Observatoire du Monde Cybernétique

Lettre n°23 – Novembre 2013

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

[The Telegraph] Les banques britanniques ont pris part à un jeu de guerre basé sur des cyberattaques

Plusieurs milliers d'équipes appartenant à des institutions financières londoniennes ont pris part à un des plus grands jeux de guerre cyber au monde. Le jeu, baptisé "Waking Shark 2", consiste à bombarder les participants de scénarios et d'annonces, imitant la manière dont une cyber attaque massive les frapperait. L'exercice global a évalué la manière dont les banques garantiraient le fonctionnement des distributeurs automatiques dans un scénario de crise cyber. Londres n'est pas seule à faire ce genre de test, New-York ayant effectué quelques mois auparavant un scénario du même type baptisé "Quantum Dawn 2".

[Bulletins Electroniques] Rapport sur le marché de la sécurité des systèmes d'information

Un rapport sur le marché de la sécurité des systèmes d'information en Allemagne a abouti à la conclusion suivante : l'économie de la sécurité des systèmes d'information constitue pour l'Allemagne l'une des plus fortes branches d'avenir. Les points forts se situent dans les domaines de la cryptographie, des cartes à puce, des infrastructures à clés publiques, des solutions de haute sécurité (signature numérique notamment). La production de biens et de services dans le secteur de la sécurité des systèmes d'information en 2012 est estimée à 6,3 milliards d'euros, et concerne 9200 entreprises. Sur la période 2005 - 2012, l'industrie de la sécurité des systèmes d'informations a connu une croissance totale de 38,9%. La filière devrait rester prometteuse au moins à moyen-terme sur le marché allemand.

[01.Net] Des « failles de sécurité béantes » dans la messagerie du Parlement européen

Un hacker aurait réussi à avoir accès à l'ensemble des courriels de 14 députés européens en utilisant une faille dans le logiciel de messagerie de Microsoft, Exchange. Il aurait fait en sorte que les téléphones portables des eurodéputés se connectent sur Internet via le wifi de son ordinateur portable. Une fois cette première étape achevée, il a pu accéder aux données personnelles et accéder aux messageries des députés en exploitant la faille. Le site du Spiegel avait déjà révélé l'obsolescence de l'équipement informatique du Parlement européen.

[Le Monde] Ecoutes : Viviane Reding propose un service de renseignement européen

L'Union européenne devrait, selon vice-présidente de la Commission de Bruxelles et commissaire à la justice, Viviane Reding, se doter d'un service de renseignement afin de faire "contrepoids" aux Etats-Unis. Si des accords de coopération existent déjà entre les vingt-huit, la création d'un service de renseignement reste un sujet sensible qui avait été lancé en 2001 et rapidement abandonné.

[The Guardian] La surveillance de masse de la NSA et du GCHQ viole la législation européenne selon un rapport

Les auteurs d'une nouvelle étude sur la surveillance de masse, Sergio Carrera et Francesco Ragazzi, ont montré que les actions du GCHQ, de la NSA, et des services équivalents aux Pays-Bas, en France, en Allemagne et en Suisse violaient l'article 4.3 traité de l'Union européenne sur la "coopération sincère" entre Etats. Le rapport indique également que des agences européennes telles qu'Europol, ainsi que des instances de partage de renseignement au niveau européen agissent probablement en violation des droits fondamentaux garantis par l'UE.

[Security Week] L'OTAN lance le plus grand exercice de cyberdéfense à ce jour

L'OTAN a lancé ce mardi 26 novembre le plus grand exercice de cyberdéfense à ce jour, qui inclut 400 experts informatiques, juristes et représentants gouvernementaux venant de 30 pays différents. Le quart des participants étant basé à proximité de Tartu, tandis que le reste d'entre eux est réparti à travers l'Europe. Les capacités de vitesse de réaction, da coordination et

de prise de décision ont été testées au cours de cet exercice baptisé Coalition 2013.

[NRC] La NSA infecte plus de 50 000 réseaux informatiques avec des logiciels malveillants

De nouveaux documents révélés par Edward Snowden prouvent que la NSA a infecté plus de 50 000 réseaux informatiques pour voler des informations. La méthode utilisée, appelée Computer Network Exploitation (CNE), installe en secret un logiciel malveillant permettant à l'attaquant d'accéder à toutes les informations sur le réseau ciblé. C'est cette méthode qui avait également été utilisée par le GCHQ contre l'opérateur télécom belge Belgacom quelques mois auparavant. Le logiciel malveillant utilisé par la NSA est très sophistiqué et peut être désactivé pour ne rester qu'une "cellule dormante" dans le réseau, activable à nouveau si nécessaire.

