Observatoire du Monde Cybernétique

Lettre n°6 - Juin 2012

Cette note est disponible sur le portail OMC. Pour y accéder, rendez-vous sur : https://omc.ceis.eu/

[lignesdedefense] Lancement de la chaire « Cyberdéfense » au CREC de Coëtquidan

Le CREC (Centre de recherche des écoles de Saint-Cyr Coëtquidan) inaugurera, le 2 juillet au cercle national des armées, une chaire dédiée à la cyberdéfense. Montée en partenariat avec Sogeti et Thales, elle aura trois objectifs principaux : le développement des enseignements dans le domaine de la cyber défense ; la mise en place d'un programme de recherche de haut niveau, avec des partenaires à la fois publics et privés, civils et militaires, français et étrangers, et intégrant d'autres centres de recherche internationaux ; l'installation, à terme, d'un centre d'expertise sur les questions de cyberdéfense aux écoles de Saint-Cyr Coëtquidan.

[LLA] Groupe de travail traitant de la confidentialité des données

Le conseiller d'Etat Olivier Schrameck dirige un groupe de travail consacré à l'adaptation de l'Administration à la « révolution numérique ». Un colloque sur le sujet se tiendra le 17 octobre. Composé, entre autres, de Laure Reinhart, DG déléguée d'Oséo, d'Olivier Régis, Directeur Général du forum pour la gestion des villes et des collectivités territoriales, et d'Agnès Verdier-Molinié, présidente de la Fondation Ifrap, ce groupe étudiera notamment les risques relatifs à la confidentialité des données.

[wsj.com] Lancement d'une enquête par le FBI sur les fuites concernant l'opération Olympic Games

Le FBI a ouvert une enquête afin de déterminer la source des révélations concernant les liens entre le gouvernement américain et le développement de Flame et Stuxnet. Selon le reporter du New York Times, David Sanger, qui a dévoilé l'affaire dans son ouvrage *« Confront and Conceal »*, de telles révélations délibérées seraient inhabituelles pour la Maison Blanche.

[defensesystem.com] Leon Panetta établit un cadre pour les cyberopérations du DoD

Le Secrétaire américain à la défense, Leon Panetta, a validé un nouveau cadre de mise en œuvre des « cyberopérations » pour toutes les agences du Ministère de la Défense, afin d'établir des normes communes.

[lefigaro.fr] La cyberguerre ou l'art de gagner du temps sur l'ennemi

Le Figaro dresse un portrait de l'industrie et de la géopolitique de la cybersécurité. Reprenant la comparaison avec l'arme atomique apparue en août 1945 faite par Michael Hayden, l'ancien patron de la CIA, le quotidien explique que l'usage de cyberarmes sert surtout à gagner du temps, par exemple en retardant le programme nucléaire iranien.

[indiatimes.com] L'Inde prête à se doter de cyber-armes

Selon le Times of India, l'Inde serait prête à se doter d'un arsenal de cyberarmes. Un projet en ce sens serait en cours de finalisation par le Conseil national de sécurité du pays, présidé par le premier ministre Manmohan Singh. Ce projet a été confié aux services secrets et à une agence de recherche nationale, la NTRO (National Technical Research Organisation).

[mehrnews.com] L'Iran prépare sa stratégie de cyberdéfense

Gholam Reza Jalali, directeur de l'Organisation de Défense Passive Iranienne, a annoncé officiellement le 15 juin la préparation d'un plan de cyberdéfense. Un cyber commandement a été établi le 19 mars ; la formulation d'une stratégie dans le cyberespace serait en cours.

[govinfosecurity.com] Le DHS nomme Rosemary Wenchel à un poste de coordination de la cybersécurité

Directrice actuelle des opérations d'information au Département de la Défense, Rosemary Wenchel va remplacer l'amiral de la Navy Michael Brown au poste de secrétaire à la coordination de la cybersécurité, au sein du Directoire de la Protection Nationale et des Programmes du DHS.

[nextgov.com] Le DHS fournira un pack de sécurité aux agences fédérales

Le *Department of Homeland Security* compte fournir en 2013 aux agences fédérales américaines un « pack de sécurité informatique » contenant des détecteurs de menaces en temps réel, un tableau de bord de gestion des tâches et des services de conseil. De tels méthodes et outils ont jusqu'à présent été testés au sein du Département d'Etat, et auraient déjà permis l'élimination de 89% de ce qui était considéré comme des risques pour les ordinateurs personnels et serveurs de l'institution.

[zdnet.com] L'Icann nomme un nouveau président

L'Icann a annoncé en fin de semaine dernière la nomination de Fadi Chehadé en tant que nouveau président. Il prendra ses fonctions à partir du 1er octobre, en remplacement de Rod Beckstrom.

[govinfosecurity.com] Une nouvelle stratégie de cyberdéfense pour Lockheed Martin

La société Lockheed Martin a décidé d'adopter une stratégie de défense originale par rapport à ses concurrents en matière de cybersécurité. Elle développerait actuellement une « Cyber Kill Chain », possédant sept niveaux de sécurité qu'un attaquant devra « escalader » afin d'accéder aux informations sensibles de sa cible, et qui représenteraient chaque fois une nouvelle opportunité pour le défenseur de recueillir des informations sur l'attaquant, à des fins de fortification de ses défenses futures.

