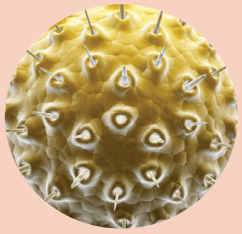


Stuxnet : le virus qui fait tout basculer

Virus mettant en œuvre une série de mécanismes sans précédent pour atteindre des objectifs ciblés, Stuxnet n'a semble-t-il pas produit de catastrophes industrielles. En revanche, ce cheval de Troie marque l'an 1 d'une véritable cyber-criminalité industrielle jusqu'alors assez peu prise au sérieux. Autre constat : l'application stricte de règles connues aurait pu éviter la propagation du virus dans de nombreux cas. Hygiène informatique peu rigoureuse ?

Mis en évidence en juin 2010 par l'éditeur bielorusse de logiciel anti-virus VirusBlokAda, le virus Stuxnet se propagerait depuis environ 18 mois à travers le monde. Ce cheval de Troie serait le fruit, selon les estimations de Symantec, d'un travail équivalent à celui d'une équipe d'une dizaine de personnes pendant 10 mois. Le travail d'un hacker isolé est donc exclus !

Le côté le plus impressionnant de cette attaque sans précédent est peut être d'avoir pris soin d'empiler plusieurs technologies permettant au virus à la fois de passer inaperçu et de pénétrer les systèmes. Pour cela, un niveau élevé de connaissances diverses a été nécessaire.

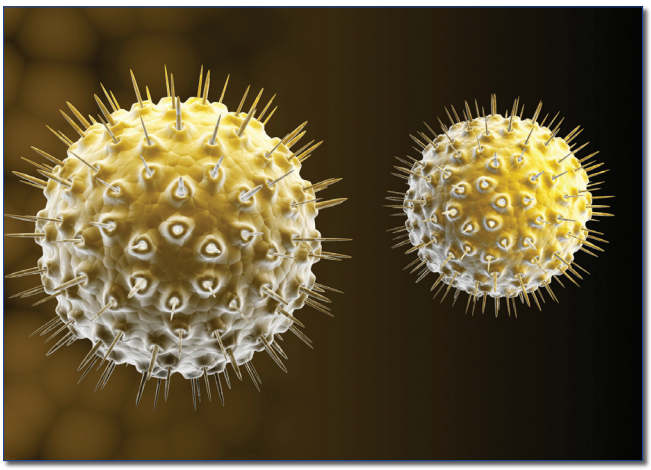
Aujourd'hui, selon Symantec, 100 000 systèmes Windows seraient contaminés, sans pour autant déclencher d'actions spécifiques. Ces ordinateurs ne réunissant pas toutes les conditions recherchées par Stuxnet (voir plus loin). Siemens, pour sa part, affirme qu'à ce jour (octobre 2010), seules 15 cas d'infection par Stuxnet ont été détectés sur ses systèmes et pour l'ensemble du monde (aucun en France), sans qu'aucun installation de production n'ait été touchée.

VOS MACHINES SONT-ELLES INFECTÉES ?

Afin de vérifier si le virus est présent sur vos machines, Siemens préconise d'analyser les systèmes embarqués « Embedded » (par exemple la Microbox), mais aussi les autres ordinateurs tels que les ordinateurs d'infrastructures (serveurs de fichiers, contrôleurs de domaine et autres serveurs), les ordinateurs avec ou sans WinCC installé et les machines virtuelles (tel que VMWARE).

– Les systèmes embarqués « embedded » doivent être scannés à partir d'un second ordinateur (non «embedded ») via des lecteurs validés. Il convient au préalable de mettre à jour le second ordinateur comme cela doit être fait pour les «autres ordinateurs », afin d'éviter une infection mutuelle.

– En ce qui concerne les «autres ordinateurs » dotés d'un OS Microsoft Windows, il s'agit de déterminer s'ils sont infectés par le virus. Pour cela, l'utilitaire antivirus Sysclean ou bien les programmes antivirus validés par Siemens tel que TrendMicro, McAfee ou Symantec, avec des signatures à partir du 25 juillet 2010, feront l'affaire.



Et si une infection est détectée ? *« A ce stade, il faut installer le patch Microsoft et la mise à jour Simatic Security Update. En outre, si une infection est détectée, le support technique de Siemens est à la disposition des clients »*, précise-t-on chez Siemens.

