ISA France Section

ISA Flash

Setting the Standard for Automation™

ISA FLASH N°40 – Novembre 2010 – Numéro spécial

Bulletin d'information d'ISA-France

Ce numéro spécial d'ISA-Flash est essentiellement consacré à l'affaire de l'attaque des systèmes de contrôle-commande par le malware Stuxnet. De nombreuses spéculations entourent l'origine et les objectifs de cette attaque tout à fait inhabituelle par l'ampleur et la sophistication des moyens qu'elle a mobilisés. Jean-Pierre Hauet, Associate Partner de KB Intelligence, Président d'ISA-France, fait le point, avec le concours de Jean-Pierre Dalzon, spécialiste cyber-sécurité d'ISA-France, sur les techniques utilisées dans cette attaque et tente une première analyse de la prévention et de la protection que peut apporter, en pareille circonstance, le respect du standard ISA-99 en cours de finalisation au sein de l'ISA.

STUXNET : le rappel de quelques faits

A la fin juin 2010, la nouvelle s'est répandue qu'un virus particulièrement sophistiqué, dénommé Win32 Stuxnet, ou plus simplement Stuxnet, s'attaquait aux systèmes d'automatismes et plus particulièrement à ceux équipés d'automates programmables en provenance de la société Siemens.

La première annonce officielle fut celle d'une société biélorusse, VirusBlokAda (www.anti-virus.by/en), spécialisée dans la commercialisation de produits antivirus, faisant état de la diffusion d'un virus infectant les operating systems Windows à partir de clés USB, mais d'une façon inusuelle, sans nécessiter le recours à un dispositif d'autorun et se cachant derrière deux « rootkits »[1] sophistiqués bénéficiant de certificats d'information en apparence valides.

Le 19 juillet, la société Siemens diffusait sur son site de service et de support une première « Product Information » faisant état de l'existence de cette menace et annonçant la mise en place de moyens d'investigation appropriés.

Depuis lors, les informations se sont succédé. La société Siemens a émis régulièrement des bulletins d'information, le dernier en date du 12 novembre 2010, faisant état du recensement de 21 clients dont le ou les systèmes de contrôle ont fait l'objet d'une infection par Stuxnet, aucune conséquence dommageable n'ayant cependant été à ce jour été rapportée.

La société Symantec a émis un rapport d'analyse très complet le 30 septembre 2010, dossier régulièrement mis à jour depuis et accessible sur :
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf .

Eric Byres, spécialiste canadien réputé, publiait le 14 octobre, sous l'entête de Tofino Security, un « white paper » s'appuyant largement sur les conclusions tirées du reengineering fait par la société Symantec.

Le présent ISA-Flash, a pour objectif de donner à nos lecteurs une information objective sur le phénomène Stuxnet, sur les risques encourus et sur la prévention et la protection qu'aurait pu apporter le standard ISA-99 en cours de développement, si les recommandations qu'il comporte avaient été suivies aussi bien par les fournisseurs que par les utilisateurs de systèmes de contrôle.

Qu'est-ce que W32 Stuxnet ?

Stuxnet est un malware complexe qui entre dans la catégorie des « computer worms », capable de s'installer dans la plupart des systèmes Windows 32 bits (Win2000, WinXP, Win2003, Vista, Win Server 2008, Win 7, Win Server 2008 R2), d'y activer ses ressources et en particulier de communiquer avec d'autres machines infectées, notamment pour opérer des mises à jour, mais aussi avec des serveurs situés à l'extérieur pour transférer des informations sur les systèmes dans lesquels il s'est installé.

Plus spécifiquement, Stuxnet est capable de détecter par les réseaux locaux, la présence de consoles de programmation du type Step 7 utilisées dans les systèmes de contrôle-commande Siemens, ainsi que les logiciels de supervision WinCC opérant sous Windows.

Une fois installé dans une console Step7, Stuxnet peut entrer en relations avec certains types d'automates de la gamme Siemens qu'il aura préalablement détectés et y altérer à la fois des modules de communication et de programmation. La cible ultime de Stuxnet apparait ainsi comme étant certains systèmes d'automatisme, sans que l'on sache exactement à quelle fin, les hypothèses de sabotage ou de piratage d'informations étant l'une et l'autre plausibles.

