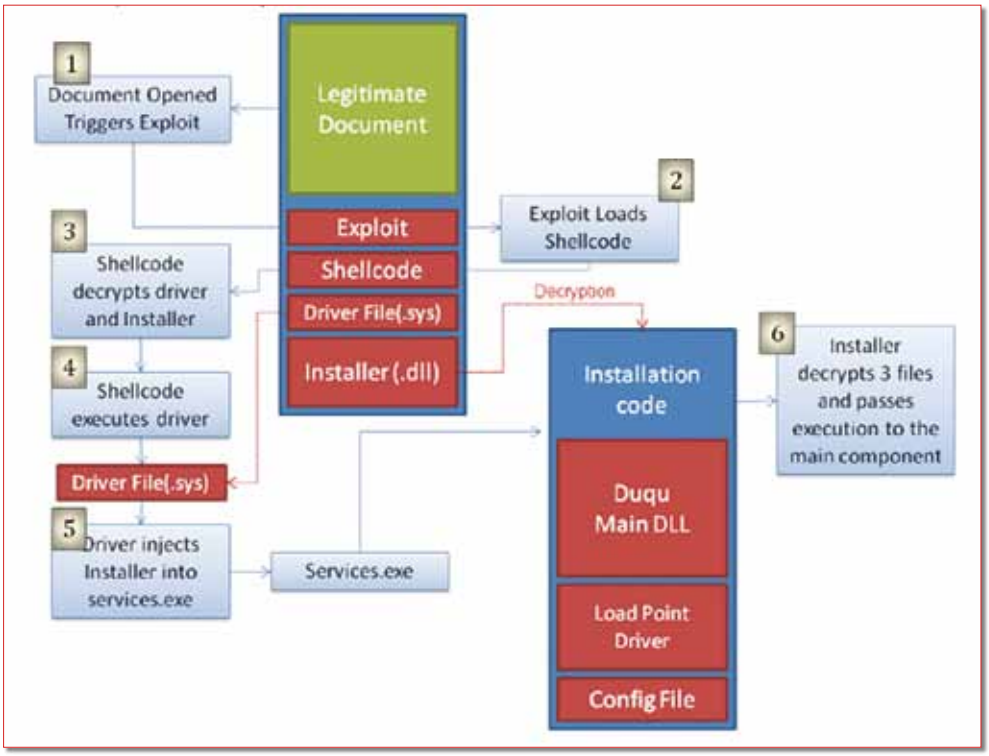
Autre point commun, Stuxnet était un code signé, c'est-à-dire qu'il disposait d'un certificat en bonne et due forme, une sorte de vrai faux passeport logiciel. C'est également le cas de Duqu, dont le certificat est apparemment valide, mais en réalité volé à un éditeur asiatique.

DES DIFFÉRENCES FLAGRANTES

En revanche, le but de ce nouveau virus est bien différent de celui de Stuxnet. Ce dernier cherchait en effet à atteindre des cibles bien précises : des ordinateurs qui pilotaient des automates industriels avec le superviseur Simatic WinCC ou l'atelier logiciel Step7 de Siemens dans des installations nucléaires iraniennes. Le sinistre ver opérait de proche en proche.

D'abord, il prenait le contrôle d'un ordinateur par le biais de plusieurs vulnérabilités de Microsoft - notez que ces failles ont depuis été rebouchées et que tout industriel qui a téléchargé les bons patchs est désormais protégé. Une fois dans la maison, Stuxnet partait à la recherche des logiciels WinCC ou PCS7 sur le réseau pour prendre le contrôle du système industriel sous-jacent, tout simplement à l'aide d'un mot de passe interne à Siemens. En fonction de la configuration détectée, Stuxnet ajoutait des blocs entiers de code dans certains automates industriels du système touché, pour semer la zizanie. Pire, c'est bel et bien du cyber-sabotage que cherchait à faire ce ver. « *Stuxnet faisait varier la vitesse de rotation des centrifugeuses de façon très précise et, surtout, sans que cela ne soit détecté par les logiciels de surpervision* », rappelle Laurent Heslault. Il s'agissait bien de dérégler sciemment les procédés visés en laissant les utilisateurs désarmés face aux dysfonctionnements.