Le patch Microsoft actuel est-il compatible avec les applications Simatic ? *« Oui, la compatibilité du patch actuel Microsoft KB2347290 avec Simatic WinCC et Simatic PCS 7 a été testée avec succès. »*

LES MÉCANISMES DE PROPAGATION DU VIRUS

Deux types de propagation sont empruntés par Stuxnet pour arriver jusqu'à un ordinateur. L'ANSSI (1) détaille les mécanismes :

Propagation par la voie des réseaux

– Stuxnet exploite une vulnérabilité connue du service Windows Server Service, corrigée par l'éditeur Microsoft le 23 octobre 2008 (Avis CERTA CERTA-2008-AVI-523). Cette

(1) L'ANSSI (Agence nationale de la sécurité des systèmes d'information), a été créée par décret du 7 juillet 2009. Cette agence reprend également les missions de l'ancienne direction centrale de la sécurité des systèmes d'information (DCSSI). L'ANSSI est rattachée au Secrétaire général de la défense et de la sécurité nationale.

vulnérabilité qui est donc corrigée depuis deux ans a été exploitée massivement en 2009 par le ver Conficker, mais le correctif est hélas trop peu appliqué, en particulier sur des systèmes de contrôle de processus industriels ou de pilotage d'automates et d'appareils de mesure. Stuxnet en a donc profité !

– Stuxnet exploite également une vulnérabilité concernant la gestion de file d'attente de l'impression (printer spooler). L'existence de cette vulnérabilité avait été signalée en 2009 dans une revue spécialisée, mais était passée inaperçue de l'éditeur et de beaucoup de spécialistes de la sécurité informatique. Résultat, elle n'a été corrigée que lorsque Stuxnet a commencé à se propager. Microsoft a ainsi émis un correctif, le 14 septembre 2010 (Avis CERTA CERTA-2010-AVI-430)

– Stuxnet peut également infecter un ordinateur sur lequel WinCC s'exécute en se connectant par voie réseau à la base de donnée SQL sous-jacente. Il s'y connecte en utilisant le mot de passe d'administration d'usine (qui est fixe !) et envoie une requête SQL malveillante qui a pour effet d'infecter l'ordinateur ciblé. Siemens déconseille de changer le mot d'administration car cela pourrait engendrer des dysfonctionnements.

Propagation par une clé USB

– Présent sur une clé USB, Stuxnet peut infecter un ordinateur sur lequel le mécanisme d'exécution automatique (autorun) n'a pas été désactivé. Cette approche, largement exploitée par d'autres programmes malveillants, peut être contrée, sur Windows 2000, Windows XP et Windows Server 2003 par l'installation d'un correctif publié par Microsoft le 5 février 2009 (Avis CERTA CERTA-2009-AVI-064). L'autorun a par ailleurs été désactivé en 2008 sur Windows Vista et Windows Server 2008 ;

– Stuxnet exploite enfin une vulnérabilité particulièrement critique existant dans le processus de traitement des fichiers de raccourcis (.lnk). Cette vulnérabilité, jusqu'alors non publique, est apparue si critique que Microsoft n'a pas attendu l'échéance mensuelle de son cycle de mises à jour. L'éditeur a publié un correctif dès le 3 août 2010 (Avis CERTA CERTA-2010-AVI-353). Dans la pratique, lorsqu'une clé USB est branchée sur un ordinateur infecté, Stuxnet se copie dessus avec un fichier de raccourci spécialement conçu. Lorsque cette clé est branchée sur un autre ordinateur, ce fichier de raccourci provoque l'infection de cet ordinateur dès lors que, comme souvent, le correctif n'est pas appliqué et que la fonctionnalité Autoplay n'est pas inhibée.

Ces différents moyens de propagations se combinent pour permettre à Stuxnet de se propager et passer de réseau en réseau jusqu'à atteindre un ordinateur qui pilote des automates avec les logiciels WinCC et PCS7.