Stuxnet est une construction complexe, dotée de ressources sophistiquées qui a vraisemblablement demandé une centaine de mois de développement de la part d'informaticiens de très haut niveau, sans compter le temps mis à obtenir des informations privilégiées tant sur Windows que sur les produits Siemens.

[1] Rootkit : outil de dissimulation d'un logiciel, souvent à des fins malveillantes

ISA-Flash est une publication périodique d'ISA-France, association loi de 1901. Directeur de la publication : Jean-Pierre HAUET Pour tout renseignement : info@isa-france.org – Tel : 01 41 29 05 09

Parmi les caractéristiques remarquables de Stuxnet, outre la richesse de ses ressources et de ses fonctionnalités, figure le fait qu'il utilise quatre failles 0-day de Windows (c'est-à-dire non préalablement identifiées), un rootkit Windows de dissimulation, le premier rootkit jamais utilisé sur un PLC et des mécanismes sophistiqués de contournement des antivirus préexistants.

Il est généralement admis que Stuxnet a été lancé début 2009 et a fait l'objet de plusieurs perfectionnements avant que son existence ne soit révélée au grand jour en juillet 2010.

Les mécanismes de primo-infection

Il est généralement admis, sans que la certitude en soit établie, que la primo-infection par Stuxnet de systèmes non connectés au monde extérieur se fait par la voie de clés USB contaminées. Le malware y est caché et rendu invisible par le rootkit répertorié Mrxnet.sys détecté par VirusBlokAda (Figure 1).

Ce driver est doté d'une signature numérique dérobée à la société Realtek Semiconductor Corp, localisée à Taiwan et révoquée par Verisign le 16 juillet 2010 (Figure 2).

Ultérieurement, le fournisseur d'antivirus Eset a détecté un autre driver doté également d'un certificat dérobé, cette fois à JMicron Technology Corp également basée à Taïwan, certificat révoqué le 22 juillet 2010.

