Observatoire du Monde Cybernétique

Lettre n°13 – Janvier 2013

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

[Global Security Mag ; CEIS] Kader Arif, Manuel Valls et Fleur Pellerin au FIC 2013 : des projets structurants annoncés

Le 5ème Forum international de la Cybersécurité s'est déroulé lundi 28 et mardi 29 janvier, à Lille Grand-Palais. Avec plus de 2000 participants, une quarantaine d'ateliers et le soutien de nombreux partenaires, cette édition a connu un véritable succès. Kader Arif, ministre délégué auprès du ministre de la Défense, chargé des Anciens Combattants, a notamment eu l'occasion de remettre le Prix du Livre Cyber à deux auteurs : Pierre-Luc Réfalo, auteur de « La sécurité numérique de l'entreprise, l'effet papillon du hacker » et Eric Freyssinet, auteur de « La cybercriminalité en mouvement ». Le FIC a également été l'occasion pour Manuel Valls, ministre de l'Intérieur, et Fleur Pellerin, ministre déléguée auprès du ministre du Redressement productif, chargée des PME, de l'Innovation et de l'Economie numérique, de procéder à quelques annonces clés. Dans son discours de clôture, Manuel Valls a rappelé la nécessité de développer la coordination entre pays pour mieux répondre à la cybercriminalité organisée, diversifiée et structurée au niveau mondial. Le ministre a également annoncé la création d'un indicateur statistique spécifique à la cybercriminalité, visant à mieux évaluer le niveau réel de la délinquance sur le Web. De son côté, Fleur Pellerin a annoncé la relance du projet d'identité numérique Idénum.

[L'Informaticien] Passeport biométrique : la CNIL s'assure de l'effacement des données surnuméraires

La CNIL s'est assurée de la bonne application de l'arrêté du Conseil d'Etat limitant le nombre d'empreintes conservées lors de la création de passeports numériques à deux, au lieu de huit comme initialement convenu. Selon la CNIL, l'Agence Nationale des Titres Sécurisés (ANTS) effectue bien une sélection automatique des deux meilleures empreintes, les six restantes étant effacées.

[Afnor] L'AFNOR lance une consultation nationale sur une norme de sécurité des TIC

L'AFNOR lance une consultation sur la norme internationale ISO/CEI 27031 en vue de sa reprise à l'échelle nationale. L'Association invite donc toute organisation privée, gouvernementale ou non-gouvernementale concernée à se prononcer sur ce projet de norme française, qui vise à renforcer la sécurité des technologies de l'information et de la communication.

[UsineNouvelle] L'Europe mutualise sa lutte contre la cybercriminalité

Le nouveau centre européen de lutte contre la cybercriminalité, créé sous l'impulsion de la France, a été inauguré vendredi 11 janvier 2013. Cette structure centralisée permettra de répondre plus efficacement aux cybermenaces. Son budget annuel est de 4,6M€. Elle possède une équipe de 40 personnes, dirigée par Troels Oerting, actuel DGA d'Europol. Le centre travaillera sur trois domaines précis : i) les fraudes en ligne, ii) la grande criminalité, iii) la défense des systèmes d'information des pays de l'UE. Parallèlement, une directive sur la cyberdéfense est actuellement à l'étude par la Commission européenne.

[EuObserver] La directive européenne sur le « cyber » bientôt terminée

La Commission européenne devrait prochainement rendre publique une première version de la directive sur la cybersécurité ; un livret de règles harmonisées devrait également être mis en ligne. Le projet de loi, piloté par la commissaire européenne chargée du numérique Neelie Kroes, devrait proposer la création d'un mécanisme de coopération afin de prévenir et de contrer les cyberattaques internationales. La directive doit proposer une nouvelle réglementation de cybersécurité, qui sera appliquée par le nouveau Centre européen de la cybercriminalité, lancé en janvier 2013.

