ISA France Section

ISA Flash

Setting the Standard for Automation™

ISA FLASH N°44 – Novembre 2011 Bulletin d'information d'ISA-France

Au sommaire de ce numéro :

Sommaire | Evénements | Standards | Technologie | Formation

ISA99 (cyber-securité) : DuQu précurseur d'un nouveau Stuxnet – Jean-Pierre HAUET – ISA-France

Stuxnet

Dans l'ISA Flash N°40 de novembre 2010, nous avions relaté l'essentiel des informations à l'époque disponibles sur le malware **Stuxnet** qui s'est avéré comme étant la construction informatique malveillante la plus sophistiquée jamais rencontrée au cours des dernières années. L'une de ses caractéristiques essentielles résidait dans son aptitude à s'implanter de façon masquée dans des équipements fonctionnant sous Windows et, partant de là, à détecter d'éventuelles consoles de programmation de la gamme Siemens. Une fois installé dans l'une de ces consoles, il pouvait altérer de façon subreptice les programmes applicatifs supportés par les automates. Il est possible que des centaines de milliers de PC aient été contaminés par Stuxnet mais soient restés à l'état de « porteurs sains ». Par contre, le virus s' est effectivement développé dans des systèmes de contrôle industriel utilisant certains automates Siemens et en particulier dans ceux contrôlant les variateurs de vitesse des moteurs des centrifugeuses du centre d'enrichissement de l'uranium de Bushehr en Iran. Il aurait occasionné des dommages importants à une fraction significative du parc. Beaucoup ont considéré que Stuxnet avait été spécifiquement développé à cette fin.

La nouveauté technique de Stuxnet résidait dans son caractère modulaire et dans sa capacité à s'organiser localement en activant différents éléments de code en fonction de l'environnement rencontré. De nombreux spécialistes avaient alors considéré que Stuxnet serait suivi par d'autres construction du même type, montrant au passage, de façon manifeste, que les systèmes de contrôle industriel n'étaient pas à l'abri du risque cyner-sécuritaire.

Duqu : Le rapport du laboratoire de cryptographie et sécurité du système (CrySyS - www.crysys.hu)

Le 14 octobre 2011, un laboratoire universitaire, le laboratoire de cryptographie et sécurité du système (CrySys), basé à l'université de technologie et d'économie de Budapest, a publié un rapport très circonstancié démontrant l'existence d'un nouveau malware, présentant de fortes similarités avec Stuxnet. Le CrySyS a proposé de dénommer ce malware Duqu (prononcez : « diu-qiu ») en raison de la création par ce malware de fichiers temporaires portant le préfixe DQ. Ce rapport universitaire est allé assez loin dans la déconstruction de Duqu, analysant son architecture et montrant l'existence de deux variantes dont l'une masquée par un certificat valide volé à Taïwan (comme dans le cas de Stuxnet). Il a montré l'existence d'une « backdoor » permettant à Duqu de communiquer avec un centre de contrôle et de commande répondant à l'adresse, encore valide à l'époque, ***206.181.11.97***. Ce rapport soulignait que des pans entiers du nouveau malware présentaient de sres semblances très poussées avec Stuxnet et prouvaient vraisemblablement de la même équipe.

Toutefois un certain nombre de questions restaient posées, et notamment :

- Duqu utilise-t-il (comme Stuxnet le faisait) des failles « zero-day » ?
- Quel mode d'infection Duqu utillise-t-il ?
- Quels sont les mécanismes d'activation et d'extinction du malware ?

W32Duqu " The precursor to the next Stuxnet" - Rapport Symantec V1.3

Comme dans le cas de Stuxnet, Symantec a immédiatement mis en place une équipe d'analyse et entrepris des investigations additionnelles dont les conclusions sont publiées sur son site. Les développements qui suivent sont largement issus de la version 1.3 en date du 1er novembre 2011, du rapport intitulé **W32Duqu " The precursor to the next Stuxnet"** .