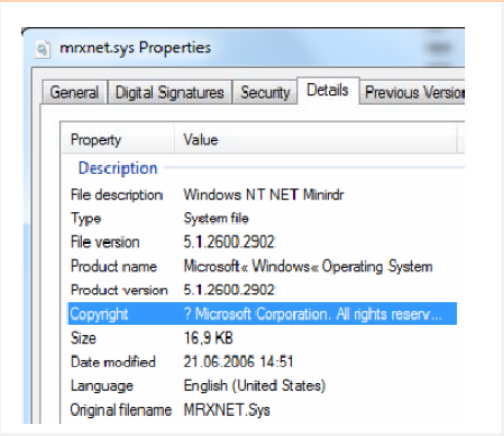

Figure 1 – Source : VirusBlokAda

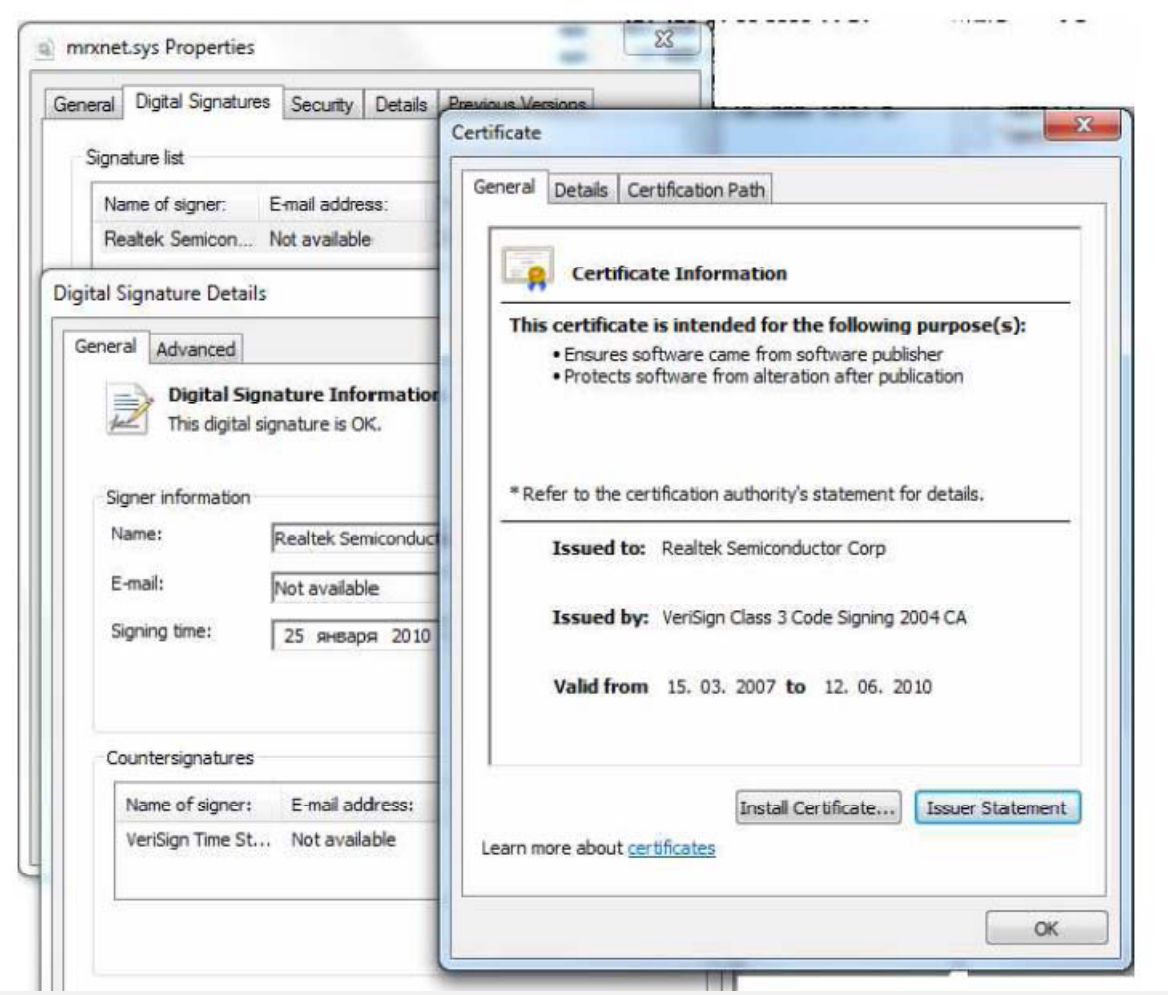

Figure 2 : Source : VirusBlokAda

ISA-Flash est une publication périodique d'ISA-France, association loi de 1901. Directeur de la publication : Jean-Pierre HAUET Pour tout renseignement : info@isa-france.org – Tel : 01 41 29 05 09

Pour pénétrer le système Windows, Stuxnet utilise une faille 0-day, touchant à la gestion des raccourcis informatiques (fichiers .lnk). Cette faille semble avoir été connue dès novembre 2008. Microsoft y a remédié par le bulletin de sécurité MS10-046 du 2 août 2010. Initialement, l'activation du malware nécessitait la présence d'un dispositif autorun sur la clé USB. La faille lnk permet de lancer le processus de transfert des fichiers Stuxnet vers l'ordinateur hôte dès que la clé USB est insérée.

Une fois dans la place, Stuxnet repère son entourage et décide, selon certains critères, de séjourner ou de disparaitre. En particulier, il ne s'installe que si la configuration hôte est antérieure au 24 juin 2012 ce qui est évidemment le cas pour l'instant. Stuxnet s'empare alors des privilèges de gestion les plus élevées en exploitant, en fonction du système d'exploitation rencontré, l'une ou l'autre de deux autres failles 0-day de Windows qui lui permettent d'escalader l'échelle des privilèges. Parmi celles-ci, l'une (intéressant Windows XP et Windows 2000) a fait l'objet du bulletin de sécurité de Microsoft répertorié MS10-073 en date du 12 octobre 2010. L'autre reste à traiter.

