Observatoire du Monde Cybernétique

Lettre n°28 – Avril 2014

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

[Usine Digitale] Axelle Lemaire s'exprime lors du sommet Net Mundial

Pour son premier déplacement hors de France depuis la prise de ses fonctions, Axelle Lemaire a tenu à rappeler l'engagement français pour une meilleure gouvernance de l'Internet. Ce dernier, entre espace d'échange potentiel pour les cultures et symbole de dynamisme économique, ne doit pas devenir une zone de non droit, mais un espace de liberté où les droits doivent être affirmés. La vision française repose sur des principes simples : ouverture, transparence, participation de toutes les parties prenantes. Une gouvernance pensée collectivement et acceptée de tous doit être mise en place. Les Etats portent la voix de ceux qui ne sont pas encore représentés, il faut donc garantir une responsabilité collective sur Internet. Le défi consiste donc à inventer un nouveau modèle de gouvernance multipartite.

[Global Security Mag] Siemens initie une formation à la cybersécurité des systèmes industriels

Une des branches de Siemens en France (le Secteur Industry) a lancé une offre de formation tournée vers la cybersécurité des systèmes industriels. Les techniciens et autres spécialistes de la sécurité des systèmes d'information seront ainsi réunis sur des périodes de deux jours et demi, afin de « se former ensemble aux bonnes pratiques de sécurité d'un système industriel ». L'entreprise propose aux stagiaires une introduction aux automatismes industriels et à la sécurité des systèmes de l'information, avec des exercices pratiques et des exemples d'attaques décrivant la manière dont elles ont été orchestrées.

[Clubic] OVH et Atos veulent un espace Schengen des données en Europe

Thierry Breton (Atos) et Octave Klaba (OVH) ont rendu un rapport commandé en 2013 par le gouvernement pour promouvoir les acteurs français du Cloud. Les PDG de ces deux groupes appellent à la création d'un cadre réglementaire permettant de mieux entourer le cloud computing en Europe. Pour eux, l'enjeu serait de bâtir une alternative aux géants américains emmenés par Amazon, Google ou Microsoft. Parmi les dix propositions formulées, on retiendra notamment la création d'un label « Secure Cloud », rassemblant « tous les services de cloud respectant un ensemble de normes en matière de qualité de service ».

[ANSSI] Heartbleed : l'ANSSI publie trois recommandations

En réaction à la faille Heartbleed affectant les bibliothèques OpenSSL, l'Anssi a publié trois recommandations. Elle préconise ainsi la vérification de la présence d'une version d'OpenSSL vulnérable et mise à jour si besoin, la révocation des certificats et génération de nouvelles clés en cas de suspicion de compromission des clés de chiffrement, et le changement des mots de passe sur les services en ligne utilisés. Si ces recommandations n'apportent pas de nouveaux éléments particuliers, un bulletin d'alerte a été mis en place, renvoyant régulièrement vers les explications techniques de la faille, ainsi qu'un bulletin d'actualité.

[Le Monde] La neutralité d'Internet sort renforcée du Parlement européen

Dans le cadre de la révision du paquet Télécom datant de 2009, le Parlement européen a « reconnu et consolidé la neutralité du net ». Ce principe est censé garantir en théorie un traitement technique identique à tous les fournisseurs de contenus. Cependant, cette neutralité était progressivement remise en question par les opérateurs de télécoms, ceux-ci restreignant l'accès à certains services. Si le projet rédigé par la commission européenne prévoyait certaines exceptions, comme le fait que les opérateurs puissent créer des « services spécialisés », le Parlement européen a réduit le nombre des exceptions, en les limitant à l'application d'une décision de justice, à la préservation de la sécurité du réseau ou à la fourniture de services ne pouvant fonctionner correctement sur un réseau classique.

[Objectifnews] Cybersécurité dans l'aéronautique et le spatial : groupes, PME, labos et universités s'allient à Toulouse

Une quinzaine d'acteurs économiques ont pris part à un programme intitulé Albatros et dédié à la lutte contre la cybercriminalité dans le domaine de l'aéronautique. Pour Emmanuel Volckringer, directeur programme chez Steria, « trois types de menaces planent sur les entreprises : une interruption de la production, une perte d'exploitation et un risque de vol d'informations stratégiques ». Parallèlement à ce rassemblement d'entreprises, deux formations universitaires spécialisées sont en train d'émerger dans la région de Toulouse. Avec ce programme, l'objectif est également de créer des emplois dans le domaine de la cybersécurité.