[SecurityAffairs] La Grande-Bretagne recrute des jeunes pour des jeux de cyberguerre

La Grande-Bretagne a récemment annoncé la création d'un programme de recrutement de 100 agents provenant du monde des « jeux vidéo », la « Xbox génération ». Certaines caractéristiques comme un profil jeune, l'absence de parcours universitaire et un intérêt fort pour les réseaux sociaux sont recherchées en priorité. Les nouvelles recrues suivront une formation de deux ans. Le projet illustre les investissements réalisés par la Grande-Bretagne - environ 650M de livres - pour renforcer la cyberdéfense du pays.

[CourierMail] L'Australie et la Grande-Bretagne signent un traité de défense

L'Australie et la Grande-Bretagne ont signé un accord invitant les deux Etats à partager des informations, de la technologie, une politique globale de défense ainsi que du personnel. Au cœur de leurs préoccupations : le changement de nature du conflit en Afghanistan et les contraintes budgétaires. La cybersécurité et les menaces internationales font aussi parti de l'agenda politique des deux pays.

[ArsTechnica] Deux centrales industrielles américaines visées par un logiciel malveillant

Deux centrales industrielles américaines ont été victimes d'attaques sur leurs systèmes de contrôle ; un logiciel malveillant serait la source du bug. Les deux infections ont été réalisées à l'aide de clés USB, et témoignent toujours un peu plus de la fragilité des infrastructures publiques du pays contre de telles attaques.

[Cimsec] Technologies émergentes et guerre navale

Face à l'augmentation des coûts de développement technologique militaire, la Navy envisage l'avenir des équipements maritimes et des techniques de combat. Ainsi, diverses nouvelles technologies et méthodes de combat sont attendues, telles que : le DMO (Distributed Maritime Operations), l'UAS (Unmanned Aerial System), les drones navals, de nouveaux systèmes de communication et de géolocalisation en mer, le développement de canons électriques, ou le renforcement des ressources cyber afin de garantir la protection des systèmes informatiques (notamment de lanceurs de missiles).

[SecurityAffairs] L'utilisation de vagues électromagnétiques sur les réseaux

Des études récentes ont été menées sur l'utilisation de vagues électromagnétiques afin d'interférer avec les systèmes de défense d'un adversaire. Un projet de ce type est né aux Etats-Unis avec l'aide du Laboratoire de recherche pour l'Armée de l'air. Le projet étudié vise à compromettre les systèmes de radar, de télécommunications et de distribution d'énergie ennemis. Dans un rapport publié par Defense News, il était question d'un tel programme étudié et géré par l'Intelligence and Information Warfare Directorate.

[PayVand] La cyber-police iranienne annonce avoir découvert les auteurs du hacking des banques américaines

Le chef de la FETA - la cyber-police iranienne - a annoncé avoir identifié la source de l'attaque contre la banque américaine Citybank, et nie toute implication de l'Iran dans cette affaire. Selon lui, la source ne proviendrait pas du territoire iranien, d'autant plus que des utilisateurs iraniens auraient également été victimes de cette attaque.

[AllVoices] L'Iran met à niveau ses capacités de cyberguerre

Chaque année le gouvernement iranien dépense plusieurs millions de dollars afin d'acquérir de nouvelles capacités militaires ; et chaque année, ces millions lui permettent de disposer d'une cyberdéfense et d'outils toujours plus performants. Selon le Général Ahmad Reza Pourdastan, l'Iran est désormais capable de gêner les communications de ses ennemis ; de plus le pays disposerait désormais de drones afin d'espionner les installations militaires avoisinantes.

[CNet] Un général américain évoque la "cyber-puissance" grandissante de l'Iran

Selon le Général de l'Armée de l'air américaine William Shelton, l'attaque Stuxnet lancée en 2010 contre l'Iran et d'autres pays a permis au

gouvernement iranien de se rendre compte des cybermenaces et de développer, en conséquences, sa cybersécurité. Depuis, l'Iran a été accusé d'avoir récemment orchestré une série de cyberattaques, notamment contre des banques américaines. De leur côté les Etats-Unis veulent renforcer leurs capacités en recrutant 1 000 personnes qui viendraient s'ajouter aux 6 000 déjà employées dans ce domaine.