EXTRAIT DU JOURNAL DE BORD VIRAL TENU À JOUR PAR SIEMENS :

17 septembre 2010 - *« Le logiciel malveillant [Stuxnet] a été isolé et mis en place sur une installation de test pour effectuer des recherches approfondies. Les caractéristiques et le comportement du logiciel malveillant analysés jusqu'ici dans l'environnement logiciel de cette installation de test laissent entendre qu'il ne s'agit pas du développement fortuit d'un hacker mais bien plus de l'œuvre d'une équipe d'experts qui, en plus de compétences IT, possède un savoir-faire spécifique concernant les automates industriels, leur utilisation dans les process industriels ainsi que dans l'ingénierie correspondante.*

Le cheval de Troie devient actif lorsque les logiciels de Siemens WinCC ou PCS7 sont installés. D'autres investigations ont montré que le virus peut théoriquement, en plus de la transmission de données, influencer des processus ou des séquences spécifiques dans des installations ou environnements d'automatismes très spécifiques. Cela signifie que le logiciel malveillant [Stuxnet], dans certaines conditions très précises, est capable d'influencer le traitement du process dans l'automate. Dans les tests et dans la pratique, ce comportement n'a, jusqu'à présent, jamais été vérifié.

Le mode de fonctionnement de Stuxnet suggère que le virus ne s'active que dans des installations ayant une configuration spécifique. Il recherche certaines configurations techniques avec certains modules et certains types de programmes, qui se rencontrent dans des process de production ciblés. Ce modèle peut être localisé, par exemple, par un bloc de données spécifique et deux blocs de code. Cela signifie que Stuxnet est visiblement ciblé sur un process ou une installation particulière et non pas sur une marque précise ou une technologie de process ni sur la majorité des applications industrielles. Cela coïncide également avec le nombre de cas connus par Siemens, pour lesquels le virus a certes été détecté mais n'était pas activé et a pu être supprimé sans avoir à déplorer de dommages jusqu'à aujourd'hui. »

CONTRÔLE À DISTANCE SELON 2 MODES

« Stuxnet présente 2 modes de communication avec ses commanditaires, explique Pierre Caron, enseignant à l'Ecole de Guerre Economique (2). Tout d'abord avec un serveur dédié chez un hébergeur, permettant une prise de commande à distance. Ensuite, par le biais d'un procédé de contrôle de proche en proche. Ainsi, chaque machine infectée peut devenir elle même un serveur de contrôle pour reprendre en main l'ensemble du réseau. Le serveur initial, localisé au Danemark, a quant à lui été neutralisé par les forces de l'ordre. »

PRISE DE CONTRÔLE DANS LE PC : LA STRATÉGIE STUXNET PAS À PAS

– Pour prendre le contrôle d'un ordinateur, Stuxnet exploite plusieurs vulnérabilités (vraisemblablement 4 failles) de l'éditeur Microsoft dont certaines étaient jusqu'alors inconnues (vulnérabilités dites zero day) ;

– Une fois l'ordinateur infecté, Stuxnet recherche la présence

(2) Ecole de commerce créée en 1997, l'EGE entend combler deux lacunes importantes dans la formation initiale et la formation continue : la prise en compte des affrontements informationnels dans la définition de la stratégie des entreprises, des administrations et des collectivités territoriales ; la problématique de l'accroissement des puissances de l'après-guerre froide dans une mondialisation des échanges de plus en plus conflictuelle.

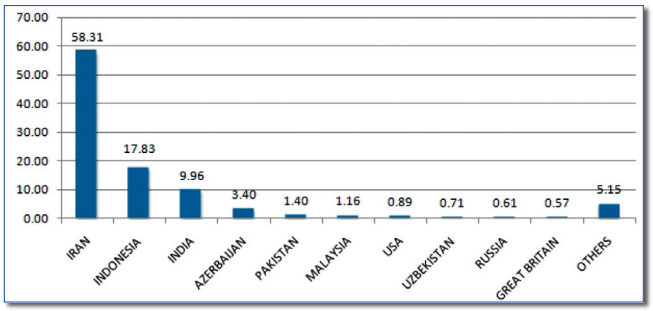
d'un logiciel de supervision et de contrôle d'installations industrielles édité par Siemens, en l'occurrence le superviseur Simatic WinCC ou l'atelier logiciel Step7 ;
– Si la présence d'un tel logiciel est détectée, Stuxnet en exploite une vulnérabilité pour prendre le contrôle du système industriel sous-jacent. Concrètement, il semblerait que le virus utilise un mot de passe interne Siemens pour pénétrer ses logiciels. Ce mot de passe serait d'ailleurs permanent ;
– Si la configuration des composants de ce système répond à certains critères de ciblage, Stuxnet essaye alors de reprogrammer certains automates industriels du système. Le virus crée alors des désordres en changeant des blocs de programmation, c'est-à-dire en les modifiant ou en injectant des blocs spécifiques.