[Journal du net] La CJUE invalide la directive sur la conservation des données personnelles

La directive sur la conservation des données personnelles imposait aux opérateurs d'archiver certaines données de communications télécoms. Pourtant, la Cour de justice de l'Union européenne a considéré que cette obligation était incompatible avec la Charte des droits fondamentaux de l'Union Européenne. Adopté en mars 2006, « le texte obligeait les opérateurs télécoms à archiver des informations sur les communications des citoyens », pour une durée de six mois à deux ans. La Cour a estimé que cette directive permettait une ingérence excessive et disproportionnée, face aux droits fondamentaux et au respect de la vie privée.

[Lemondeinformatique] Heartbleed force les grands acteurs IT à s'allier autour d'OpenSSL

Microsoft, IBM, Google, Facebook, VMware et huit autres grands noms de l'industrie informatique ont rejoint l'initiative Core Infrastructure supportée par la fondation Linux et visant à renforcer la sécurité des projets Open Source les plus sensibles et vulnérables. Ils vont ainsi apporter leur soutien financier et leur expertise à cette « Core Infrastructure Service », représentant tout de même un financement de plusieurs millions de dollars. Parmi les projets prioritaires de cette fondation figure la résolution des problèmes persistants à la suite de la découverte de la faille Heartbleed.

[Securityweek] Le centre de recherche aérospatial allemand aurait été la cible d'une cyber-attaque

Le centre de recherche aérospatial allemand aurait été la cible d'une cyber-attaque commanditée par une agence de renseignement étrangère pendant plusieurs mois. En effet, les ordinateurs de scientifiques et d'administrateurs réseaux auraient été infiltrés par des programmes espions. Le gouvernement allemand a considéré cette attaque comme étant très sérieuse, sachant que des technologies de l'armement étaient visées. Des experts en informatique ont découvert que ces logiciels espions étaient programmés pour s'autodétruire une fois découverts.

[Usine Digitale] Verizon Communications publie son rapport annuel

Selon le rapport annuel de Verizon Communications intitulé « Data Breach Investigations Report », si pour 49% des cas, les intrusions malveillantes « motivées par l'espionnage » provenaient de Chine et d'autres pays d'Asie Orientale, dans environ 25% des cas, l'origine géographique de l'intrusion n'a pas pu être déterminée. Surtout, cette étude attribue les cas d'espionnage informatique aux Etats dans 87% des cas.

[New-York Times] Obama permet l'usage de certaines failles informatiques par la NSA

Le président américain Barack Obama a considéré que dans la plupart des cas, les bugs découverts devaient être révélés dans le but de protéger le public et les entreprises, permettant également de réduire les risques d'espionnage ou d'attaques. Cependant, il a également indiqué qu'une exception devait être prise en compte, lorsque qu'une faille peut toucher à la sécurité nationale ou à l'application de la loi. Dans ces cas précis, la NSA ne serait pas obligée de publier les failles découvertes et pourrait les utiliser.

[Usine Digitale] Le Brésil protège ses citoyens de la NSA avec une « constitution internet »

Dans le but de protéger les citoyens du pays contre l'utilisation de leurs données par de grands groupes ou par des Etats, le Congrès brésilien a adopté une Constitution Internet. Celle-ci vient réglementer les usages sur Internet, en protégeant et garantissant la confidentialité des données émises par les usagers d'Internet. Ce texte représente une certaine avancée en ce qu'il empêche la « coopération entre les entreprises du secteur de l'IT et les agences et services d'espionnage électronique ».

[Le Monde Informatique] Une start-up israélienne teste un système de détection des attaques similaires à Stuxnet

La start-up israélienne ThetaRay a développé, en partenariat avec General Electric, une technologie de sécurité permettant de détecter les attaques similaires à celles du ver Stuxnet sur les systèmes d'infrastructures critiques dans le domaine de l'énergie. Cette solution serait actuellement testée dans une centrale électrique de l'Etat de New-York. Et aurait reçu l'appui financier de plusieurs partenaires.