S'étant ainsi emparé des droits d'administration les plus élevés, le malware transfère le rootkit qui le masque, collecte des informations sur l'ordinateur hôte, active les fonctionnalités qui lui permettront de communiquer en local avec d'autres machines et en externe, via http, avec des serveurs distants, via Internet. En particulier des pointeurs vers des serveurs répertoriés sous les url www.mypremierfutbol.com et www.todaysfutbol.com ont été repérés. Ceci tend à accréditer l'hypothèse selon laquelle l'objectif de Stuxnet n'est pas seulement de perturber le fonctionnement des machines infectées mais aussi de rapatrier vers une destination inconnue des informations sur ces machines. Toutefois aucun trafic de ce type, dans un sens comme dans l'autre, n'a été à ce jour repéré ou rapporté.

La propagation de Stuxnet

Contrairement à une idée largement répandue, les clés USB ne constituent pas le seul moyen de propagation de Stuxnet. A ce jour, trois grands modes de programmation ont été repérés :

- **Les réseaux locaux**, en utilisant cinq possibilités :
  - En utilisant le mécanisme RPC (Remote Procedure call) avec des machines déjà infectées, ce qui permet d'échanger les versions les plus récentes de Stuxnet,
  - En se propageant vers les ressources partagées sur le réseau (network shares), en invoquant tous les numéros de comptes que Stuxnet peut trouver sur l'ordinateur hôte,
  - En pénétrant les machines Windows supportant le logiciel de supervision WinCC de Siemens grâce à la connaissance d'un mot de passe codé « en dur » dans le logiciel et permettant l'accès à la base de données de WinCC. Une fois dans la place, Stuxnet s'installe mais aussi modifie un écran de WinCC en ajoutant du code chaque fois que la vue est appelée.
  - En utilisant une faille 0-day, sur le service spouleur d'impression de Windows. Quoique signalée dès avril 2009, cette faille n'a été patchée que le 14 septembre 2010 sous la référence du bulletin MS10-061.
  - En utilisant une vulnérabilité sur le Windows Server service déjà utilisée par le virus W32.Downadup (Conficker), en contournant, en tant que de besoin, les dispositifs anti-virus rencontrés. Cette faille avait été patchée par le bulletin MS08-67 du 23 octobre 2008.
- **Les clés USB,** qui sont contaminées chaque fois qu'elles sont insérées dans le système et qu'elles utilisent par la suite la vulnérabilité sur les raccourcis .lnk, patchée MS10-046. A noter qu'une clé USB qui aura à son tour contaminé d'autres machines se trouve libérée de Stuxnet après trois contaminations, ce qui entrave les investigations éventuelles.
- **Enfin les projets développés sous STEP 7** se trouvent contaminés si leurs fichiers portent l'une des extensions .tmp, .s7p ou .mcp. Pour chacune de ces extensions, la contamination n'a lieu que si des conditions assez restrictives sont réunies, ce qui laisse à penser que Stuxnet a été conçu pour viser un ensemble de cibles très particulières.

La diversité des modes de propagation fait qu'un très grand nombre de machine Windows se trouvent aujourd'hui contaminées. Dans la première version de son analyse, Symantec estimait que 100 000 machines se trouvaient infectées dont plus de 60% en Iran (Figure 3).

Depuis cette date, les remontées d'information en provenance d'Iran se sont arrêtées et aucune donnée plus récente n'est disponible. Ceci, ainsi qu'autres détails plus subtils, tend à accréditer l'hypothèse d'une attaque ciblée en direction de certaines installations de ce pays.
Ce qui est clair, c'est que la contamination des machines opérant sous Windows n'est pas l'objectif recherché. Ces machines, très nombreuses, ne semblent pas, à ce jour, présenter de troubles pathologiques. Ce sont en quelque sorte des porteurs sains, victimes collatérales d'une infection ciblée, mais qui ont cependant la redoutable faculté de contaminer certaines catégories d'automates.