Une construction similaire à Stuxnet mais avec un objectif différent

Dans son rapport, Symantec confirme la similarité profonde entre les deux menaces Stuxnet et Duqu. Toutefois Duqu est une construction moins accomplie que Stuxnet et son objectif semble différent. Duqu ne dispose pas de capacités d'altérer les programmes résidents dans un ordinateur contaminé. Sa finalité semble être de rasse mbler un maximum d'informations sur les systèmes dans lesquels il s'est implanté et sur les infrastructures que ceux-ci contrôlent, afin de, probablement, pouvoir construire dans un deuxème temps une nouvelle version de Stuxnet visant de nouvelles cibles. D'où le qualificatif de **" The precursor to the next Stuxnet"** donné à Duqu.

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

Duqu est donc **cheval de Troie** qui ne contient pas d'éléments de code relatifs à un système de contrôle particulier (à la différence de Stuxnet) mais est destiné à récupérer et à transmettre des éléments d'information tels que l'enregistrement des commandes clavier, la liste des processus actifs, la liste des ordinateurs connectés etc.

Une attaque peut-être toujours active

Symantec fait remonter à décembre 2010 la première attaque de Duqu sur la base de sa première variante. La variante 2 (dont le driver est doté du certificat subtilisé à une entreprise de Taïpeh) semble avoir été utilisée à partir d'août 2001. Des téléchargements illicites ont été observés jusqu'au 18 octobre, c'est-à-dire après que l'existence de l'attaque a été mise en évidence par le CrySys. Il est donc possible que l'équipe à l'origine de l'attaque soit toujours active.

Le processus d'attaque

Celui-ci ne semble pas connu de façon certaine. Dans un cas, il a été démontré que Duqu parvenait à sa cible par l'intermédiaire d'un document Word corrompu, attaché à un e-mail, permettant à Duqu de s'installer grâce à une faille « zero-day » sur le moteur d'analyse de la police Win32k TrueType. Cette faille a fait l'objet le 4 novembre d'un avis de sécurité de la part de Microsoft (voir http://technet.microsoft.com/fr-fr/security/advisory/2639658) auquel est associé un correctif provisoire. L'ouverture du document Word permet à un noyau (dropper) de s'activer. Celui extrait du document Word un driver et un « installer » puis s'autodétruit. L'installer déchiffre trois fichiers détenus en interne qui seront les seuls à subsister après achèvement du processus d'installation.