VOL DE CERTIFICATS D'AUTHENTIFICATION

Les développeurs de Stuxnet ont poussé leur démarche jusqu'à utiliser des certificats d'authentification de logiciels afin que le virus passe vraiment inaperçu. Ces morceaux de code aux propriétés cryptographiques non falsifiables n'ont pu être que volés, d'abord chez Realtek Semiconductor, puis chez JMicron Technology, deux entreprises basées à Taïwan... sur le même parc technologique (Hsinchu Science Park) ! Utiliser ainsi de tels certificats, c'est un peu comme dérober un vrai tampon officiel pour réaliser et attester de vrais faux documents.

UNE PROGRESSION QUI AURAIT PU ÊTRE RALENTIE !

Quels obstacles ont manqué dans le cas de Stuxnet ? *« Plusieurs mises à jour, si elles avaient été appliquées, auraient pu ralentir l'épidémie Stuxnet, explique-t-on à l'ANSSI. Par ailleurs, la conservation d'un mot de passe usine par les utilisateurs a permis la modification d'une base de données. Le cloisonnement (flux réseau et supports amovibles) était probablement insuffisant pour endiguer la propagation. De plus, un éditeur a malheureusement manqué une publication de vulnérabilité le concernant. Enfin, nous soulignons l'absence de mécanismes de contrôle d'intégrité et d'authentification forte au niveau des automates eux-mêmes pour protéger l'accès en écriture du programme qui a facilité l'injection de nouveaux blocs par Stuxnet. »*



Dans un rapport sur Stuxnet, Symantec estime qu'au 29 septembre 2010, 100 000 hôtes étaient contaminés dans le monde… dont 60 % en Iran. (Source : Symantec)

Jean-Pierre Hauet, associed partner de KB Intelligence et président de l'ISA-France : *« Le pare-feu, en charge du contrôle des liaisons et des accès à l'ordinateur, nécessite un paramétrage pointu. Il doit contrôler chaque port utilisé et désinhiber les accès non utilisés. Ces opérations sont souvent négligées ! »*

TOUS LES ACTEURS DE LA FILIÈRE SONT CONCERNÉS

Selon l'ANSSI, les éditeurs de logiciels doivent intégrer la nécessité de permettre aux utilisateurs d'appliquer les correctifs de sécurité des systèmes d'exploitation et des briques logicielles qu'ils utilisent, ou fournir très rapidement les correctifs personnalisés correspondants. Cette deuxième solution permet de tester la compatibilité avec les développements propres à l'environnement, tels que les pilotes réseau pour les communications par les bus industriels. Les éditeurs doivent également permettre aux utilisateurs de modifier les mots de passe d'administration des systèmes, en particulier ne pas les fixer dans le programme ou dans des fichiers de configuration mal protégés.

« Pour leur part, les utilisateurs doivent conserver les nouveaux mots de passe de manière sécurisée, c'est-à-dire accessibles uniquement en cas de besoin, et par les seules personnes habilitées, mais disponibles sans retard dans ce cas. La mise sous enveloppe au coffre avec la mention des personnes autorisées à ouvrir l'enveloppe est une procédure minimale. Le mot de passe ne doit pas être simple, facile à deviner (3). »

Par ailleurs, l'ANSSI insiste sur le fait que :
– 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

COMMENT DÉTERMINER SI UN SYSTÈME D'AUTOMATISATION A ÉTÉ INFECTÉ ?

Le logiciel malveillant dispose de ses propres blocs (par exemple DB890, FC1865, 1874) ; il essaie de les charger dans la CPU et de les intégrer dans le programme. Si les blocs cités sont déjà présents, le logiciel malveillant n'infiltre pas le programme utilisateur. Si les blocs cités ne sont pas présents dans le programme d'origine mais que leur présence est désormais détectée, c'est que le virus a infecté le système. Dans ce cas, Siemens recommande de restaurer de manière urgente l'état original de l'installation.

(3) www.securite-informatique.gouv.fr/gp_rubrique_34.

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.

La discrétion des personnels, informaticiens, automaticiens ou simples opérateurs, rendra plus difficile la réalisation d'un attaque informatique ciblée, tout comme la mise en place de mécanismes de contrôle d'accès physique.