[bits.blogs.nytimes.com] Invincea va équiper les militaires américains de smartphones sécurisés

La DARPA prévoit d'équiper les militaires américains de smartphones Android sécurisés. Un environnement virtuel hébergeant les applications des smartphones sera conçu par Invincea, pour un montant de 21 millions de dollars.

[afcea.org] Appel international pour une coordination de la cybersécurité

L'Association des Industries, des Technologies et d'Électronique du Japon, Digitaleurope, et le Conseil pour l'Industrie des Technologies de l'Information (ITI), ont élaboré les lignes directrices d'une collaboration internationale en matière de cybersécurité. Ils préconisent la transparence dans l'élaboration des législations, règlements et politiques de cybersécurité, la collaboration entre les secteurs public et privé lors de l'élaboration de telles politiques, ainsi que l'utilisation de normes reconnues mondialement (tests et certifications).

[symantec.com] Zemra : un nouveau botnet pour lancer des attaques DDoS

Symantec a détecté un nouveau botnet permettant de lancer des attaques DDoS contre plusieurs organisations à des fins d'extorsion de données. Le pack contenant le malware possède, comme pour Zeus ou SpyEye, un tableau de contrôle hébergé sur un serveur distant. Ses fonctionnalités sont étendues : communications chiffrées entre victimes et serveur d'attaque, contrôle de périphériques, téléchargement et exécution de fichiers binaires, vérification de la persistance de l'infection, propagation par périphériques USB, installation, mise à jour, et désinstallation automatiques.

[reuters.com] La Chine change sa législation concernant Internet

Les changements apportés à la politique chinoise de l'Internet ont été rassemblés sous le titre « Méthodes de gouvernance des services d'information de l'Internet ».

Ils élargissent la définition des fournisseurs d'informations sur Internet pour y inclure forums, blogs et microblogs. Cet élargissement forcera les utilisateurs à s'inscrire en utilisant leur véritable identité.

[koreaherald.com] La Corée du Nord disposerait-elle de la troisième plus grande capacité de cyberguerre ?

Selon le professeur sud-coréen Lee Dong-hoon, la Corée du Nord serait en train de renforcer ses capacités de cyberguerre. Le pays se placerait ainsi directement derrière la Russie et les États-Unis.

[ssi.gouv.fr] L'ANSSI publie un guide sur la cybersécurité des systèmes industriels

L'ANSSI a publié un guide sur la cybersécurité des SCADAs. Le guide, accompagné d'un cas pratique, se veut pragmatique et vise à accompagner les acteurs du monde industriel dans la prise en compte des enjeux liés à la cybersécurité. Sa méthodologie est présentée comme simple et illustrée par des situations concrètes.

[ssi.gouv.fr] L'ANSSI et l'AFNIC publient un état des lieux de la résilience de l'Internet français

L'ANSSI et l'AFNIC ont publié un rapport s'intéressant à la résilience de l'Internet français. Il est basé sur l'analyse des protocoles BGP et DNS pour établir un état des lieux de la situation actuelle. Le rapport considère le niveau de résilience français comme « acceptable ».

[Owni] Les rapports de la DCRI sur Anonymous

Le site OWNI a publié des extraits de procès-verbaux concernant les recherches de la DCRI sur le collectif Anonymous, après que ces derniers aient attaqué en 2011 plusieurs opérateurs électriques à travers le monde, dont EDF en France. Ces recherches auraient notamment amené les autorités à s'intéresser au Parti Pirate allemand.

[ewi.info] Un modèle de « santé publique » pour Internet

L'institut EastWest publie un rapport sponsorisé par Microsoft qui tente de s'inspirer du secteur de la santé publique, pour développer des pratiques de prévention et de lutte contre les virus informatiques.

[energy.gov] Le Département de l'Énergie américain publie un outil de renforcement de la cybersécurité des infrastructures électriques

Le 31 Mai 2011, le Département de l'Énergie a publié un Modèle de Maturité des Capacités de Cybersécurité dans le sous-secteur de l'électricité. Ce dernier est un outil d'évaluation et de renforcement des capacités de cybersécurité et de priorisation des actions associées.

[defense.gov] Le DoD américain publie une stratégie concernant les dispositifs et applications mobiles

Le DoD américain a annoncé la publication d'une stratégie relative aux terminaux mobiles, abordant tout particulièrement les problématiques critiques que sont la fiabilité, la sécurité et la flexibilité des infrastructures sans fil, des terminaux et applications mobiles.

Olympic Games, la « guerre secrète d'Obama »

Le 5 juin dernier était publié le livre du journaliste David E. Sanger, *« Confront and Conceal : Obama's secret wars and surprising use of american power »*. L'ouvrage relate avec une surprenante précision, les dessous de l'affaire Stuxnet. Selon le journaliste, le programme « Olympic Games » (le nom Stuxnet ne correspond en effet qu'à des extraits découverts dans le code)[1], aurait bien été orchestré par les Etats-Unis et Israël afin d'empêcher Téhéran de se doter de l'arme nucléaire. Il corrobore ainsi les conclusions des chercheurs comme Ralph Langner[2] ou Brian Krebs[3] en se basant sur des sources anonymes gouvernementales américaines, européennes et israéliennes. Il transforme en certitudes ce qui n'était jusque-là que des suppositions.