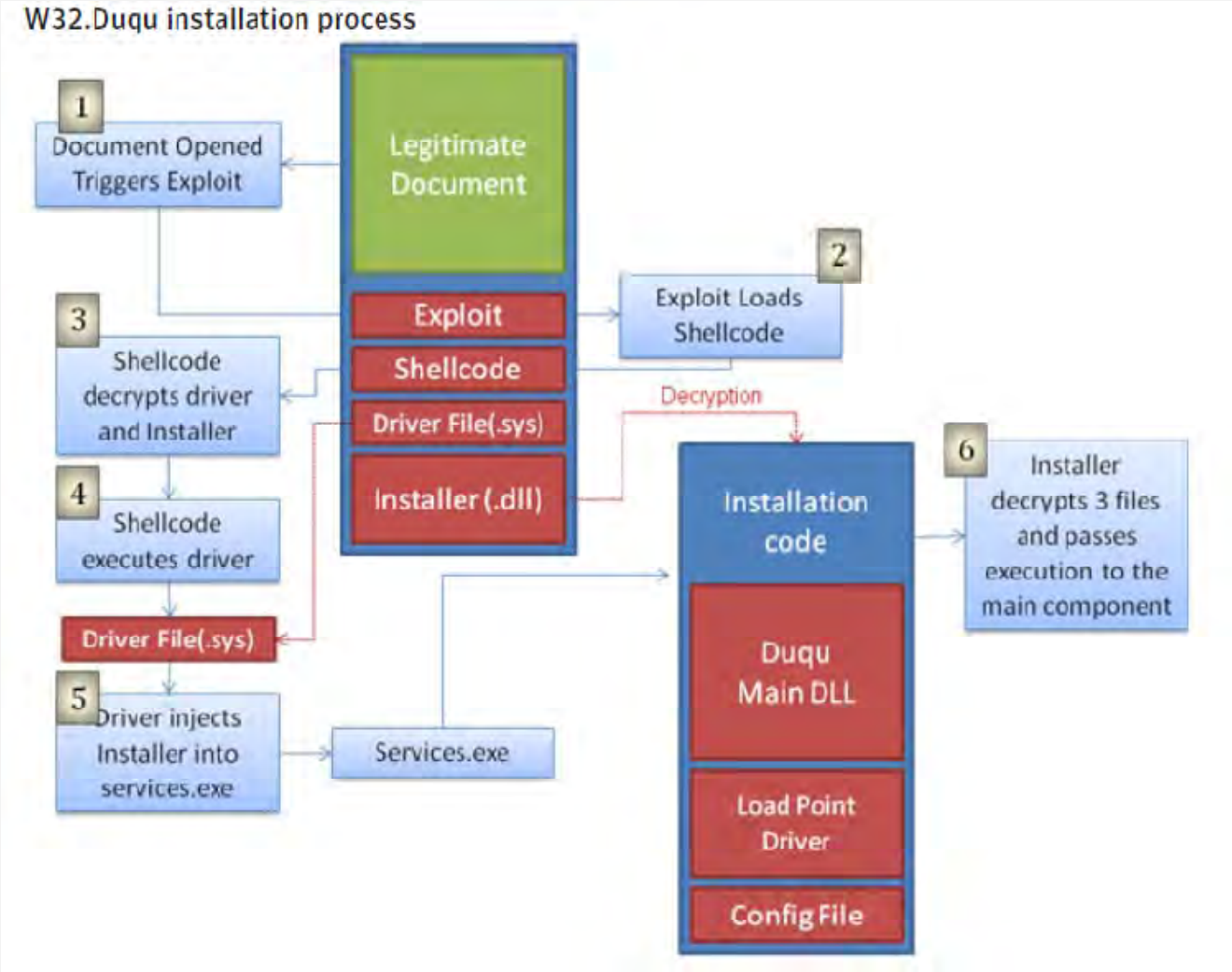


Figure 1 : Processus d'installation de Duqu. Source : *Symantec*

Le processus de télécontrôle et de propagation

Une fois installé, Duqu a la possibilité de communiquer, via http ou https, avec un centre de commande et de contrôle. Les adresses IP de deux serveurs, à présent inactives, ont été repérées, l'une en Inde (***206.183.111.97***), l'autre en Belgique (***77.241.93.160***). A partir de ces centres, les attaquants ont eu la possibilité de télécharger d'autres exécutables et d'installer en particulier le module de vol d'information permettant de rapatrier des informations en provenance du système contaminé. La communication se fait notamment en utilisant des fichiers fantoches de type Jpeg complétés par des informations chiffrées.

Duqu ne se reproduit pas par lui-même. Il peut recevoir de la part du centre de commande et de contrôle (C&C) les instructions lui permettant d'établir des connexions à l'intérieur du réseau de sa cible, via des ressources partagées. La machine contaminée sert de proxy du C&C pour aller infecter d'autres machines qui n'ont donc pas à entrer directement en communication avec le C&C, contournant ainsi les protections généralement mises en place.

Etat de la contamination début novembre 2011 et outil de détection

Selon Microsoft, la contamination par Duqu reste aujourd'hui limitée. Cependant Symantec fait état, dans son rapport V1.3 du 1er novembre, de l'existence de six organisations contaminées dans huit pays : France, Pays-Bas, Suisse, Ukraine, Inde, Iran, Soudan, Vietnam. Le malware aurait été aussi détecté en Autriche, Hongrie, Indonésie et Royaume Uni, ce qui conduit à la carte ci-contre publiée par Symantec.
Selon certains, la propagation serait rapide, selon d'autres, elle resterait limitée.