[Miami Herald] L'industrie de l'énergie américaine en alerte face aux cyber attaques croissantes

L'industrie de l'énergie américaine a concentré 53% des cyberattaques contre le territoire américain entre octobre 2012 et mai 2013, et ce nombre va croissant. Les attaques d'Anonymous contre Shell, Exxon Mobile et British Petroleum ne sont que des exemples de façade face à des tentatives d'infiltration dans des systèmes beaucoup plus sensibles. 61% des entreprises du secteur de l'énergie aux Etats-Unis ont en effet subi des cyber attaques cherchant à prendre le contrôle de pipelines ou d'autres installations critiques. Selon McAfee, la cyberattaque la plus poussée - baptisée "night dragon" - aurait été effectuée par des hackers chinois et leur aurait permis d'exfiltrer depuis 2011 une très grande quantité de données confidentielles relatives au fonctionnement des infrastructures américaines et aux accords commerciaux en cours de négociation.

[Renesys] Les services DNS de Google quittent le Brésil en anticipation d'une nouvelle loi

En réponse à l'espionnage de la NSA, le gouvernement brésilien pousse pour l'adoption d'une loi obligeant les entreprises à stocker les données sur le territoire national. Cette loi pourrait être votée dans la semaine. En réaction, certains services DNS de Google ont commencé à quitter le pays tout comme ils l'avaient fait en Chine. Aucune décision officielle n'a encore été prise cependant de la part du géant d'internet américain.

[Les Echos] Espionnage: les fonctionnaires russes interdits de Gmail

Le FSB (service fédéral de sécurité) russe a interdit aux responsables de l'Etat de se servir de messageries étrangères, dans une lettre adressée aux représentants du Président russe dans les régions. Cette annonce fait suite aux différentes révélations d'Edward Snowden sur la NSA, et se fait dans le cadre d'une plus forte implication du FSB dans les questions de cybersécurité. Celui-ci devrait notamment recevoir le commandement du Cyber Command Russe d'ici la fin de l'année 2013.

[The Register] Les opérations secrètes des hackers chinois renforcent encore leur niveau de discrétion

Suite à la révélation du lien entre le groupe de hackers APT1 et l'Armée de Libération Populaire (PLA) chinoise par le rapport Mandiant en février dernier, les hackers chinois ont décidé de renforcer leur discrétion sur internet. Pékin continue de nier son implication dans les activités d'espionnage en ligne.

[Defense News] L'Inde débat de l'établissement d'un Cyber Command

Le commandement militaire Indien débat en ce moment de la mise en place d'un Cyber Command indépendant. Les révélations de la NSA et la fréquence des cyberattaques provenant des territoire Pakistanais et Chinois ont accéléré la décision stratégique indienne. S'adressant le 22 novembre aux responsables du ministère de la Défense du pays, le Premier ministre Indien Manmohan Singh a insisté sur le besoin de pouvoir contrer les "moyens de surveillance globaux". Un des débats concerne la désignation de l'entité qui sera en charge du Cyber Command, et qui ne

devrait pas relever du Ministère de la Défense Indien.

[France 24] Singapour relève son niveau d'alerte cyber suite à des menaces

Un hacker se revendiquant des Anonymous s'est servi de l'ordinateur infecté d'un journaliste pour annoncer que l'état de Singapour ferait l'objet de cyberattaques s'il n'acceptait pas de réduire les restrictions mises en place sur internet. En conséquence, Singapour a relevé son niveau d'alerte cyber et renforcé la protection de ses systèmes d'information.

[The Bahamas Weekly] Le gouvernement des Bahamas se concentre sur la protection des données

Le Premier Ministre, Perry G. Christie, a annoncé lors d'un symposium dédié à la protection des données, que celle-ci était critique pour la vie privée et la sécurité économique du pays. Les ministères de l'Economie et de la Justice travailleraient activement sur le sujet pour permettre aux Bahamas de bénéficier d'un niveau de sécurité rehaussé.

[ArsTechnica] Le cours du Bitcoin grimpe, et les coûts des rançongiciels baisse

Cryptolocker, le logiciel malveillant qui prend le contrôle de la machine d'un individu jusqu'à ce qu'il accepte de payer une rançon, s'est adapté à l'augmentation de la valeur du Bitcoin en divisant par deux la rançon que ses victimes ont à verser. Ces hackers, très au fait des théories économiques, ont ainsi adapté les rançons au prix qui apparaît "acceptable" pour les victimes. Cette stratégie devrait ainsi leur permettre de continuer leur activité de rançonnage malgré les fluctuations de la valeur du Bitcoin.