Sans revenir dans le détail sur toutes les étapes de la mise en œuvre d'Olympic Games, il est possible de retenir de l'ouvrage de Sanger quelques éléments essentiels.

D'Olympic Games à Stuxnet

> ***« The most elegant cyberattacks are a lot like the most elegant bank frauds […] They work best when the victim doesn't even know he's been robbed ».***

Stuxnet a réalisé sa mission avec brio, de façon discrète et anonyme, pendant près de trois ans. Frappant chirurgicalement les centrifugeuses de la centrale de Natanz, il provoquait ce qui passait pour de simples dysfonctionnements internes. Après chaque « frappe », le président Obama et ses conseillers se réunissaient en « salle de situation » pour faire le bilan : quelle est l'étendue des dommages réalisés ? De combien de mois les projets iraniens d'enrichissement nucléaire sont-ils repoussés ?

> ***« We think there was a modification done by the Israelis », aurait-on dit à Barack Obama, lors d'une réunion de crise après la propagation du ver.***

Les choses se sont envenimées lorsqu'un chercheur a involontairement diffusé le ver sur Internet après avoir connecté son ordinateur au système d'information de Natanz. Selon l'ouvrage de Sanger, les « *cyberguerriers* » auraient péché par excès d'ambition. Et une modification opérée par les israéliens dans le code du ver serait à l'origine de ce débordement. De quoi inquiéter la Maison Blanche sur les éventuels effets collatéraux de la propagation du malware et de sa potentielle découverte.

> ***« The worm was loose » - titre du prologue de l'ouvrage de David E. Sanger.***

Obama, un acteur clé. L'ouvrage révèle une facette du président Obama jusque-là ignorée. Il aurait en effet expressément donné l'ordre de poursuivre l'opération Olympic Games, et même, d'accroitre les offensives, malgré la diffusion incontrôlée du ver sur Internet et les risques de dégâts collatéraux difficiles à évaluer.

[1] Le terme de « programme » pour Olympic Games est à prendre au sens courant (ensemble de projets concourant à un même objectif). Stuxnet est bien le nom d'un « programme informatique » (un ver, en l'occurrence), nommé en référence à des mots-clés présents dans le code source.
[2] http://www.langner.com/en/blog/
[3] http://krebsonsecurity.com/tag/stuxnet/

L'annonce d'un changement de stratégie ?

La diffusion de ces informations à caractère hautement confidentiel soulève d'importantes interrogations. Est-il de l'intérêt des Etats-Unis de dévoiler les dessous de ce que Sanger considère comme la cyberattaque la plus sophistiquée et complexe que les Etats-Unis ont pu élaborer ?

La réponse à cette question ne peut être aisément tranchée. Les Etats-Unis chercheraient peut-être à légitimer ce qu'on appellerait une « cyberguerre juste »[4], « tolérable », en ayant choisi « la troisième option ». Objectif : éviter la première option : « laisser l'Iran se doter de la bombe » ou la seconde « entrer en guerre pour l'empêcher ». En décidant de poursuivre l'opération Olympic Games, Obama aurait ainsi évité le choix de méthodes plus conventionnelles, « à l'ancienne » : une frappe aérienne, qui aurait plongé les trois Etats dans une guerre sans précédent. Selon les propres termes de David E. Sanger : *« Olympic games was a new president's best shot at avoiding a new war, just as he was trying to end two others »*.

Certains avancent également que les fuites ayant conduit Sanger à révéler les dessous du programme Olympic Games ne peuvent qu'avoir été approuvées par l'administration Obama qui, en période d'année électorale, cherche à renforcer son leadership et sa fermeté contre le programme nucléaire iranien.

La perte de l'anonymat et la crainte du « strike back »

L'un des principaux avantages de l'attaque informatique est l'anonymat qu'elle procure. Anonymat qui réduit presqu'à néant tout espoir de riposte justifiée de la part de la victime. Si les informations divulguées par David E. Sanger sont vérifiées, ou suffisamment fiables, elles remettent en cause l'anonymat des instigateurs, allant jusqu'à frôler la justification d'une éventuelle riposte de la part de l'Iran. Que penser également de la « fuite » de Stuxnet sur Internet ? La question du reverse engineering de malware et des conséquences de la récupération et de l'amélioration du code à des fins, soit de riposte contre son créateur, soit d'exploitation par d'autres pays ou des groupes cybercriminels est, en effet, cruciale.

Une radicalisation qui pourrait stimuler la course à l'armement informatique

Un des autres effets serait surtout d'encourager certains Etats à poursuivre leur course à l'armement informatique et l'adoption de cybercapacités offensives. Certains experts comme Mikko Hyponnen de F-Secure considèrent en effet que les Etats-Unis ont ouvert la « boîte de Pandore[5] » en lançant Stuxnet (aucun démenti de la part des Américains ni des Israéliens) et qu'ils regretteront cette décision tôt ou tard.