ISA-Flash est une publication périodique d'ISA-France, association loi de 1901. Directeur de la publication : Jean-Pierre HAUET Pour tout renseignement : info@isa-france.org – Tel : 01 41 29 05 09

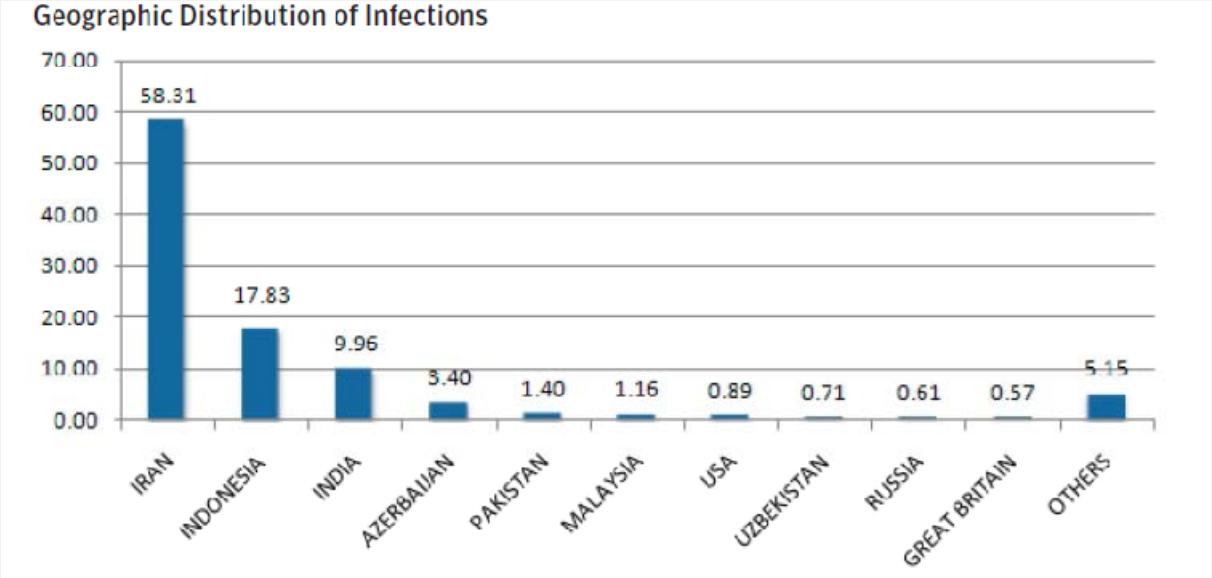

Figure 3 : Répartition des infections Stuxnet dans le monde à la fin septembre 2010 – Source : Symantec

La contamination des automates Siemens

Stuxnet, implanté dans la console Siemens Step 7, a la possibilité d'altérer le fichier répertorié s7otbxdx.dll qui permet la communication avec les automates. La version saine du fichier est conservée et renommée et c'est elle qui sera présentée au cas ou une demande de lecture serait faite sur ce fichier s7otbxdx.dll. La version maligne de la ressource permet quant à elle de corrompre certaines instructions d'import ou d'export entre la console et l'automate, notamment en utilisant au moins l'un de trois mécanismes, fonction de l'automate identifié. Il faut ici souligner que seuls certains types d'automates des types 6ES7-315-2 ou 6ES7-417 sont susceptibles d'être affectés, selon Symantec. Ceci vient renforcer la thèse d'une attaque bien ciblée.

La corruption générée à l'intérieur de l'automate par Stuxnet porte sur un bloc du système de communication Modbus et sur deux blocs de programme : OB1 et OB35. Un rootkit hébergé par la version maligne du s7otbxdx.dll interdit de voir les modifications opérées.

Les effets de ces altérations et l'impact de la corruption éventuelles des informations transitant avec certaines entrées/sorties sont évidemment étroitement dépendant du procédé contrôlé par l'automate. Dans la dernière version de son analyse, Symantec démontre que les mécanismes de corruption mis en place peuvent conduire, dans le cas où les automates pilotent une série de variateurs de vitesse, à un fonctionnement apparemment anarchique du système, dans lequel la vitesse de rotation des moteurs se trouve accélérée puis revient à son régime normal pendant environ 27 jours, puis se trouve ralentie avant de revenir à son régime normal, etc. Un élément de code ajouté dans le bloc OB35 semble destiné à faire remonter l'information selon laquelle l'objectif visé aurait été atteint.