[Le Parisien] Pas de surveillance « massive » en Russie, répond Poutine à Snowden

Edward Snowden, ex-consultant la NSA, a fait une intervention surprise lors de la séance annuelle de questions-réponses du président Vladimir Poutine, en interrogeant ce dernier sur la surveillance en cours en Russie. Or, si Vladimir Poutine a précisé que les services spéciaux utilisaient les « moyens modernes appropriés » pour effectuer de la surveillance, la mise en place d'une surveillance à l'image de celle mise en place par la NSA est pour lui tout bonnement impossible, en raison des moyens techniques moins important dont disposent la Russie, mais également de son règlement juridique strict « concernant l'utilisation par les services spéciaux de ces moyens ».

[Nextgov] Echanger sur la cybersécurité n'enfreint pas la concurrence

Les responsables américains ont annoncé que des entreprises qui partageraient des informations en matière de cybersécurité pour se protéger de piratages informatiques ne seraient pas poursuivies pour avoir enfreint les règles relatives à la concurrence. Certaines entreprises craignaient d'être poursuivies pour pratiques anticoncurrentielles si elles partageaient des informations concernant la cybersécurité et les attaques informatiques dont elles pouvaient faire l'objet.

[Kaspersky] La dernière étude de Kaspersky montre une augmentation de l'utilisation des malwares

La dernière étude menée par la société Kaspersky montre une augmentation de l'utilisation des malwares destinées aux attaques financières. Depuis 2013, le nombre de piratages perpétués à l'aide de malwares a augmenté jusqu'à atteindre le chiffre de 28, 4 millions, soit une augmentation de près de 27, 4% par rapport à 2012. Deux nouvelles formes de malware auraient été découvertes par Kaspersky, une s'attaquant par exemple au contenu des portefeuilles de bitcoins.

[National Cybersecurity] L'ECA vise la Syrie

Un hacker du nom de "ZerOPwn" s'est récemment infiltré sur les sites dédiés à l'emploi en Syrie, présentant les noms de domaine « job.sy » et « realestate.sy ». Il a ainsi pu révéler une liste de 60 000 noms, pseudonymes, numéros de téléphone et adresses personnelles, ainsi que plusieurs mots de passe. Ce n'est pas la première fois que ce hacker s'en prend à des sites syriens. Déjà le mois dernier, il s'était attaqué à des sites bancaires ou encore d'autres sites officiels du gouvernement.

[Cyberland] Attaque sur le service Google Public DNS

Google Public DNS, service lancé en 2009, « a été créé pour rendre le web plus rapide et plus sûr » en proposant à ses utilisateurs une arborescence de serveurs récursifs. Or, à la mi-mars 2014, certains serveurs du service ont été attaqués et détournés pendant près d'une demi-heure, touchant les réseaux du Brésil et du Venezuela, obligeant à une redirection du trafic vers des réseaux BT – Amérique Latine. Ayant probablement exploité une vulnérabilité de Border Gateway protocol, cette attaque permet de rediriger le trafic vers un routeur contrôlé par le pirate.

[Networkworld] Le malware Zeus exploiterait des certificats numériques valides

Une variante du cheval de Troie Zeus s'attaquant aux banques a récemment été découverte. Cette variante utilise une vraie signature électronique, lui permettant d'échapper à la surveillance des navigateurs Internet et des anti-virus. L'entreprise de cybersécurité Comodo a annoncé avoir repéré près de 200 fois ce cheval de Troie en analysant les données de ses clients.

.

AET : buzzword ou véritable menace ?

Les termes désignant les différents types de cyberattaques sont de plus en plus nombreux. Qualifiés de « buzzwords », certains recouvrent toutefois une réalité bien concrète, à l'image des AET *(« Avanced Evasion Techniques »).*

Une technique d'attaque silencieuse

Plus évoluées, plus nombreuses, il est incontestable que les attaques contre les systèmes d'information ont des conséquences de plus en plus importantes : en 2013, ce sont plus de 40 000 cyberattaques qui ont été recensées[1].

Parmi les attaques, les APT (« *Advanced Persistant Threat* » - menaces persistantes avancées) font beaucoup parler d'elles, notamment du fait de leur fréquence : une attaque de type APT serait détectée toutes les 1,5 seconde[2]. Le « succès » de ces attaques s'explique en partie par l'emploi de techniques qui connaissent une certaine popularité, tant au niveau de leur utilisation par les attaquants que par les éditeurs de solutions de sécurité qui proposent de nouvelles systèmes de protection. A leur tour, les AET (pour « *Avanced Evasion Techniques* »), ou *techniques d'évasion avancées*, font également beaucoup parler d'elles. Les AET constituent un nouveau défi pour les systèmes de sécurité des réseaux : à la différence des moyens de contournement connus, les AET permettent à l'attaquant d'infiltrer le réseau de manière furtive, invisible, pour les solutions de sécurité classiques.