La logique de dissuasion telle que perçue auparavant, axée sur la discrétion des acteurs, tend à se renverser[6]. Les Etats-Unis se dirigeraient-ils vers une stratégie plus « ouverte » consistant à assumer l'adoption de cybercapacités offensives ? La publication de ce livre, la diffusion d'offres d'emploi[7] explicitement tournées vers l'offensif ou les récents projets de la DARPA abondent en ce sens. Certains évoquent même l'apparition d'une nouvelle *« forme alternative de dissuasion, plus proche des modèles connus et conçue comme un objectif à long-terme où les instruments classiques de*

[4] http://www.theatlantic.com/technology/archive/2012/06/is-it-possible-to-wage-a-just-cyberwar/258106/

[5] http://www.nytimes.com/roomfordebate/2012/06/04/do-cyberattacks-on-iran-make-us-vulnerable-12/a-pandoras-box-we-will-regret-opening

[6] Voir les développements suivants : http://cidris-news.blogspot.fr/2012/06/linde-developpe-sa-lio-ou-comment-la.html

[7] http://threatpost.com/en_us/blogs/defense-contractor-northrop-grumman-hiring-offensive-cyber-ops-051812 et http://www.clearancejobs.com/jobs/1536410/cyber-software-engineer-2 (consulté le 20 - 05 -2012)

la diplomatie pourraient également être utilisés évacuant également les questions d'attributions des attaques »[8] ; dissuasion qui encouragerait certaines cyberpuissances émergentes à assumer, à leur tour, l'élévation de leurs capacités offensives dans le cyberespace[9].

Des éléments de contexte à retenir

L'ouvrage de David E. Sanger apporte aussi des éléments de contexte majeurs.

La place du droit des conflits armés dans la cyberstratégie américaine.

Un passage surprenant de l'ouvrage relate que le personnel chargé de l'élaboration d'Olympic Games aurait passé une majeure partie de son temps à s'assurer que le virus ne violerait pas le droit des conflits armés. Ce qui n'est pas sans rappeler le débat désormais récurrent portant sur la qualification d'une cyberattaque en agression armée. Les instigateurs d'Olympic Games auraient ainsi écarté, un à un, tous les critères de cette agression, en se garantissant : l'anonymat (pas d'imputabilité à un acteur étatique) ; la discrétion des effets du virus qui, passant pour de simples dysfonctionnements, évitaient de causer des dommages suffisamment graves et quantifiables pour atteindre le seuil exigé par la qualification d'agression telle que perçue par le Conseil de sécurité de l'ONU.

La sécurité des SCADAs.

L'auteur du livre éclaire le lecteur sur les différentes étapes ayant conduit à la compromission des ordinateurs de la centrale de Natanz. En cause, notamment, la « naïveté » des iraniens qui, sachant que leurs systèmes d'information seraient une cible prioritaire, n'ont trouvé d'autre solution que de les déconnecter purement et simplement d'Internet. Solution qui n'a pas résisté longtemps à des méthodes plus traditionnelles de pénétration physique des locaux par des agents de renseignement israéliens. Cette anecdote rappelle la place essentielle et souvent négligée de la sécurité physique en matière de sécurité des SCADAs (pour plus d'informations, voir article suivant « SCADAs : des cibles vulnérables et exposées sur Internet »).

[8] http://cidris-news.blogspot.fr/2012/06/linde-developpe-sa-lio-ou-comment-la.html
[9] http://articles.timesofindia.indiatimes.com/2012-06-11/india/32174336_1_cyber-attacks-offensive-cyber-government-networks

SCADAs : des cibles vulnérables et exposées sur Internet

La découverte de Stuxnet en 2010 a levé le voile sur les vulnérabilités des SCADAs. Ces systèmes de commande et contrôle industriels étaient historiquement considérés comme « sûrs » car isolés d'Internet et exploitant des technologies et protocoles de communication spécifiques. Stuxnet a remis en cause ces certitudes.

Aujourd'hui, ces SCADAs utilisent des technologies plus classiques et sont interconnectés aux différents systèmes d'information de l'entreprise. Connectés ou non à Internet, ces systèmes industriels, déployés dans des installations sensibles (centrale nucléaire, distribution d'électricité et de gaz, transport, pipeline, etc.), font donc face à des risques de cyberattaques ciblées, dont les conséquences peuvent être critiques.

Ces systèmes industriels restent néanmoins très différents par rapport à des systèmes d'information « de gestion ». Ils présentent des finalités, des contraintes et des cycles de vie très spécifiques. Ils nécessitent donc une approche de la sécurité plus proche de la sûreté de fonctionnement que de la Sécurité des Systèmes d'Information.

Quelques mythes entourant la sécurité des systèmes industriels

En juin 2012, l'ANSSI a publié un guide sur la cybersécurité industrielle. Il examine notamment les mythes relatifs aux systèmes d'information industriels :

Un réseau isolé donc protégé => les systèmes SCADAs sont de plus en plus souvent interconnectés aux réseaux bureautiques et de gestion de l'entreprise et parfois à Internet. Les clés USB (exemple de Stuxnet) et les interfaces de maintenance (contrôle à distance) sont autant de portes ouvertes pour la propagation de logiciels malveillants.

Utilisation de logiciels propriétaires spécifiques => ces logiciels comportent des vulnérabilités souvent dû à l'utilisation de composants standards (pour des raisons de coût) ou à l'absence d'analyse de risques menée pendant le développement du projet.

La SSI est incompatible avec la sûreté de fonctionnement => les principes de l'analyse de risque sont très proches de ceux de la sûreté de fonctionnement.