Duqu est également un ver, mais il ne cherche pas à prendre le contrôle de nos usines. En revanche, il vise aussi le monde industriel… par la bande puisque ses cibles privilégiées sont des éditeurs des logiciels destinés à piloter des automates. « *Il s'agit d'un Infostealer. Il n'a pas de relation directe avec des systèmes de contrôle industriel ; son but est au contraire de récupérer des informations relatives à la programmation de PLC* », explique Lurent Heslault. Des informations qui pourraient ensuite servir à attaquer des contrôles industriels et à en prendre le contrôle, comme l'a fait l'autre virus en 2010. C'est d'ailleurs ce qui fait dire à Symantec que Duqu n'est pas un nouveau Stuxnet, mais « *un précurseur d'un prochain Stuxnet* ». Il pourrait aussi s'agir tout simplement d'espionnage industriel…



En six étapes, Duqu prend le contrôle de votre machine.

Selon le spécialiste de la lutte antivirus, une dizaine d'entreprises auraient été touchées, dans huit pays (l'Iran, le Soudan, le Vietnam, l'Inde, la France, les Pays-Bas, la Suisse et l'Ukraine), et toutes développant des logiciels destinés à contrôler des PLC.

UN VERMISSEAU DANGEREUX

Autre différence marquante, Duqu n'a rien à voir avec la machine de guerre qu'était Stuxnet. Celui-ci était en effet une force de la nature. En particulier, il était très complexe et accusait un poids de près de 600 ko, alors que les maliciels classiques ne pèsent généralement que quelques dizaines de ko. Ce poids lourd exploitait en outre pas moins de sept vulnérabilités différentes, dont quatre inconnues – on parle de vulnérabilité zéroday. Ce sont des failles qui ne sont détectées que par leurs effets –. Jamais un virus n'avait utilisé autant de portes à la fois. DuQu, lui, est beaucoup plus simple et ne possède *a priori* pas beaucoup de vecteurs d'infection. Il exploite ainsi une seule vulnérabilité du traitement de texte Microsoft Word, liée à l'utilisation des polices TrueType. Encore une vulnérabilité zéroday… Concrètement, le virus crée un mail avec un fichier Word qui, une fois ouvert, va faire ses emplettes d'informations critiques. Reste que si Duqu est plus simple que son grand frère, il est tout aussi efficace et déterminé. En effet, *« il envoie un mail ciblé et forgé, c'est-à-dire que le destinataire est parfaitement identifié et que les informations apparentes comme l'intitulé du mail n'éveillent pas son attention. Par exemple, vous recevez un mail de votre patron à propos d'une prochaine réunion effectivement programmée »*, explique Laurent Heslault. Ce vermisseau serait même capable d'infecter des ordinateurs qui ne sont pas connectés à Internet, en passant par les dossiers partagés sur le réseau. Enfin, Duqu est un champion du camouflage, qui s'autodétruit au bout de 36 mois et efface à cette occasion toutes les traces de son passage. Un James Bond numérique ! C'est d'ailleurs une des raisons qui peut expliquer le temps qui s'est écoulé avant qu'on le mette à jour.

QUI A FAIT ÇA ? QUELS SONT LES RISQUES ?

Difficile de dire d'où vient ce virus. *« Nous avons identifié le serveur vers lequel remonte les informations. Il est en Belgique mais ce n'est évidemment pas la destination final des informations »*, déclare Laurent Heslault. Reste que le directeur des stratégies de sécurité en est certain, ceux qui ont développé Duqu ont eu Stuxnet en main. *« Il est très difficile de se procurer le code source d'un virus comme celui-là »*, argumente-t-il.