[SlashDot] Cuba utiliserait un câble Internet sous-marin pour se connecter à Internet

Un changement dans la structure du trafic Internet cubain depuis une semaine conduit certains analystes à penser que Cuba aurait opté pour un câble sous-marin en fibre-optique qui connecterait l'ile à Internet à partir du Venezuela.

[CNet] Le groupe Anonymous intensifie sa cyberguerre contre Israël

Le groupe de hackers Anonymous continue d'intensifier ses cyberattaques contre Israël afin de protester contre les offensives menées dans la bande de Gaza. Anonymous a notamment mis en ligne un document - jugé ancien et non mis à jour - contenant les noms et adresses de personnalités qui participent à la Coalition pour l'Unité d'Israël. Une autre tentative consistait à empêcher les connections à plus de 600 sites Internet israéliens ; elle aurait néanmoins été bloquée par les systèmes de cyberdéfense israéliens.

[JewishNews] Israël : des jeunes entraînés à lutter contre les cybermenaces

Israël annonce la création d'un centre d'excellence de cybersécurité, l'Ashkelon Academic College, dans lequel des centaines de jeunes de 16 à 18 ans seront formés à la cybersécurité. Ce programme vise non seulement à améliorer les capacités israéliennes de cybersécurité et de cyberdéfense, mais participe également à l'intégration socio-économique de jeunes défavorisés dans des secteurs économiques compétitifs.

[CNN] La Corée du Sud recrute les meilleurs hackers pour faire face à la cybercriminalité

La Corée du Sud subirait une grande quantité de cyberattaques, aussi bien sur ses entreprises que sur ses institutions gouvernementales, ciblées notamment par la Corée du Nord. Pour faire face à ces attaques, la Corée du Sud a choisi de former et recruter les meilleurs hackers du pays. Un programme a ainsi créé pour recruter les meilleurs éléments ou les référer aux grandes entreprises coréennes pour assurer leur protection. Plutôt que combattre les hackers, la Corée du Sud fait ainsi le choix de les valoriser.

[Yonhap] La Banque mondiale cherche à établir un centre de cybersécurité en Corée du Sud

La Banque mondiale et la Commission Coréenne des Communications (KCC), organisme en charge de la politique du pays vis-vis d'Internet et des télécommunications, prévoient d'ouvrir conjointement un « Centre mondial de cybersécurité » en Corée du Sud, dont la mission sera de promouvoir la cybersécurité et la protection des informations dans les pays en développement.

[ANSSI] L'ANSSI publie la version finalisée du guide d'hygiène informatique

Patrick Pailloux a, à l'occasion du FIC 2013, annoncé la publication du « Guide d'hygiène informatique » de l'ANSSI. Ebauché en ctobre 2012, la version finale du document recense de nombreuses bonnes pratiques : connaitre le SI et ses utilisateurs, maîtriser le réseau, mettre à niveau les logiciels, authentifier l'utilisateur, sécuriser l'intérieur du réseau, protéger le réseau interne de l'Internet ou encore sensibiliser. L'humain tient une place essentielle dans ces recommandations.

[ANSSI] L'ANSSI publie un référentiel métier de l'architecte référent en sécurité des systèmes d'information

Avec ce document, l'ANSSI souhaite *« définir les compétences de l'architecte référent en sécurité des systèmes d'information, ou « ARSSI », par le biais d'un référentiel métier »*. Egalement annoncé à l'occasion du FIC 2013, le référentiel établit la liste de compétences clés en matière de SSI.

[Parliament] Un rapport britannique analyse la stratégie de cyberdéfense du pays

Un rapport, publié en décembre 2012 par le Comité de Défense de la Chambre des Communes, et qui fait suite à la Stratégie de Sécurité nationale (2010), analyse les implications de la cybersécurité pour la défense du pays. Il recommande le développement d'outils afin de renforcer les capacités militaires de la Grande-Bretagne et, à cette fin, suggère d'utiliser le Programme national de Cybersécurité. Le rapprochement avec le Centre de cyberdéfense de l'OTAN est également salué. Face aux menaces existantes, le Comité encourage à de nouveaux efforts.