Le chiffrement, l'authentification, le filtrage sont incompatibles avec les contraintes des systèmes d'information industriels => les performances des composants utilisés dans les SI industriels permettent l'implémentation de ces mécanismes de sécurité (c'est plus compliqué pour les systèmes « temps réel »).

Une attaque informatique aura toujours moins d'impact qu'une attaque physique => une cyberattaque peut provoquer des dysfonctionnements volontaires ou un effet de bord, qui dans le cas d'installations sensibles, pourraient avoir des conséquences sur des vies humaines).

Des systèmes industriels vulnérables

Après Stuxnet, la communauté cybersécurité s'est intéressée aux failles spécifiques aux composants des systèmes SCADA. La publication de ces vulnérabilités a alors commencé à se multiplier et les éditeurs de solutions de SCADA ont enfin pris conscience de l'importance de les détecter et de les corriger :

- Au printemps 2011, Luigi Auriemma, un chercheur italien, publie 34 failles « 0-day » sur différents systèmes SCADA (Siemens Tecnomatix, Iconics GENESIS, 7-Technologies IGSS, et DATAC RealWin). La plupart des failles découvertes sont basiques : « buffer overflow », déni de service… Ces vulnérabilités sont rapidement converties en « exploits » exploitables dans les logiciels de test d'intrusion (Metasploit[10]). Une société russe Gleg[11] met en vente pour 1 000 $ un pack d'exploit spécial SCADA.

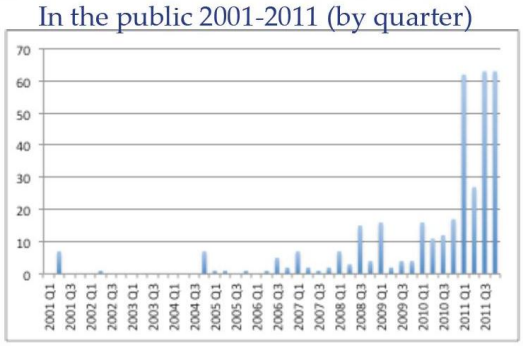
- Pendant l'été 2011, plusieurs chercheurs comme Ralph Langer ou Dillon Berresford publient des rapports sur des techniques d'attaques contre des automates SCADA de Siemens (déjà mis en difficulté avec Stuxnet). Des démonstrations sont effectuées lors de la conférence de sécurité Black Hat en août 2011. D'autres chercheurs publient de nouvelles vulnérabilités mais après les avoir communiquées aux éditeurs concernés et attendu la diffusion des correctifs. Une douzaine de failles est notamment mise à jour sur les produits Ecava Integraxor, 7-technologies IGSS, Samsung Data management, Siemens Simatic S7, Rockwell Rslinx Classic, Progea Movicon, Sunway Forcecontrol, Indusoft ISSymbol, Azeotech DAQfactory, Rockwell FactoryTalk, et Siemens Simatic WINCC.

- A l'automne 2011, Luigi Auriemma, publie une nouvelle liste de failles sur d'autres produits : Beckhoff TwinCAT, Measuresoft ScadaPro, Rockwell RSLogix, Carel PlantVisor, Progea Movicon / PowerHMI, DAQFactory, Cogent DataHub, eSignal, MetaStock, ISI rFactor et Race WTCC. Les failles sont répertoriées- sur son site Internet : http://aluigi.altervista.org/. Si en Europe, on préfère évoquer le cas des vulnérabilités SCADAs chinois, aux Etats-Unis, le CERT-ICS (dépendant du DHS) émet des alertes de sécurité pour chaque faille publiée.

- Toujours à l'automne 2011, l'avalanche de publication de failles s'accompagne de campagnes d'attaques par phishing (avec pièce-jointe malveillante) visant des ingénieurs automaticiens américains des secteurs du nucléaire et de l'énergie[12].

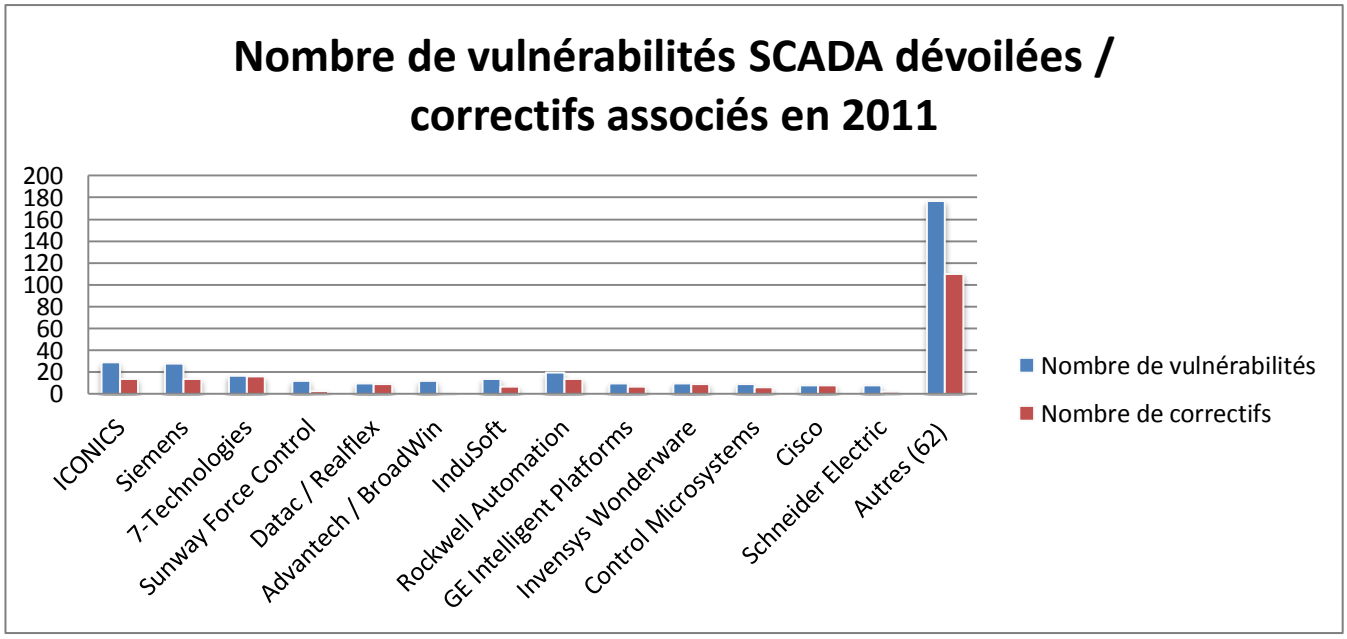
Fin janvier 2012 s'est tenu le « SCADA Security Scientific Symposium » (S4) à Miami. Cet événement, riche en enseignements en matière de cybersécurité industrielle, a notamment présenté des statistiques sur l'explosion du nombre de vulnérabilités des SCADAs. Principaux constats :