Mesures de prophylaxie et de désinfection

Siemens aussi bien que les grands éditeurs d'antivirus proposent des outils ou des méthodes permettant d'identifier la présence de Stuxnet et, s'il y a lieu, de l'éradiquer. La difficulté réside dans la complexité tout à fait hors du commun du malware et de ses modes de propagation. En particulier, si sa présence est détectée sur une machine Windows, il faut se souvenir qu'il peut continuer à résider dans les automates et dans les fichiers de projet créés à parti de la console. On ne peut pas donc dire aujourd'hui que la situation soit totalement sous contrôle.

Inversement, le ciblage quasi-certain de l'attaque incite à garder la tête froide. Les infections constatées sur de très nombreuses machines Windows et chez une bonne vingtaine de clients Siemens n'ont pas eu à ce jour de conséquences dommageables connues. En parallèle on ne sait pas quel a pu être l'effet de l'attaque sur les machines auxquelles elle était destinée. Selon les autorités iraniennes, Stuxnet a effectivement touché l'Iran, comme les rapports d'exploitation le laissaient entendre. Néanmoins, Téhéran a démenti les dommages industriels causés par Stuxnet et affirmé que la centrale nucléaire de Bushehr avait été épargnée. Toutefois, des ordinateurs personnels d'employés de la centrale auraient été infectés. Certains évoquent un ralentissement de la production d'uranium enrichi par les centrifugeuses. Nous sommes là dans le domaine de la communication de crise et le lecteur pourra se faire son opinion au travers des nombreuses coupures de presse publiées.

ISA-Flash est une publication périodique d'ISA-France, association loi de 1901. Directeur de la publication : Jean-Pierre HAUET Pour tout renseignement : info@isa-france.org – Tel : 01 41 29 05 09

Stuxnet et ISA-99

L'épisode Stuxnet amène évidemment à s'interroger sur l'efficacité de la protection qu'aurait pu apporter le respect des recommandations du standard ISA-99 en cours de finalisation, tant par les vendeurs de systèmes et d'équipements que par les utilisateurs.

ISA-France participe très activement à l'élaboration de l'ensemble normatif ISA-99 dont la nécessité était apparue aux USA après les attaques du 9 septembre. Le raisonnement était le suivant : si des terroristes étaient arrivés à se former au pilotage d'avions sophistiqués, il leur était a priori possible de s'initier au fonctionnement des systèmes contrôlant des infrastructures stratégiques ; alimentation en eau, centrales et réseaux électriques, moyens de transports, installations réputées sensibles en chimie, pharmacie, agro alimentaire. Il fallait donc s'y préparer et le comité ISA 99 a entrepris, en liaison avec la CEI, l'élaboration d'un ensemble normatif qui est aujourd'hui bien avancé et qui se présente comme résumé sur la figure 4.