A titre d'exemple, les équipes de Stonesoft et de l'Université de South Wales ont testé les solutions classiques de sécurité disponibles sur le marché et ont conclu à l'issue de leurs recherches que celles-ci faisaient l'objet d'un contournement par AET[3]. Le test consistait à utiliser plusieurs types d'AET pour cacher le ver Conficker, bien connu depuis les dégâts que celui-ci a occasionné[4] - et donc normalement détecté assez aisément par les systèmes de sécurité, à 10 IPS reconnus[5] : aucun d'entre eux n'a détecté cette combinaison de techniques d'intrusion. Cette découverte a mis en exergue le fait que cette technique permettait aux cybercriminels de mener des attaques sur un système vulnérable sans être détectés.

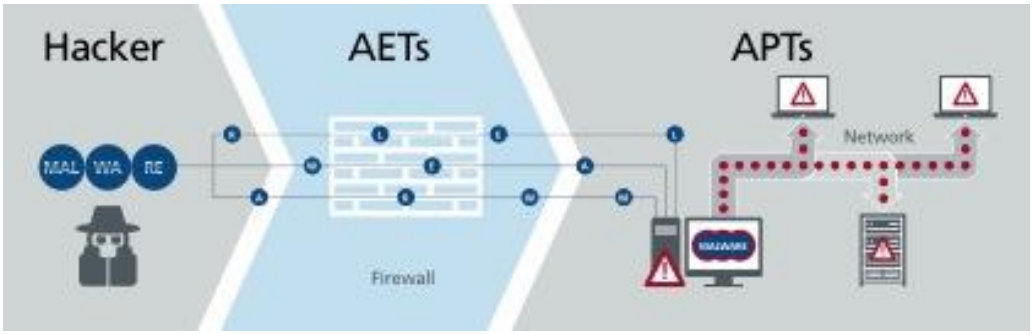
L'échec des solutions « classiques » de sécurité

Le nombre de variantes d'AET[6] qui vont servir aux attaquants pour mener de manière indétectable une attaque est estimée à plus de 2250, ce qui se traduit par un risque élevé pour les systèmes d'information qui, protégés par des solutions classiques de sécurité telles que les IPS (Intrusion Prevention System) ou un pare-feu, deviennent donc très vulnérables aux attaques.

A titre d'exemple, le cheval de Troie *ZeuS* a utilisé des AET pour créer une entrée dans le registre du système d'exploitation de la cible de l'attaque[7], permettant ainsi d'infecter le navigateur internet de manière invisible

[1] http://www.infosecurity-magazine.com/view/37247/enterprise-cyberattacks-more-than-double-in-2013/
[2] http://www.silicon.fr/dave-merkel-fireeye-lutter-contre-apt-technologies-hommes-93395.html
[3] http://www.zataz.com/news/21095/Advanced-Evasion-Techniques.html
[4] http://ibnlive.in.com/news/worst-virus-in-years-infects-65-mn-computers/82996-11.html
[5] Magic Quadrant - Gartner
[6] http://www.solutions-logiciels.com/magazine_articles.php?titre=Lavion-furtif-du-hacker&id_article=562
[7] http://www.processor.com/editorial/article.asp?article=articles/P3302/34p02/34p02.asp&guid=

et de subtiliser de la même façon les informations entrées par l'utilisateur (login, mots de passe, etc.). Ce cheval de Troie a été utilisé pour voler des informations bancaires de particulier mais aussi pour subtiliser des informations sensibles au sein d'entités gouvernementales ou d'entreprises.



McAfee - *The Security Industry's Dirty Little Secret, the debate over advanced evasion techniques (AETs)*, p. 4

Malgré cela, les entreprises ont tout de même investi l'an passé plus de 13 milliards $ dans les solutions de sécurité dites « traditionnelles »[8], ce qui mettrait en avant l'absence de sensibilisation de ces dernières sur l'évolution des menaces.