- Explosion du nombre de vulnérabilités publiques depuis 2011.
- Les constructeurs et éditeurs de solutions SCADAs sont tous concernés par ces failles. Ils n'ont jamais intégré la sécurité à leurs projets de développement informatique.
- Les correctifs de sécurité tardent à être publiés et sont, pour la plupart, inefficaces.



Source : CERT ICS

[10] http://scadahacker.com/resources/msf-scada.html
[11] http://scadahacker.blogspot.fr/2011/11/gleg-releases-ver-18-of-scada-exploit.html
[12] http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Sep2011.pdf

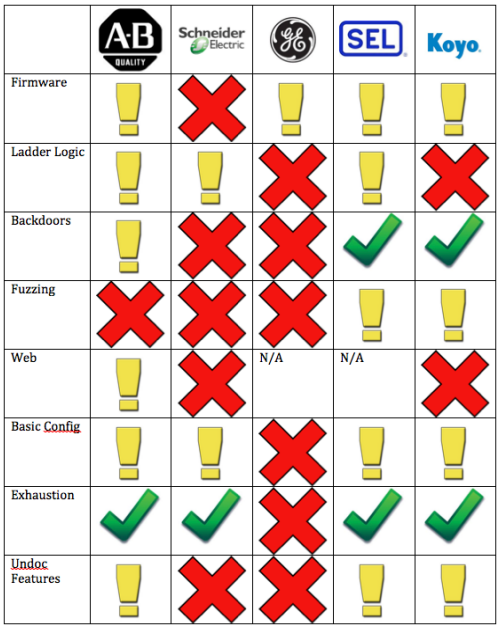


Source : CERT ICS

Le Symposium S4 a également été l'occasion de présenter le projet « BootCamp » visant notamment à dénoncer le peu de réaction des vendeurs de solutions SCADAs. Six chercheurs ont testé cinq constructeurs différents:

- Control Microsystems SCADAPack (bricked early on) ;
- General Electric D20ME ;
- Koyo / Direct LOGIC H4-ES ;
- Rockwell Automation / Allen-Bradley ControlLogix ;
- Rockwell Automation / Allen-Bradley MicroLogix ;
- Schneider Electric Modicon Quantum ;
- Schweitzer SEL-2032.

Les chercheurs ont également développé des « exploits » de certaines failles découvertes. Ces exploits ont été intégrés au logiciel de test d'intrusion « Metasploit » et à Nessus (pour les détecter).



- La croix rouge = une faille facilement exploitable sur la fonctionnalité
- Le point d'exclamation = une faille difficile à exploiter,
- La coche verte = aucune faille détectée

Des systèmes industriels exposés sur Internet

Comme évoqué précédemment, la (prétendue) sécurité des systèmes SCADAs reposaient en partie sur le postulat selon lequel ces systèmes industriels critiques n'étaient pas connectés à Internet. La démonstration d'Eireann Leverett, chercheur en sécurité, lors du Symposium S4, fait voler en éclat ce mythe[13].

Grâce au moteur de recherche de vulnérabilités « Shodan[14] » et en utilisant des mots-clés (associant nom du constructeur et nom de page d'administration), Eireann Leverett a découvert plus de 10 000 systèmes SCADAs connectés à Internet dont une majorité apparaissait en rouge (voir ci-dessous), donc vulnérables. Ce moteur de recherche permet en effet de retrouver très facilement des interfaces d'administration de modules SCADAs connectés à Internet (certaines entreprises, à qui appartiennent ces systèmes industriels, auraient reconnu qu'ils ignoraient que certains d'entre eux étaient directement connectés à Internet). Ces interfaces peuvent être vulnérables à des failles web classiques et à l'authentification (par exemple : utilisation des identifiants et mots de passe par défaut ou cassage par force brute).