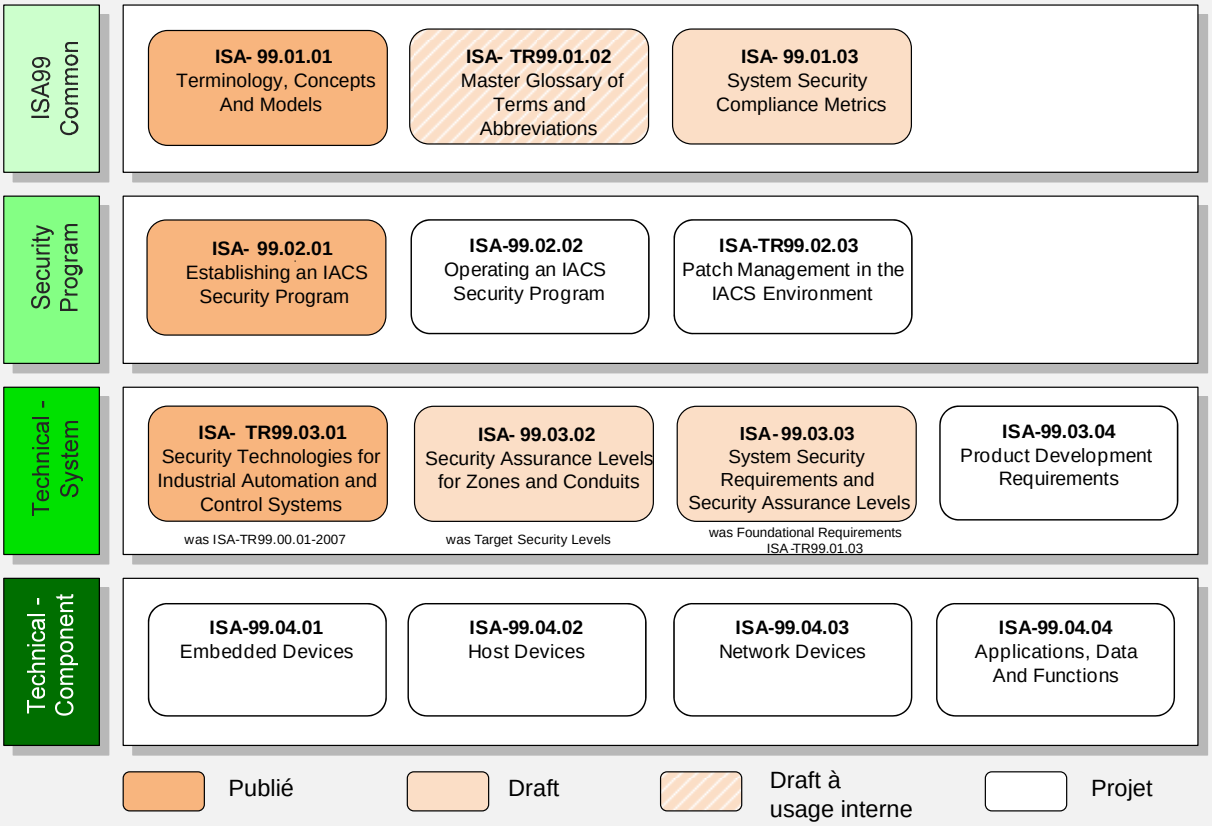

Figure 4 : Plan documentaire de l'ISA-99 – Sources : ISA et ISA-France

On notera tout d'abord que l'épisode Stuxnet démontre clairement la réalité du risque d'attaques majeures sur des installations sensibles de contrôle-commande. Après Stuxnet, il devient impossible de soutenir que le risque cyber-sécuritaire sur des installations de contrôle, fussent-elle isolées du monde extérieur, relève de la paranoïa ou de l'intoxication commerciale. D'autant plus que les moyens apparemment mis en œuvre pour le développement de Stuxnet, tout étant très importants, ne sont pas incommensurables au regard de ceux dont peut disposer une organisation terroriste.

Bien évidemment Stuxnet est clairement dans la typologie définie par l'ISA-99 une attaque de niveau 4 (niveau le plus élevé) c'est-à-dire « une attaque provenant d'une équipe disposant de ressources importantes notamment des moyens de calcul puissants et en grand nombre, et disposant d'un lapse de temps suffisant ». Parmi ce type d'attaques, l'ISA-99 cite « …celles provenant d'une organisation ayant les ressources et la motivation pour passer des semaines à analyser un système et développer des attaques 0-day ».

Au regard de l'ISA-99, les systèmes infiltrés ne présentaient pas un degré de protection suffisant face à au moins quatre des sept Foundational Requirements imposés par l'ISA-99 :

- FR1 – Access Control
  Identify and authenticate IACS users (including human users, processes, and devices), assign them to a pre-defined role, and allow them access to the system or assets.
- FR2 – Use control
  Enforce the assigned privileges of an authenticated IACS user to perform the requested action on the system

ISA-Flash est une publication périodique d'ISA-France, association loi de 1901. Directeur de la publication : Jean-Pierre HAUET Pour tout renseignement : info@isa-france.org – Tel : 01 41 29 05 09

or assets, and monitor the use of these privileges.

- FR3 – Data Integrity
  Ensure the integrity of information on communication channels and in data repositories to prevent unauthorized manipulation.
- FR4 – Data Confidentiality
  Ensure the confidentiality of information on communication channels and in data repositories to prevent dissemination.

Ceci rappelé, l'ISA-99 apporte-t-il une protection suffisante face à des attaques du type Stuxnet? La modestie s'impose compte tenu de la mise en œuvre dans Stuxnet de techniques extrêmement sophistiquées et notamment de quatre attaques 0-day contre lesquelles il est difficile de se prémunir faute d'en avoir préalablement identifié l'existence et le risque.