Autre indice, Stuxnet a disparu des écrans radar en avril 2010 et les premières versions bêta de DuQu auraient fait leur apparition il y a près d'un an. De là à conclure à une suite logique… Une chose est sûre, depuis un an, ce nouveau ver a certainement récolté une grande quantité d'informations sensibles en lien avec des équipements pilotant potentiellement des sites de production du monde entier…

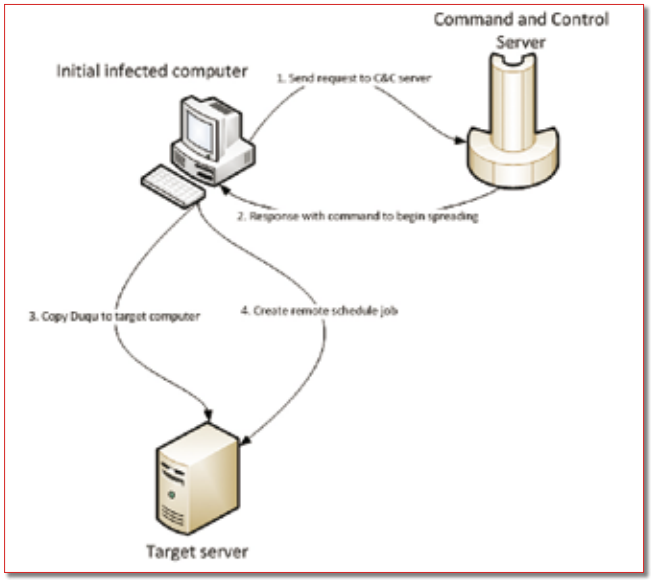
Les types d'informations remontés sont très précis, tels que des enregistrements de frappes, des enregistrements d'écrans toutes les 30 secondes… Les données visées sont d'abord clairement des identifiant et des mots de passe. D'autres informations sont plus difficiles à déterminer. Seule certitude : *« les informations remontent sous forme d'images*, déclare Laurent Heslault. *Cela pourrait indiquer l'usage d'une technique de stéganographie [qui consiste à dissimuler des informations dans une image, de façon à ce que seuls les individus disposant des clés de codage retrouvent les données, [NDLR]. La difficulté, c'est que nous ne savons pas quoi chercher… »* Quant à l'ampleur de la menace, elle est impossible à déterminer pour l'instant. Mais

Actuellement, huit pays sont touchés officiellement par Duqu, dont la France.

imaginez les dégâts que pourrait générer un virus qui perturbe, sans que l'on s'en aperçoive, la préparation de nos aliments, la formulation de nos médicaments, ou affecte nos sources d'énergies et d'utilités (eau, gaz, pétrole…).

TOUS VULNÉRABLES

A priori, rares sont ceux qui sont épargnés par la menace. Dans un avis publié en octobre, Microsoft note que *« toutes les versions supportées de Microsoft Windows sont affectées à l'exception des éditions Core de Windows Server 2008 et Windows Serveur 2008 R2, qui ne sont pas affectées par cette vulnérabilité »*. Et le géant de Redmond de détailler : *« le logiciel malveillant Duqu se propage notamment via l'exploitation d'une vulnérabilité non corrigée dans les polices TrueType. À ce jour, le code malveillant utilise pour vecteur un document Microsoft Word mais toute application reposant sur la fonctionnalité des polices embarquées est potentiellement vulnérable. Pour mettre en œuvre son code d'exploitation, l'attaquant va intégrer à un document une police malveillante dont le chargement par le système va déclencher l'exécution de code arbitraire. Enfin, il est important de prendre en compte les différents vecteurs que la plateforme Windows propose en terme de transport de polices de caractères. La technologie Embedded Open Type (EOT) permet d'intégrer des polices TrueType à des documents HTML. Lors de l'ouverture d'une page Web, Internet Explorer va ouvrir le conteneur EOT et déclencher le chargement par Windows de la police TrueType contenue provoquant alors l'exécution de code arbitraire. Internet Explorer est le seul navigateur à supporter la technologie Embedded Open Type. »*



Une fois installé, Duqu agit en quatre temps : une requête au serveur de destination (en Belgique) entraîne une réponse. Le virus infecte alors sa cible et pompe les infos.