Figure 2 : Contamination par Duqu au 1er novembre 2011. Source : *Symantec*

Microsoft, après avoir diffusé un correctif provisoire, travaille sur la mise au point d'un correctif mais la tâche semble assez complexe. De plus, la révélation de détails sur la faille zero-day utilisée pour l'implantation de Duqu, faille qui touche l'ensemble des machines Windows, pourrait faciliter les attaques en direction des machines où le patch n'aurait pas encore été installé.

Le 10 novembre, le CrySys, à l'origine de la découverte de Duqu, a diffusé en open-source un outil de détection de présence de Duqu sur des ordinateurs ou sur des réseaux. Ce toolkit est accessible à l'adresse http://www.crysys.hu/duqudetector.html.

Conclusions – L'ISA99 au cœur du problème

Les tenants et les aboutissants de Duqu ne sont pas encore bien connus. Il est possible que cet épisode du théâtre des attaques cyber-sécuritaires n'ait que des conséquences limitées. Mais il montre, une nouvelle fois, la vulnérabilité des systèmes de contrôle à de telles attaques si les précautions nécessaires ne sont pas prises. Il vient souligner le caractère essentiel de l'action entreprise par l'ISA dans le cadre du comité ISA-99 (voir ISA-Flash N°43).

Chaque responsable de la conception, de l'exploitation et de la maintenance d'un système d'automatismes ou de contrôle de procédé, doit, en liaison avec les services informatiques de l'entreprise, être formé aux différents aspects de la menace cyber-sécuritaire et à la meilleure façon de s'en prémunir méthodiquement.

La prochaine formation ISA-France sur l'ISA99 se tiendra à Rueil-Malmaison le 8 décembre 2011. Inscrivez-vous dès aujourd'hui sur www.isa-france.org.

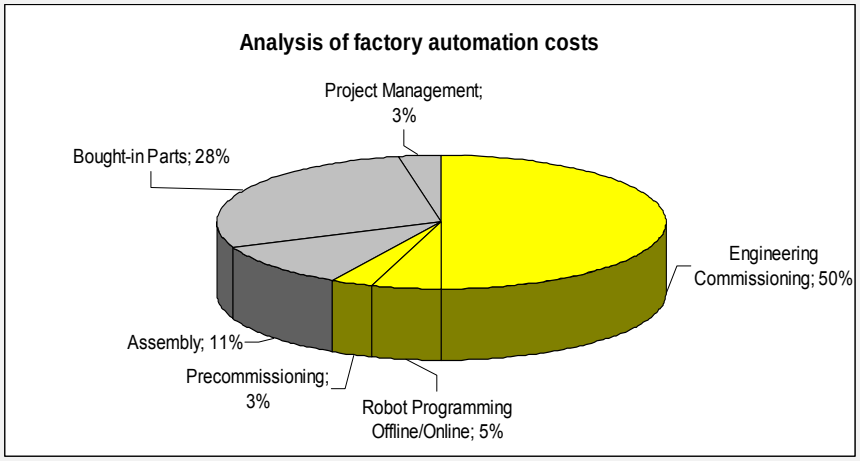
Jean-Pierre Hauet
jean-pierre.hauet@kbintelligence.com

Sommaire | Evénements | Standards | Technologie | Formation

AutomationML : Un nouveau standard pour réduire les coûts d'ingénierie et de mise en service – Christian Verney – ISA-France

Dans le domaine du process control et dans celui du manufacturier, les utilisateurs sont désormais à l'initiative de projets de normalisation et les fabricants de constituants d'automatisme sont amenés à se concerter et à répondre aux nouvelles demandes qui leur sont ainsi formulées. Le sujet développé ci après illustre cette nouvelle tendance. Nous pouvons nous réjouir de voir les différents acteurs se réunir pour élaborer un nouveau standard.