[Gadgets.NDTV] Le marché de la drogue en ligne, Silk Road, a rouvert un mois après sa fermeture par le FBI.

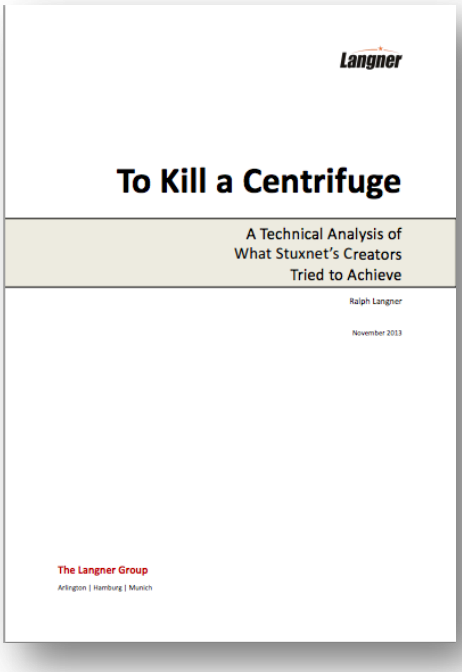
Un nouveau marché de la drogue en ligne, complètement anonyme, a rouvert ce mercredi en reprenant le même nom et la même apparence que son prédécesseur, Silk Road. Le FBI avait fait fermer le site le 1er octobre 2013 avec l'arrestation de son prétendu "cerveau", Ross William Ulbricht connu sous le nom de "Dread Pirates Roberts". Il aura fallu un mois pour recréer un site que le FBI aura tenté de fermer pendant deux ans et demi.

Stuxnet et objectifs politiques : deux versions, deux visions

Le ver informatique Stuxnet, découvert en 2010 par une société de sécurité informatique Biélorusse, a été conçu pour affecter les systèmes SCADA iraniens, plus particulièrement ceux de la centrale d'enrichissement de l'uranium de Natanz.

Selon le journaliste américain David Sanger, il aurait été conçu conjointement par les Etats-Unis et Israël, dans le cadre de l'opération Olympic Games visant à ralentir le programme nucléaire militaire iranien. Stuxnet est considéré comme la première "cyber arme" de par son niveau de sophistication élevé et les objectifs politiques clairement identifiables.

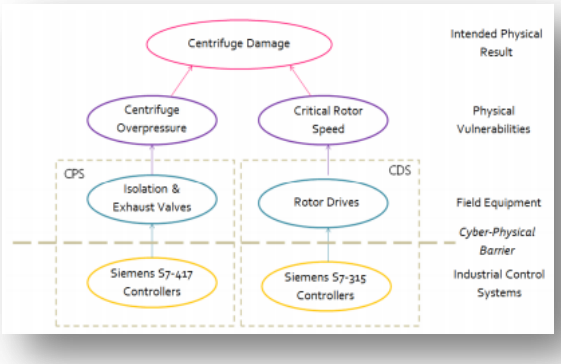
Une récente étude réalisée par Ralph Langner a montré que deux versions du virus avaient été conçues au cours de la campagne Olympic Games, aux caractéristiques et objectifs bien distincts.



Fonctionnement et faiblesses des systèmes de la centrale de Natanz

La centrale de Natanz fonctionne à l'aide de centrifugeuses d'enrichissement de l'uranium de type IR-1 datant des années 1960 - 1970. Celles-ci se sont montrées peu efficaces et peu fiables, mais faciles à construire de manière industrielle. Elles connaissent de manière fréquente des pannes et des dysfonctionnements nécessitant des opérations de maintenance voire de remplacement.

Pour remédier à la faible fiabilité des centrifugeuses, l'Iran a mis en place un système de protection en cascade permettant d'isoler les centrifugeuses défectueuses au cours d'une opération d'enrichissement, et d'évacuer la pression supplémentaire contenue dans celles toujours fonctionnelles. Les défauts des centrifugeuses étaient donc intégrés dans le processus d'enrichissement de l'uranium, et limités par un système de vannes permettant de les compartimenter et d'évacuer la pression.



Le système de protection en cascade était coordonné par un système de contrôle industriel conçu par Siemens dans les années 1990, S7-417. Il permettait aux ingénieurs de surveiller le

processus d'enrichissement de l'uranium et de détecter les défauts de fonctionnement des centrifugeuses à partir de panneaux de contrôle.