Une absence de sensibilisation des entreprises

Cette tendance est confirmée par une récente étude commandée par McAfee au cabinet Vason Bourne[9], menée auprès de 800 DSI (américains, britanniques, allemands, français, australiens, brésiliens, et sud-africains), qui reconnaissent que leurs entreprises restent dans l'ensemble très peu sensibilisées à ces techniques d'attaques. Toujours selon ce même rapport, un quart des personnes interrogées admettent que leur réseau a été la cible d'attaques informatiques, 40 % d'entre-elles estimant que les AET ont joué un rôle important dans ces menaces.

Deux difficultés semblent ressortir :

- D'une part, les acteurs de la sécurité semblent encore trop peu sensibilisés à l'impact des AET, préférant se réfugier dans la facilité des solutions plus « classiques ». Les entreprises ont tendance à privilégier la mise à jour de solutions déjà existantes et maîtrisées par leurs équipes.

- D'autre part, les acteurs responsables de la sécurité des systèmes d'information au sein de l'entreprise, lorsqu'ils sont sensibilisés à ces nouvelles techniques, rencontrent des difficultés à convaincre les décideurs de la réalité de ces techniques mais aussi des dégâts que les attaques qui en découlent provoquent.

Partant de ce constat, il apparait normal que les attaques utilisant ces techniques se généralisent et aient des conséquences majeures pour les entreprises (financières, industrielles ou réputationnelles). Ces dernières devraient ainsi remettre en cause leurs paradigmes de sécurité actuel et à accroitre leur niveau de protection.

[8] http://www.gartner.com/newsroom/id/2595015
[9] http://www.mcafee.com/us/resources/reports/rp-security-industry-dirty-little-secret.pdf

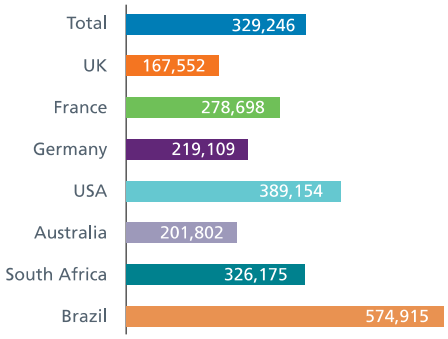
AET, vrai menace ou marketing?

En 2010, le directeur des recherches de Gartner (Bob Walder), expliquait dans une note de recherche intitulée *Advanced Evasion Techniques (AET) : Weapon of Mass Destruction or Absolute Dud*[10] que « *les techniques d'évasion ne sont certes pas nouvelles mais elles représentent malgré tout une véritable menace pour la sécurité des infrastructures réseau* […] *Les recherches récentes sur le sujet ont remis le sujet au goût du jour et c'est une bonne chose. Les éditeurs de sécurité réseau doivent désormais consacrer du temps et des ressources à la recherche de solutions pour contrer ce problème* ».

Cela pose donc la question de savoir si les AET, même si elles contribuent à la prolifération des menaces, ne constituent pas également un argument commercial mis en avant par certains éditeurs de solutions de sécurité pour promouvoir leurs produits ou proposer de nouvelles offres[11]. Car le marché mondial de la cybersécurité se porte bien et devrait passer de 63,7 milliards en 2011 à plus de 120 milliards en 2017[12]. En France, ce marché, qui atteignait 900 millions € en 2013, connait une croissance annuelle de plus de 9% qui devrait se maintenir jusqu'en 2017.

L'engouement pour la protection contre les AET par les éditeurs de solutions de sécurité pousse donc à s'interroger sur leurs rôles dans une certaine forme de « course à l'armement », conséquence d'une culture de la peur entretenue chez les utilisateurs[13].

Toutefois, même s'il est certain que ce « marketing de la peur » existe, il l'est tout autant que les menaces sont bien réelles. Les organisations les plus sensibles se doivent d'exercer une vigilance accrue à l'égard de menaces réseau traditionnelles car selon le rapport suscité, plus de 800 000 attaques ayant employées des AET auraient été menées, avec une moyenne de plus de 320 000 AET découvertes par les responsables de la sécurité des entreprises interrogées.



McAfee – Réponse à la question : "Combien d'AET pensez-vous avoir découvert?"

Les AET mettent également en exergue l'importance considérable, voir excessive, apportée aux performances des produits au détriment de la sécurité réelle. Les entreprises se trouvent ainsi dans l'obligation de repenser la sécurité des architectures afin que leurs systèmes d'information soient correctement protégés.