[CCDCOE] Les actes de la Cycon 2012 en ligne

Les actes de la conférence du CCDCOE intitulée « Military and Paramilitary Activities in Cyberspace » sont en ligne. Ils portent sur les sujets suivants : le rôle des Etats dans la structure globale d'Internet, Politiques et stratégies dans le cyberespace ; Cyberconflits, théorie et principes ; Cyberconflits : les acteurs ; Cyberattaques : méthodes et classifications ; Cyberdéfense, méthodes et outils.

[Federal News Radio] Le DoD élabore un cadre référentiel pour la cybersécurité

Le Département de la Défense américain élabore un cadre de références dans lequel les compétences cyber apparaissent cruciales et essentielles. Le DoD prépare également un exercice de formation commune avec l'Agence des Systèmes d'Information de Défense et du personnel civil. L'objectif est de former des militaires à des techniques qui dépassent le seul cadre militaire/civil. Ce type d'exercices devrait croître en 2013 et 2014.

[CSMonitor] La cybersécurité comme principal enjeu sécuritaire pour les Etats Unis en 2013

Dans un rapport prévisionnel pour l'année 2013, le Christian Science Monitor fait de la cybersécurité le principal enjeu sécuritaire présenté aux Etats-Unis. Ainsi, les auteurs estiment que les Etats-Unis devront faire face à une recrudescence des attaques par déni de service sur leurs infrastructures clés, notamment les banques, ainsi qu'à un cyberespionnage orchestré par des gouvernements étrangers sur les secteurs de l'énergie, les hydrocarbures et la chimie entre autres. Les auteurs considèrent que les futures forces ou faiblesses des Etats-Unis en termes de cybersécurité dépendront de la volonté du Congrès à voter la première loi sur la cybersécurité et de la portée qui lui sera donnée.

[Epic] Publication d'un guide des bonnes pratiques pour les applications mobiles

Le procureur général de Californie a publié un rapport dans lequel il propose un guide des bonnes pratiques pour assurer la confidentialité des applications mobiles. Celui-ci invite les développeurs d'applications à utiliser le Privacy by Design et à développer une réelle politique de confidentialité. Le rapport s'adresse aussi bien aux développeurs d'applications et de systèmes d'exploitation qu'aux fournisseurs de plateformes d'applications et aux détenteurs de mobiles.

Red October

Une cybermenace « sous-marine »

Le 14 janvier 2013, le fournisseur de solutions de sécurité informatique Kaspersky Lab, annonçait de façon retentissante la découverte de l'opération « Red October » (ou ROCRA), apparemment active depuis mai 2007. Il s'agit d'une attaque de cyberespionnage à grande échelle et d'une ampleur peu commune, qui aurait touché de *nombreuses « représentations diplomatiques, [ainsi que] des administrations, des organismes de recherche scientifique, des groupes énergétiques et nucléaires ou des entreprises dans le secteur du commerce et de l'aéronautique »* dans plusieurs pays.

Ecrit en russe, le logiciel malveillant utilise un code d'exploitation chinois et serait toujours en activité en janvier 2013. Plus précisément, *« le code des attaques [aurait] été élaboré par des hackers chinois et avait déjà été utilisé lors de cyberattaques contre des activistes tibétains. Les modules malveillants auraient quant à eux été créés par des informaticiens russophones »* .

Quelles cibles géographiques ?

De nombreux pays ont pu être infectés durant les cinq années d'activité du logiciel ROCRA et l'étendue des dommages n'est pas encore déterminée. Néanmoins le recensement des attaques effectué par Kaspersky[1] permet de constater que certaines zones géographiques ont été particulièrement touchées par ce phénomène. Si plusieurs centaines d'infections ont été dénombrées, ces dernières ont été particulièrement nombreuses en Europe de l'Est, mais aussi en Amérique du Nord, en Europe de l'Ouest et en Asie Centrale.