Mauvaise nouvelle, de l'aveu de Microsoft, aucun remède (dans ce domaine, on parle de patch) à la faille exploitée par Duqu n'est prêt. *« Seuls des contournements provisoires sont disponibles »*, indique-t-il. Celui proposé par l'éditeur de Windows consiste tout simplement à bloquer des fonctionnalités de polices embarquées, afin qu'elles ne soient plus transmises au composant Windows vulnérable en charge des polices TrueType. Et la solution est loin d'être idéale. *« Le déploiement du contournement implique que les applications utilisant cette technologie connaîtront des problèmes d'affichage et/ou d'impression, les polices embarquées n'étant plus utilisables »*, annonce Microsoft.

PROTÉGEZ-VOUS !

Voilà pour l'éradication de la contagion, qui concerne *a priori* plutôt les éditeurs de solutions implémentées dans des PLC. Pour le reste, c'est-à-dire la protection contre une éventuelle attaque d'un Stuxnet 2 – et là, tous les industriels sont concernés –, *Jautomatise* vous indiquait déjà les consignes, dictées par l'Agence nationale de la sécurité des systèmes d'information (Anssi) dans son numéro 73 de novembre/décembre 2010 :

- Les utilisateurs doivent utiliser les mécanismes de protection en lecture et écriture disponibles sur les automates ;
- Les configurations des ordinateurs doivent être durcies pour limiter les possibilités d'intrusion ;
- Les services et les logiciels ou les extensions de logiciels inutiles doivent être désactivés, voire désinstallés ;
- Les utilisateurs ne doivent pas posséder des droits d'administration pour l'utilisation quotidienne de leur poste ;
- Les supports amovibles doivent être soumis à une gestion rigoureuse. Ceux étant susceptible d'être branchés sur le réseau de production doivent être inspectés et nettoyés régulièrement (Note CERTA CERTA-2006-INF-006) ;
- Il en est de même pour les ordinateurs, y compris ceux des prestataires chargés de la maintenance ;
- Les flux réseaux autorisés doivent être réduits à l'indispensable. La justification de chaque flux autorisé doit être consignée et la matrice des flux documentée ;
- Les journaux d'évènements et de connexion doivent être analysés, idéalement au fil de l'eau, pour détecter les anomalies et réagir en conséquence ;
- Des audits techniques peuvent compléter ces mesures.

Autre précaution importante : *« mettre les machines à jour »*, martèle Laurent Heslault. Et foce est de constater que généralement, si les solutions existent au travers de Service Packs proposés par les éditeurs de logiciels, rares sont les utilisateurs qui font l'effort de les installer dès leur sortie. Enfin, si vous utilisez un superviseur, sachez qu'il vous est aussi possible de le vérifier, comme un PC classique. *« Nous proposons des scans de vulnérabilité sur des machines de type scada, afin de contrôler qu'ils ne sont pas infectés »*, note Laurent Heslault. Evidemment, ne pensez pas à installer un antivirus sur ces machines. En revanche, il existe peut-être des solutions pour les protéger. *« On pourrait mettre en place l'inverse d'un antivirus classique, c'est-à-dire que plutôt que de détecter tout processus bizarre, on indiquerait clairement tous les processus autorisés à s'exécuter. Cela est notamment utilisé dans les banques »*, déclare le directeur des stratégies de sécurité chez Symantec. Reste que ce type de dispositif s'avèrerait très lourd, car il ne faut surtout rien oublier en mettant en place les verrous, sous peine de brider les machines, ou pire. La meilleure des consignes ? Elle est dictée par le bon sens : RESTEZ VIGILANTS. ■