[10] http://www.brain-networks.fr/wa_files/Les_20recommandations_20du_20Gartner_20relatives_20aux_20AET_20_28EN_29.pdf
[11] http://www.globalsecuritymag.fr/Stonesoft-sensibilise-aux-Advanced,20110407,23056.html
[12] http://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html
[13] http://www.frc.ch/articles/personne-ne-veut-supporter-le-cout-de-la-securite-informatique/

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

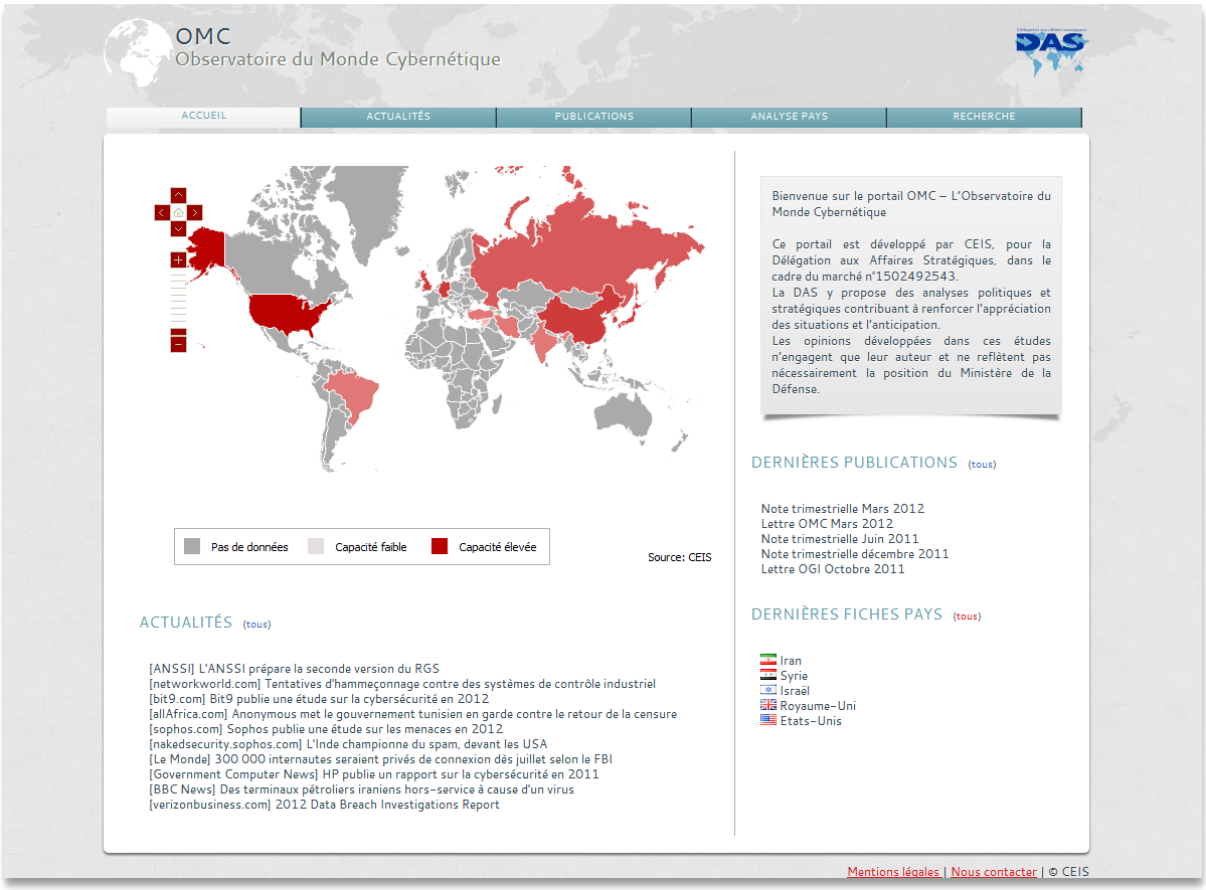


Figure 1. Page d'accueil du portail OMC - https://omc.ceis.eu/

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

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

NETmundial	Sao Paulo, Brésil	23 - 24 avril
The Third International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec2014)	Beyrouth	29 avril
Info Security	London	29 avril – 01 mai
EUROCRYPT 2014	Copenhague	11 mai
4ème Forum Europe – BIG DATA : usages et enjeux de transformation	Paris	13 mai
Infiltrate 2014	Miami	15 mai
SSTIC	Rennes	4 – 6 juin

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