QUELLE LEÇON TIRER DE CETTE VAGUE D'ATTAQUES VIRALES ?

« La sécurité de l'information fera l'objet d'une vigilance accrue à l'avenir, précise-t-on chez Siemens. La sécurité informatique ne se résume pas à un produit, ni à une solution technique, il s'agit de mettre en œuvre un processus. Ce processus inclut notamment la formation et la sensibilisation des opérateurs, une structure claire des liaisons de communication au sein d'un réseau mondial, un concept de sécurité de l'information avec des règles de comportement et des mesures techniques et un processus continu de recherche et d'élimination des failles. C'est avant tout aux opérateurs responsables des installations que revient la responsabilité d'assurer la sécurité de l'information et d'ériger un pare-feu. A ce titre, le système d'information d'un site de production doit être isolé et protégé de l'Internet et de l'environnement bureautique, et être protégé et séparé par un pare-feu. »

UNE FEUILLE DE ROUTE POUR CHACUN...

Et l'ANSSI de conclure : *« L'apparition de Stuxnet a confirmé la faisabilité et l'intérêt, pour certains attaquants, de cibler des systèmes critiques de production industrielle.*

Les éditeurs de logiciels SCADA doivent donc respecter dans leurs développements les exigences de sécurité des systèmes d'information, notamment la possibilité de mettre à jour les systèmes sous-jacents. Les opérateurs d'installations industrielles peuvent les y inciter en prévoyant dans les contrats ces possibilités de mises à jour. Les opérateurs doivent également veiller à la mise en place de mesures défensives telles que celles exposées précédemment.

Les coûts induits par ces mesures défensives doivent être mis en regard des pertes en cas d'arrêt de production ou d'accident. Les études sur la sûreté de fonctionnement doivent quant à elles couvrir le maintien de l'intégrité des systèmes automatisés de production face à une attaque informatique, également susceptible de porter sur les systèmes déconnectés de l'Internet. » ■

ISA99 : UNE STRATÉGIE DE PROTECTION ?

Au travers de l'application de l'ISA99, le contrôle des connexions physiques et informatiques conduit à l'organisation d'un système et à la prévention des risques. Jean-Pierre Hauet, associed partner de KB Intelligence et président de l'ISA-France : *« Plus les systèmes sont cloisonnés en restreignant les communications au strict nécessaire, moins il y a de risques de propagation des virus.*

L'ISA99 considère la cyber-sécurité comme une extension de la sécurité fonctionnelle. Sécurité fonctionnelle qui introduit la notion de Safety Integrity Level (de SIL1 à SIL4). Cette norme impose l'analyse du système face aux agressions internes et externes. Mais au moment de sa conception, les cyber-attaques étaient encore du second ordre.

C'est pourquoi, à présent, après définition de « zones » et de « conduits », les standards ISA-99.03.02 et 03 définissent une méthodologie permettant d'assigner un niveau d'assurance sécurité (SALs) à chaque zone d'un système, selon 4 niveaux différents. Dans le cas d'une attaque Stuxnet, les vecteurs SALs auraient dû être de niveau 4 (résistance à attaque sophistiquée et organisée, utilisant des failles 0-day) au moins pour les composantes AC (Access Control), UC (Use Control), DI (Data Integrity). »

PRISE DE CONSCIENCE DANS L'INDUSTRIE

Pierre Caron, enseignant à l'Ecole de Guerre Economique (3), en charge d'un module de formation sur la cyber-criminalité : *« Stuxnet fait preuve d'une prouesse technologique jamais vue jusqu'alors, notamment dans la sphère industrielle, car il s'agit là d'une conjonction d'outils technologiques : exploitations de failles inédites, utilisation de certificats dérobés, atteinte ciblé à un Scada... Cela inquiète particulièrement les experts !*

Jusqu'à présent, les préoccupations des responsables de l'informatique de gestion en matière d'attaques virales ont été différentes des responsables informatiques côté production. Ces derniers n'ont jamais été véritablement inquiétés à ce sujet. Stuxnet prouve aujourd'hui le contraire.

Cette attaque montre aussi que la diversité des operating systems peut être un sérieux atout pour lutter contre la cyber-criminalité ! »

Pierre Caron, enseignant à l'Ecole de Guerre Economique (3), en charge d'un module de formation sur la cyber-criminalité.