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



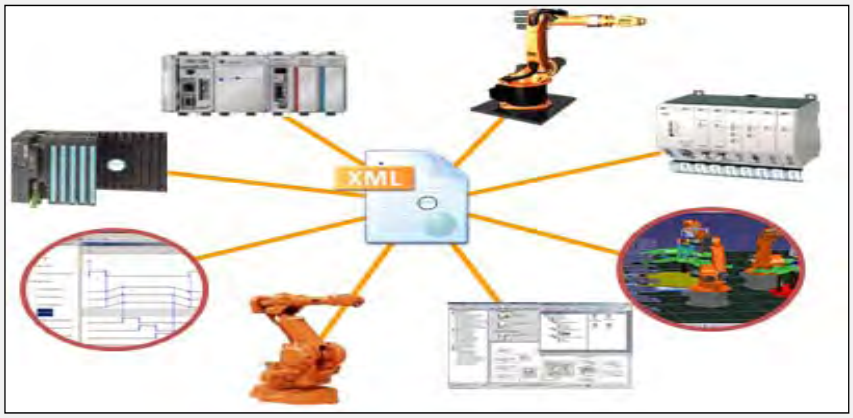
Pour un industriel la réduction des coûts est un souci permanent afin de conserver ses clients et son avance sur la concurrence. La figure ci contre montre que pour les contrôles d'application et la robotique 60% des coûts sont liés à l'ingénierie et la mise en service.

Les stratégies d'optimisation des coûts qui se sont focalisées par le passé sur la gestion des composants se concentrent désormais sur l'ingénierie.

Dans un environnement hétérogène le partage de données entre les différents outils est un facteur très important.

Les interfaces propriétaires et les différents outils compliquent considérablement ce partage d'information et conduisent à une efficacité des procédés désastreuse.

AutomationML (Automation Markup Language) est un format d'échange de données, basé sur XML, utilisé pour l'échange et le stockage des données de fabrication. L'objectif de ce standard est de permettre l'échange des données entre les outils hétérogènes d'une unité de fabrication.

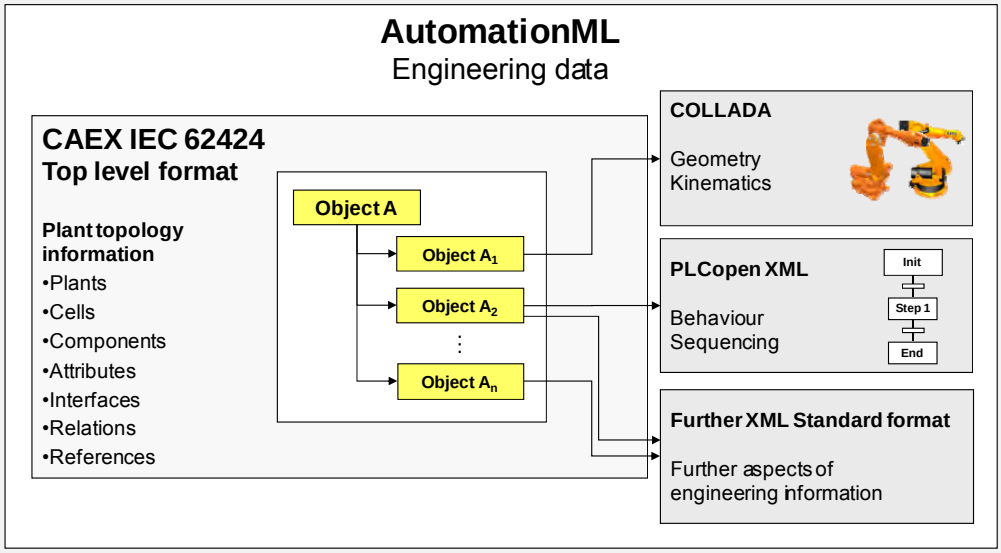


Comme le montre la figure ci contre, cela concerne les outils permettant la conception mécanique, les schémas électriques, les outils de dialogue homme machine, les automates et les outils de robotique.

Le cœur d'AutomationML est le format CAEX défini par la norme IEC 62424 (Computer Aided Engineering eXchange) qui permet d'interfacer les différents formats de données.