2007 - 2009 : Stuxnet, première version

David Sanger fait remonter les origines de Stuxnet à la crise entre Israël et l'Iran de 2006. L'infection par clé USB de la centrale nucléaire de Natanz aurait eu lieu entre 2006 et 2007, inoculant une première version de Stuxnet qui prit le contrôle des systèmes de contrôle industriel (SCADA) de Siemens S7-417. Une fois le ver dans les systèmes, il prend le contrôle des SCADA et est en mesure de montrer aux administrateurs une représentation faussée du système de protection en cascade. Programmé pour ne s'activer qu'une fois par mois, Stuxnet enregistre l'état des systèmes 21s avant de s'activer: il passe ensuite en boucle ces 21s, rendant l'état réel des centrifugeuses invisible aux yeux des administrateurs iraniens devant les écrans de contrôle. Une fois activé, le ver ne montre que ce qu'il souhaite montrer. S'ensuit une série de fermetures des valves qui permettent d'évacuer la pression, entraînant des dommages importants voire la destruction des centrifugeuses.

Cette première version de Stuxnet a pour caractéristique principale la furtivité. S'il causait des dommages aux centrifugeuses, ceux-ci restaient limités afin de ne pas attirer les soupçons. Ralph Langner estime que 50% des coûts de conception du ver ont été dédiés à la furtivité, et ce de manière effective puisqu'en 2009 - lorsque la seconde version de Stuxnet est apparue - la première version n'avait toujours pas été détectée.

Stuxnet, seconde version

La seconde version de Stuxnet date de 2009 et a des caractéristiques différentes de son prédécesseur. Dans cette version, le ver sacrifie sa furtivité pour gagner en potentiel destructeur. Alors que la première version de Stuxnet avait été inoculée directement par clé USB, la seconde version se réplique et se propage largement au-delà des systèmes SCADA de Siemens. Une fois inoculé, le virus s'active une fois par mois pour accélérer la vitesse de rotation des turbines de 15% par rapport au seuil nécessaire, entraînant des risques élevés d'auto destruction.

La seconde version de Stuxnet est plus directe et utilise des moyens plus destructeurs pour ralentir le programme d'enrichissement de l'uranium iranien. Elle est cependant bien moins furtive car la destruction simultanée de plusieurs centrifugeuses d'enrichissement risque d'attirer l'attention des ingénieurs iraniens.

Evolution des objectifs politiques à travers les deux versions du ver

La première version de Stuxnet se fond parfaitement dans le fonctionnement normal des SCADA. Le fait qu'il ait été inoculé directement par clé USB, et qu'il mette l'accent sur la furtivité plutôt que sur la destruction montre que son concepteur souhaitait avant tout que celui-ci ne soit pas identifié.

La seconde version introduit une rupture très intéressante, et une prise de risque -calculée ou non - supplémentaire de la part des attaquants. Le fait tout d'abord que la seconde version puisse se propager sur des systèmes autres que les SCADA Siemens indique que les attaquants avaient apparemment perdu leur capacité à injecter directement le virus, et devaient donc prendre le risque que Stuxnet se propage en dehors de la centrale de Natanz, augmentant ainsi le risque qu'il soit repéré.

Plusieurs raisons peuvent expliquer le changement de 2009.

La première est expliquée par David Sanger et est corroboré par l'analyse faite par Ralph Langner : les attaquants n'avaient aucune idée de l'efficacité de la première version de Stuxnet. Son haut niveau de complexité et sa furtivité ne garantissaient pas de résultats tangibles en termes de ralentissement du programme iranien. La perte du renseignement "interne" qui aurait inoculé directement la première version de Stuxnet par une clé USB pourrait avoir encore réduit la capacité des attaquants à estimer les dégâts causés. Le choix d'un mode de fonctionnement plus destructeur aurait pu être motivé par la volonté de poursuivre Olympic Games avec des résultats plus tangibles.

La seconde est la possibilité pour les attaquants de se revendiquer, ou d'être identifié malgré l'absence de reconnaissance officielle, comme les concepteurs de la première "cyber arme" inaugurant un nouveau champ de bataille dans le cyberespace. La seconde version de Stuxnet date en effet de 2009, année d'entrée en fonction du président américain Barack Obama, qui a mis l'accent sur les programmes de cyber défense mais aussi sur la mise en place de capacités cyber offensives à travers le Cyber Command et la NSA, tous deux dirigés par le général Alexander.