Toutefois les experts consultés s'accordent pour considérer que les préconisations de l'ISA-99 sont de nature à réduire considérablement l'étendue et les conséquences d'une contamination par un malware du type Stuxnet.

C'est d'abord **une question d'hygiène informatique générale** et l'ISA-99 souligne la nécessite de sensibiliser aux questions de cyber-sécurité tous les personnels amenés à travailler sur les systèmes de contrôle et à en assurer la formation. Cette sensibilisation se traduit notamment par une surveillance permanente de tous les accès au système, y compris les accès à distance et les accès physiques. Cela implique la surveillance de tous les points sensibles, le contrôle de toutes les modifications physiques ou logicielles, de toutes les manipulations, la prévention de l'introduction de tout dispositif de nature à causer des désordres matériels ou logiciels ou permettre la captation d'information, etc.

Un autre principe essentiel est celui du **contrôle des autorisations consenties** aux utilisateurs d'un équipement donné afin de ne leur consentir que les privilèges qui leur sont strictement nécessaires (principes du least priviledge et des least functionalities), en vérifiant, avant de laisser exécuter une action telle que le téléchargement de programmes ou de paramètres de configuration, que les privilèges correspondants ont été valablement attribués.

Les **mots de passe** doivent être gérés de façon rigoureuse. Leur temps de vie doit être limité et leur transfert doit faire l'objet d'une autorisation.

Un point essentiel, largement développé dans l'ISA-99, est le « **use control for portable and mobile devices** ». Le caractère critique des équipements tels que les clés USB y est souligné et la nécessité d'assurer un contrôle strict de l'usage de ces équipements est affirmé. Rappelons que, dans le cas de Stuxnet, la primo-infection est probablement liée à l'introduction de clés USB contaminées.

Le **contournement des pare-feu** joue, dans le cas de Stuxnet un certain rôle dans la propagation dès lors qu'elle repose sur des failles répertoriées. L'ISA-99 invite à installer des pare-feu pour assurer le cloisonnement des zones de sécurité définies dans le système mais incite à une certaine prudence quant à leur efficacité, tant il est vrai que trop souvent, la présence d'un pare-feu est considérée comme une panacée. Surtout l'ISA-99 invite à une gestion duale des pare-feu, associant une configuration positive des canaux utilisés en situation opérationnelle à une configuration négative interdisant l'utilisation des accès et des liaisons non utilisées.

De façon plus technique, la mise en place d'IDS (**Intrusion Detection Sofware**) est recommandée afin de surveiller l'accès aux données ainsi que le trafic sur les réseaux.

De même, il est recommandé de mettre en œuvre des SRP (**Software restriction Policies**) fournis avec Windows de façon à se protéger contre les logiciels non autorisés.

Ces dernières mesures trouvent évidemment leurs limites dans le fait qu'une attaque comme Stuxnet repose sur des failles 0-day et s'entoure de précautions extrêmes afin de rendre le code pirate invisible.
In fine, il resterait à examiner au niveau des systèmes touchés par les attaques si les principes de **défense en profondeur,** fondés sur un découpage des systèmes en zones et conduits suffisamment ilotés, ont été respectés afin de circonscrire l'impact des attaques et de leurs incidences éventuelles sur le fonctionnement des systèmes.

Stuxnet constituera à coup sûr pour les années à venir une référence et un cas d'école. Les enseignements à tirer de cet épisode iront en s'enrichissant au fur et à mesure que s'affinera la connaissance des mécanismes utilisés, de la résilience des systèmes visés et des conséquences qui auront pu, à court ou moyen terme, en résulter.
Dans le court terme, nous ne pouvons qu'inciter les concepteurs et les opérateurs de systèmes d'automatisme à s'investir suffisamment dans la prise de connaissance de l'ISA-99, seul référentiel aujourd'hui disponible appréhendant les problèmes de cyber-sécurité de façon rationnelle, partant des concepts généraux, puis venant aux dispositions à prendre au niveau des entreprises, des systèmes et des composants.

ISA-Flash est une publication périodique d'ISA-France, association loi de 1901. Directeur de la publication : Jean-Pierre HAUET Pour tout renseignement : info@isa-france.org – Tel : 01 41 29 05 09