Des failles basiques pour des systèmes critiques

En décembre 2011, Billy Rios, un ingénieur sécurité de Google, avait révélé que les identifiants et mots de passe par défaut des systèmes Siemens SIMATIC SCADA (login : Administrateur et mot de passe : 100). En novembre 2011, un pirate associé au pseudonyme "pr0f" publiait sur Internet des captures d'écran prouvant qu'il avait pu accéder au système de contrôle d'une usine d'approvisionnement en eau dans le sud de Houston. "pr0f" avait affirmé que l'accès au système était protégé par un mot de passe de trois caractères... Les vulnérabilités sur les systèmes SCADAs sont souvent publiques et trouver des victimes avec « Shodan » est relativement facile. Ces SCADAs vulnérables pourraient devenir des cibles privilégiées des hacktivistes ou de cybercriminels qui chercheraient à extorquer de l'argent aux exploitants de ces systèmes industriels.

Des hacktivistes (dont certains se réclamant d'Anonymous) ont également utilisé le réseau social Twitter et le site Pastebin.com pour diffuser des listes d'adresses IP appartenant à des SCADAs et des détails pour se connecter à certains d'entre eux, avec les identifiants et mots de passe par défaut. Israël et les Etats-Unis ont notamment été touchés par une fuite de données[15] de ce type et la France n'est pas épargnée. Dans l'une de ces listes figuraient également des données sur des systèmes industriels français[16] (appartenant à EDF). Si dans tous ces cas, rien n'indique formellement que ces interfaces permettent d'accéder à des systèmes critiques, le simple fait qu'elles soient exposées sur Internet est un risque.

Le logiciel Shodan - source : wired.com

Spécialistes en cybersécurité industrielle

France :

- Patrice Bock, Euriware

Monde :

- Eric Byres, Tofino
- Ralph Langner
- Joe Weiss, Applied Control Solution

[13] http://www.wired.com/images_blogs/threatlevel/2012/01/2011-Leverett-industrial.pdf
[14] http://raidersec.blogspot.fr/2012/02/searching-for-devices-using-shodan.html
[15] http://www.lemondeinformatique.fr/actualites/lire-anonymous-publie-des-details-sur-les-systemes-scada-israeliens-47388.html
[16] http://www.cyber-securite.fr/2012/01/25/cyber-menaces-contre-les-scada-francais/

Conclusion

La cybersécurité est un enjeu critique des systèmes industriels. De plus en plus connectés à Internet mais dépendant de technologies anciennes (voire obsolètes ce qui explique que, souvent, les fournisseurs déclarent tout simplement qu'ils ne publieront pas de correctif de sécurité), leur niveau de sécurité est encore loin de l'état de l'art. Les vendeurs de solutions SCADAs prennent seulement conscience des risques et des vulnérabilités qui touchent leurs produits. La cybersécurité n'a en effet jamais été au cœur de leur processus de conception.

Les recherches autour de la sécurité des systèmes SCADA se poursuivent en 2012. De nouvelles failles ont été dévoilées et rendues publiques au premier trimestre 2012. Le CERT-ICS continue de publier régulièrement des alertes de sécurité. L'organisme américain a également communiqué[17] récemment sur une recrudescence d'attaques ciblées (spear-phishing) menées contre des systèmes d'infrastructures critiques appartenant notamment à des entreprises de distribution de gaz. Des efforts commencent néanmoins à être menés en matière de cybersécurité industrielle. Ils émanent de différents acteurs :

- Des vendeurs : Siemens[18] a décidé d'intégrer des mécanismes de sécurité (firewall, VPN) à ses produits SCADA.
- Des Etats : le gouvernement américain, au travers du DoE (Departement of Energy) a lancé fin 2011 un plan stratégique décennal pour sécuriser les approvisionnements énergétiques du pays (électricité, gaz et pétrole).
- Des organismes normatifs comme le NIST (SP 800-82[19]) ou l'ISA (99[20]) qui ont publié des référentiels spécifiques pour améliorer la sécurité des systèmes industriels.
- Des agences nationales de cybersécurité : l'ANSSI[21] a publié en juin 2012 un guide sur la cybersécurité des systèmes industriels à l'attention des acteurs concernés.

Selon Patrice Bock[22], spécialiste français de la cybersécurité industrielle, « *la réalité du terrain n'est pas celle des patchs et des failles* ». Le brusque intérêt pour la sécurité des systèmes industriels (de la part des médias, des responsables de sites industriels mais aussi des organisations gouvernementales) a créé des besoins en matière d'audits et d'analyses de risques. Toujours selon Patrice Bock, les cabinets de conseil ne proposent pas encore de vraies offres concrètes et spécifiques pour les systèmes d'information industriels, ou alors elles ne sont pas adaptées voire dangereuses (en pratiquant des tests de vulnérabilités qui peuvent causer de vrais incidents industriels).