Comme le conclut Ralph Langner, "les effets les plus significatifs de Stuxnet ne sont pas à constater à Natanz, mais à Washington DC et à Fort Meade".

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

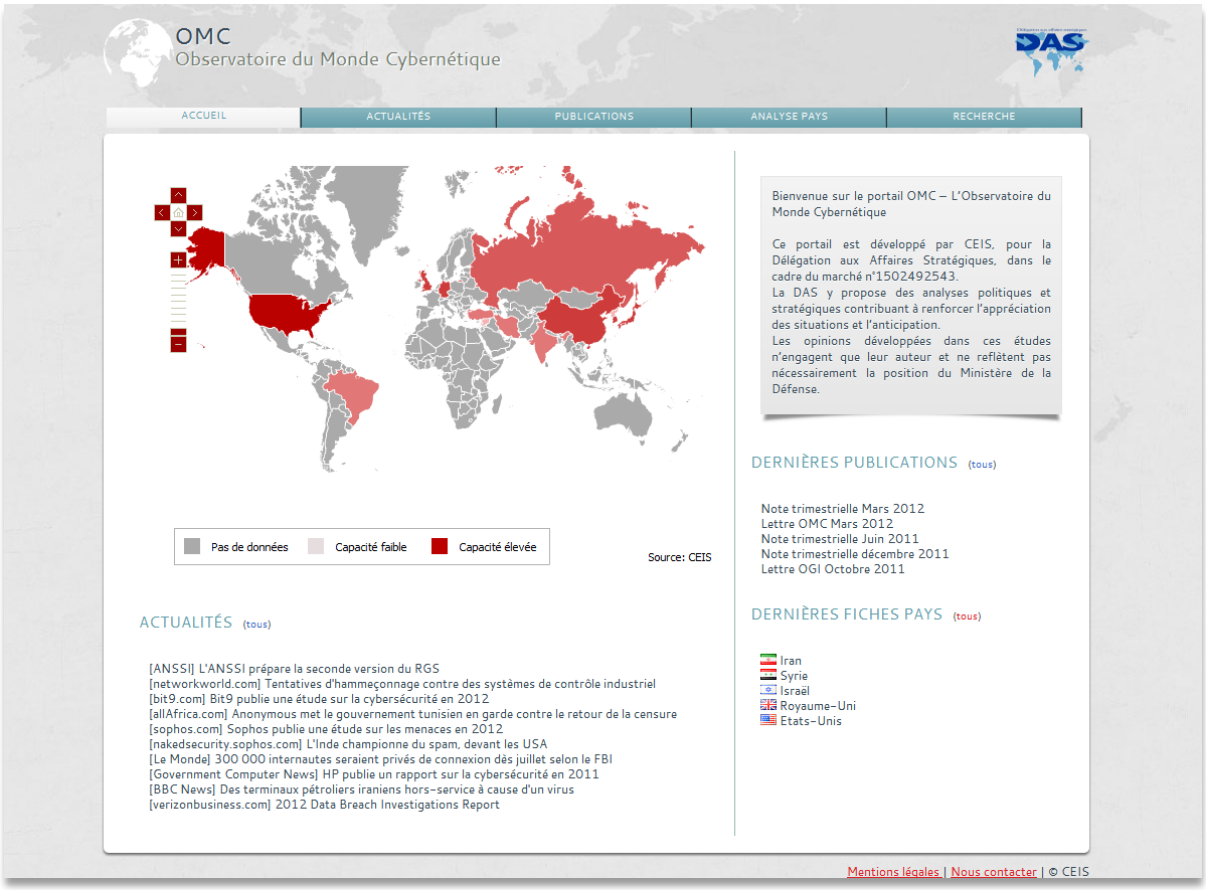


Figure 1. Page d'accueil du portail OMC - https://omc.ceis.eu/

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

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

Cyber Security and Digital Forensic 2013	Kala Lumpur (Malaisie)	3 - 5 décembre
Botconf'13	Nantes	5 - 6 décembre
Conférence CLUSIF : L'Europe, le monde, la SSI... et leurs règles	Paris	12 décembre
Colloque annuel du CDSE : "La sécurité au service de l'éthique"	Paris	19 décembre
Panorama de la cybercriminalité du CLUSIF	Paris	16 janvier
Forum International de la Cybersécurité	Lille	21- 22 janvier
Université AFCDP des Correspondants Informatique et Libertés	Issy-les-Moulineaux	27 janvier

Compagnie Européenne d'Intelligence Stratégique

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

Les opinions exprimées dans cette lettre n'engagent que la responsabilité de leurs auteurs.

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