Pays les plus touchés par les infections de ROCRA [*à partir d'au moins 5 infections*][2] :

1. La Fédération de Russie – 35 infections
2. Le Kazakhstan – 21 infections
3. L'Azerbaïdjan – 15 infections
4. La Belgique – 15 infections
5. L'Inde – 14 infections
6. L'Afghanistan – 10 infections
7. L'Arménie – 10 infections

[1] Plusieurs articles reprennent une carte dessinée par la société Kaspersky Lab sur laquelle il est aisé de voir les victimes de l'attaque. Voir notamment : http://www.washingtonpost.com/wp-srv/politics/images/Red_October_Infographic_3_1.png

[2] SecureList, http://www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies

8. L'Iran – 7 infections

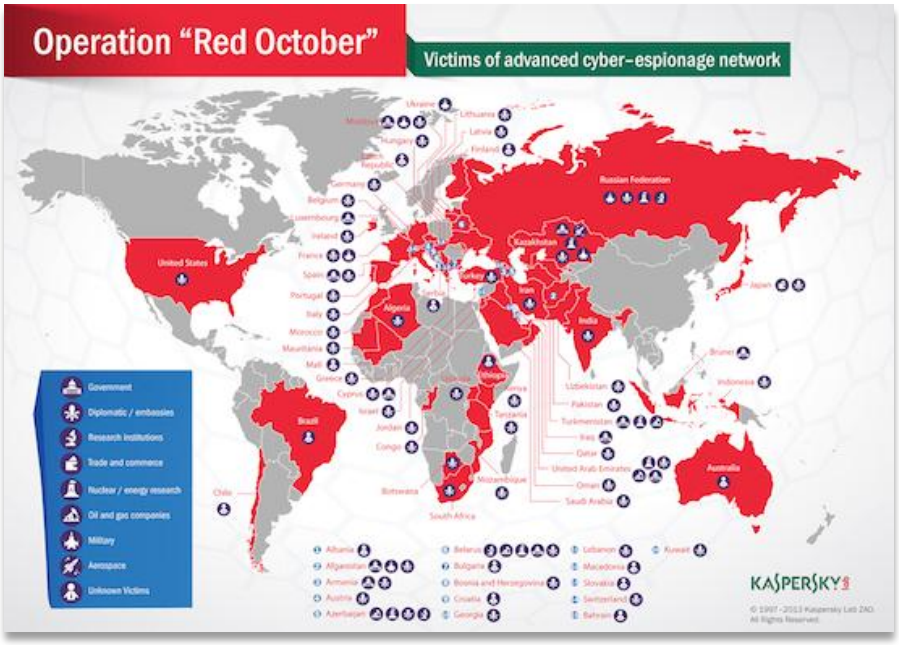
9. Le Turkménistan – 7 infections

10. L'Ukraine – 6 infections

[La France a reçu moins de 5 infections]

Quelle origine ?

Au total 39 pays auraient été touchés, dont la France, qui aurait néanmoins reçu moins de 5 infections. Il est à noter que l'Iran, la Russie ou encore les Etats-Unis ont chacun reçu des attaques et été infectés par ROCRA. Ce qui, selon certains analystes, exclurait de fait la responsabilité de ces Etats dans l'élaboration de l'opération Octobre Rouge. A moins, cependant, et dans le cas où l'origine de ces attaques proviendrait d'un Etat, que l'une des victimes se soit volontairement infectée afin d'éloigner des soupçons qui auraient pu, autrement, naître sur sa responsabilité.



Quel mode opératoire ?

« *De toute évidence, les informations volées par les hackers sont de la plus haute importance et incluent des données géopolitiques pouvant être utilisées par des Etats* », estime Kaspersky[3]. Le schéma opérationnel de ROCRA, simplifié, est le suivant : il est envoyé la plupart du temps par courriel à des personnes qui sont ciblées au sein des structures publiques ou privées énumérées ci-dessus (« *représentations diplomatiques,*

[3] Sos Ordi, « Octobre Rouge : quand Kaspersky dévoile un réseau de cyber-espionnage en sous-marin depuis plus de 5 ans », http://www.sosordi.eu/News/1068-3-octobre-rouge-quand-kaspersky-devoile-reseau-cyber-espionnage-sous-marin-depuis-plus-ans

[ainsi que] *des administrations, des organismes de recherche scientifique, des groupes énergétiques et nucléaires ou des entreprises dans le secteur du commerce et de l'aéronautique* »[4]).