[17] http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Apr2012.pdf
[18] http://www.darkreading.com/advanced-threats/167901091/security/vulnerabilities/240001644/siemens-enhances-security-in-post-stuxnet-scada-world.html?utm_source=twitterfeed&utm_medium=twitter
[19] http://securid.novaclic.com/cyber-securite-industrielle/nist-800-82.html
[20] http://securid.novaclic.com/cyber-securite-industrielle/synthese-referentiels-cyber-secu-industrielle.html
[21] http://www.ssi.gouv.fr/fr/anssi/publications/communiques-de-presse/l-anssi-publie-un-guide-sur-la-cybersecurite-des-systemes-industriels.html
[22] http://securid.novaclic.com/cyber-securite-industrielle/no-news-good-news.html

Découvrez le nouveau portail OMC. Pour y accéder, rendez-vous sur : https://omc.ceis.eu/

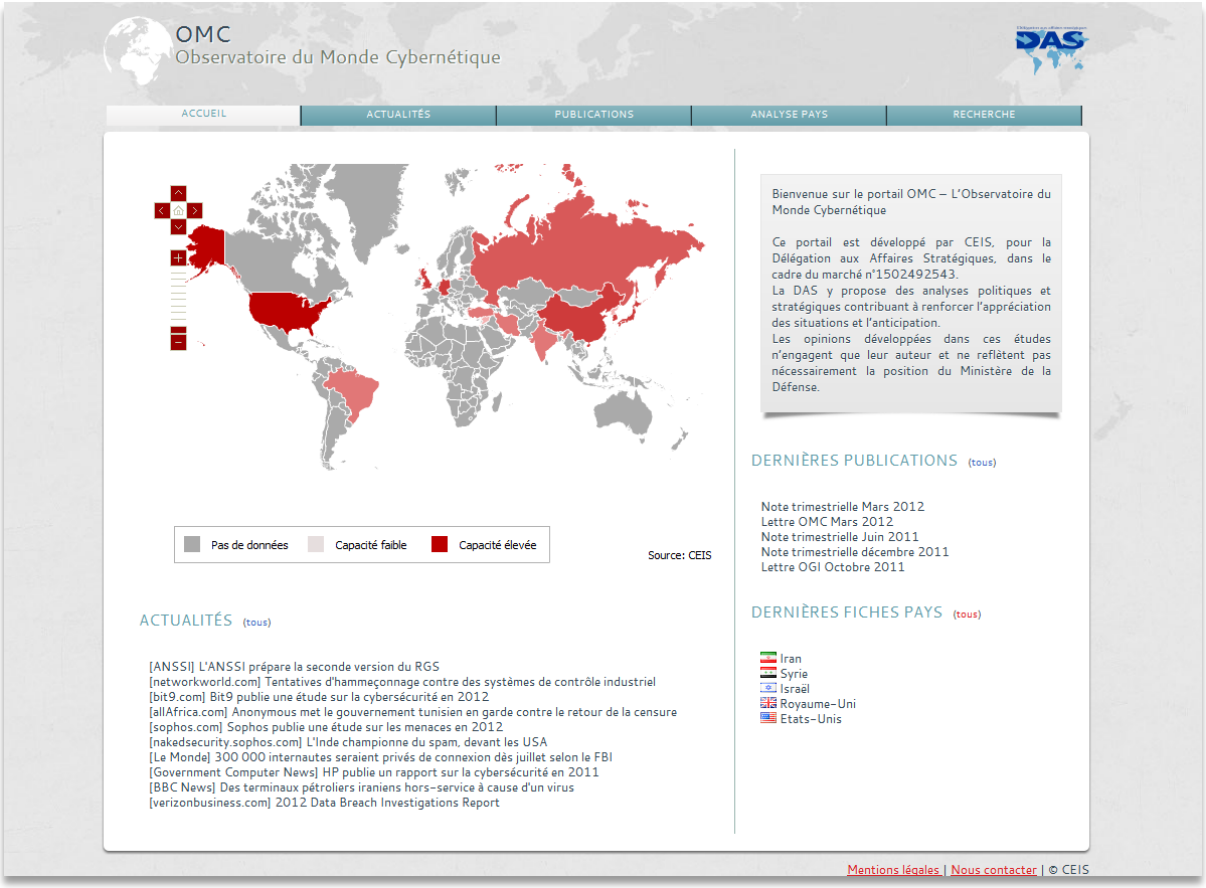


Figure 1 - Page d'accueil du portail OMC - https://omc.ceis.eu/

Pour vous y connecter, n'hésitez pas à demander vos identifiants à CEIS.

Contact : Barbara Louis-Sidney - blouis@ceis.eu et omc@ceis.eu

Conférence RSA Chine	Tallinn, Estonie	5 – 8 juin 2012
Black Hat Trainings & Briefings USA 2012	Las Vegas	21 – 26 juillet
Defcon 20	Las Vegas	26 – 19 juillet
Petit Déjeuner SecurityVibes	Paris	20 septembre
InfoSecurity International Summit 2012	Shanghai	25 – 26 septembre

Compagnie Européenne
d'Intelligence Stratégique

Téléphone : 01 45 55 00 20
Télécopie : 01 45 55 00 60
E-mail : gtissier@ceis.eu

Retrouvez cette lettre et l'ensemble des articles cités sur le portail
https://omc.ceis.eu/
(Accès soumis à authentification)

La Délégation aux Affaires Stratégiques propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation.

Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la DAS a confié à la **Compagnie Européenne d'Intelligence Stratégique (CEIS)** cet Observatoire du Monde Cybernétique, sous le numéro de marché 1502492543.

Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère de la défense et des anciens combattants
Délégation aux Affaires Stratégiques
Sous-direction Politique et Prospective de Défense
14 rue St Dominique 75700 PARIS SP 07