AutomationML, basé sur le concept orienté objet, permet la modélisation des différents aspects des composants industriels. Un objet peut être composé de sous-objets ou faire partie d'une plus grande composition. Les informations sur la topologie, la géométrie, la cinématique et la logique (séquence, comportement et le contrôle) sont les objets typiques à prendre en considération.

La figure suivante présente l'architecture de base d'AutomationML et le déploiement vers les données de topologie, géométrie, cinématique et de logique.



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

Ce standard "chapeau" de description d'un modèle objet en XML a la volonté de fédérer plusieurs modèles existants:

- Description de la cinématique 3D (robots) basé sur **COLLADA**
  COLLADA (Collaborative Design Activity) a pour but d'établir un format de fichier d'échange pour les applications 3D interactives. COLLADA définit un standard de schéma XML ouvert pour échanger les acquisitions numériques entre différents types d'applications logicielles graphiques

- Description de la logique automate: **PLCopenXML**
  PLCopen XML est un format d'échange neutre pour l'échange et le stockage des données de programmation des automates programmables basé sur le standard IEC 61131-3

- Des extensions sont possibles vers d'autres grammaires **XML "métier"**

Sous l'impulsion de l'industrie automobile le comité Allemand du TC65 (Industrial Process Measurement, Control and Automation) de la CEI a déposé un « new work item » qui a été accepté par les comités nationaux et un groupe de travail a été récemment formé au sein du SC65E (Device and Integration in Enterprise Systems).

AutomationML sera prochainement un standard multi parties sous la référence IEC 62714-x

Christian Verney
cv@cverney.com

Sommaire | Evénements | Standards | Technologie | Formation

ISA-France - Programme de formation de fin 2011

Code	Désignation	Calendrier 2011	
		Lieu	Date
JPH1	ISA-100 et les applications nouvelles des radiocommunications dans l'industrie - Deux jours	Rueil-Malmaison KB Intelligence 10, rue Lionel TERRAY	13 et 14 décembre 2011
JPH2	Réseau maillé ISA-100 - Approfondissement et mise en œuvre- Un jour *Le suivi préalable de la formation JPH1 est recommandé*	Rueil-Malmaison KB Intelligence 10, rue Lionel TERRAY	15 décembre 2011
JVI1	ISA-88 - Conception fonctionnelle du contrôle-commande industriel		Nous consulter
JVI2	ISA-95 - MES et intégration ERP/Exécution		Nous consulter
JVI3	ISA-88/95 - Architecture d'entreprise - Système de production industriel		Nous consulter
JVI4	B2MML/BatchML - Pratique des interfaces entre systèmes informatiques industriels		Nous consulter
JV15	ISA-88/ISA-95/B2MML : Spécification fonctionnelle et interopérabilité en informatique industrielle - Deux jours	Rueil-Malmaison KB Intelligence 10, rue Lionel TERRAY	20 et 21 décembre 2011
JVI6	Manufacturing Intelligence : Construire la Performance dans l'Entreprise	Rueil-Malmaison KB Intelligence 10, rue Lionel TERRAY	22 et 23 novembre 2011
BRI1	ISA-84 - Sûreté de fonctionnement avec les normes IEC61508 et IEC61511- Deux jours	Rueil-Malmaison KB Intelligence 10, rue Lionel TERRAY	6 et 7 décembre 2011
JPD1	ISA-99 - Cyber-sécurité des systèmes de contrôle - Un jour	Rueil-Malmaison KB Intelligence 10, rue Lionel TERRAY	8 décembre 2011

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

Adhérer à l'ISA et à l'ISA-France, c'est :

- **Accéder à des conditions préférentielles à 150 standards reconnus mondialement et à plus de 2500 documents techniques,**
- **Bénéficier de réductions importantes sur les manifestations ou formations organisées par l'ISA ou l'ISA-France,**
- **Accéder à une base documentaire de milliers de documents**
- **Entrer dans un réseau de 25 000 professionnels de l'automation**

Informations et bulletins d'adhésion sur www.isa-france.org et www.isa.org

Pour toute demande de renseignements : Tel +33 1 41 29 05 09 ou info@isa-france.org