Puis, il déchiffre les informations trouvées, avant de se connecter à un serveur à distance et, « *dans l'attente de nouvelles commandes ou téléchargements,* [d'exécuter] *alors des transferts illicites de données* »[5]. Les données volées sont jugées extrêmement sensibles, puisque selon Roel Schouwenberg – un chercheur de Kaspersky Lab – ROCRA aurait détourné des codes d'accès, des documents confidentiels, des dossiers encryptés, des clés de décryptage ainsi que des fichiers élaborés avec le logiciel *Acid Cryptofiler*, employé par l'Union européenne et l'OTAN[6].

Le fonctionnement en sous-marin de ROCRA :

Le logiciel malveillant possède un système de lecture de la disposition des réseaux informatiques infiltrés, et peut enregistrer la configuration des routeurs, ce qui lui donne la possibilité de soustraire des dossiers depuis des terminaux mobiles (Windows, iPhone, Nokia). Il réalise également des captures d'écran, et peut récupérer des fichiers effacés.

Selon les analystes de Kaspersky Lab, des données sont toujours envoyées par les terminaux infectés à de nombreux serveurs. En effet les hackers ont créé environ soixante noms de domaine – pour la majorité en Allemagne et en Russie – afin de contrôler les terminaux infectés. De plus, « *le système mis en œuvre combine des tâches persistantes (enregistrement des frappes du clavier, attente de connexion d'un appareil pour l'infecter à son tour, etc.) et des tâches ponctuelles (extraction de mots de passe, exécution de codes, etc.)* ».

Enfin, l'étude de cette attaque démontre l'exploitation par ROCRA des failles Windows : l'une d'elles concernerait le logiciel Excel puisque des cyberattaques auraient été recensées dessus entre 2010 et 2011 ; une autre impliquerait le logiciel de traitement de texte Word[7]. Il y a quelques jours, des chercheurs ont découvert que le logiciel malveillant utilisait également les failles Java[8].

Une finalité encore incertaine

La véritable originalité de Red october reste sa cible. Totalement désintéressé des informations pouvant usuellement être convoitées par les virus plus classiques, Red October subtilisait des documents politiques, diplomatiques, des études stratégiques et géoéconomiques, etc. Selon Ouran Parfentiev, analyste du Centre régional des technologies internet de Kaspersky Lab, *« il n'est pas à exclure qu'une partie des informations obtenues de cette manière, ait été publiée sur WikiLeaks, par exemple ».*

[4] RP Defense, http://rpdefense.over-blog.com/categorie-11791082.html, consulté le 22 janvier 2013
[5] IT One, http://www.itone.lu/article/red-october-noobies
[6] Washington Post, http://www.washingtonpost.com/world/national-security/computer-malware-targets-europe-agencies/2013/01/14/a8cf2d5c-5c09-11e2-beee-6e38f5215402_story.html
[7] Sos Ordi, *op. cit.*
[8] PCWorld, http://www.pcworld.com/article/2025328/red-october-malware-discovered-after-years-of-stealing-data-in-the-wild.html

Le portail OMC
La nouvelle plateforme de la DAS

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

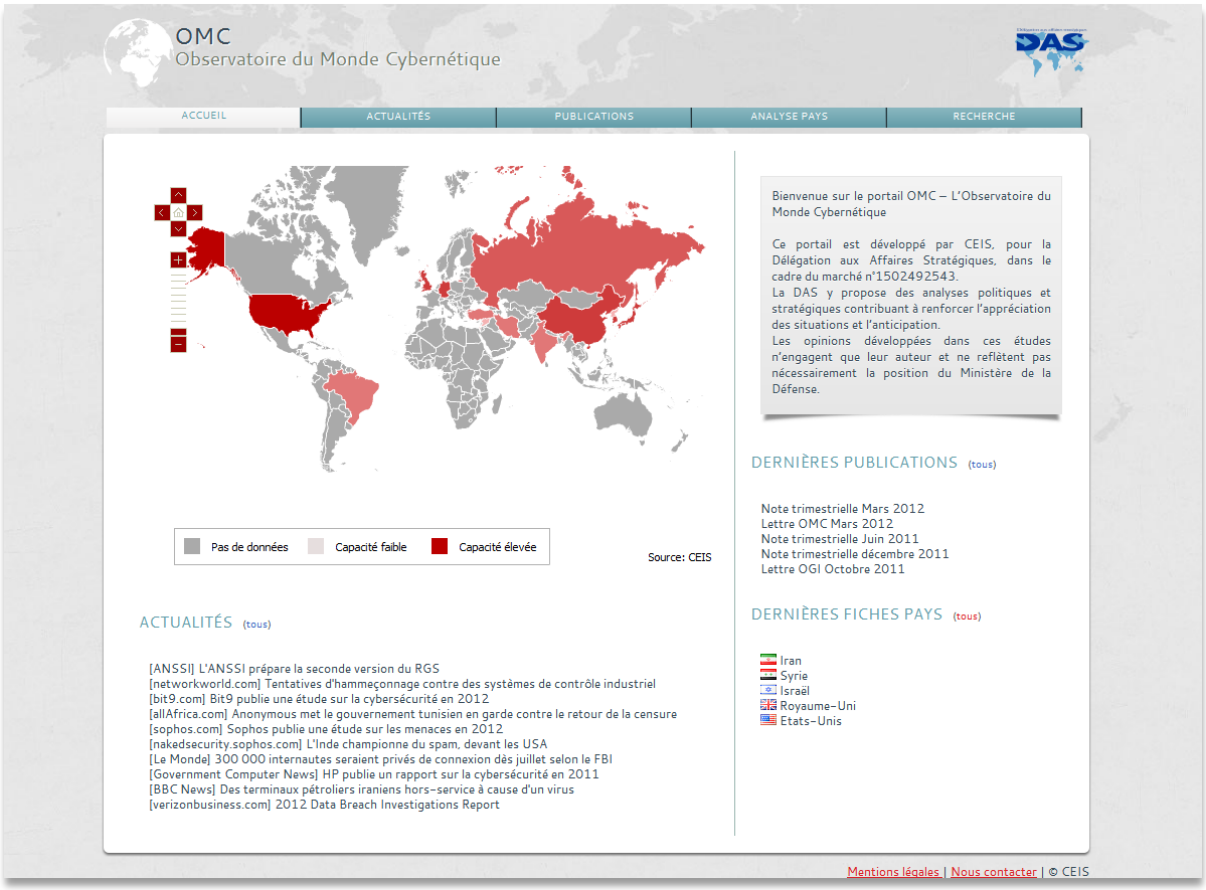


Figure 1. Page d'accueil du portail OMC - https://omc.ceis.eu/

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

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

Cyber Defence & Network Security 2013	Londres	28 – 31 janvier
Information Security Day	Luxembourg	6 – 7 février
Reboot Annual Privacy and Security Conference	Vancouver	15 – 17 février
SANS Security Belgium	Bruxelles	18 – 23 février
Cyber Security Implementation Workshop	Savannah, Etats-Unis	19 – 21 février
Nullcon Goa	Goa, Inde	27 février – 2 mars
International IT Conference	Abou Dhabi	31 Mars – 1er avril
Cyber Africa 2013	Accra, Ghana	mai
SSTIC 2013	Rennes	5 – 7 juin
International Symposium on Engineering Securse Software and Systems	Paris	27 février – 1er mars
GS Days	Paris	4 avril
ACM Workshop on Information Hiding and Multimedia Security	Montpellier	17 – 19 juin
Hack in Paris	Paris	17 – 21 juin
La Nuit du Hack	Marne La Vallée	22 – 23 juin
Les Assises de la Sécurité et des Systèmes d'Information	Monaco	2 – 5 octobre

CEIS

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