Observatoire du Monde Cybernétique

Lettre n°21 – Septembre 2013

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

[InfoDéfense] Premier colloque des réservistes citoyens de la cyberdéfense française

Organisé conjointement avec l'IRSEM et la DAS à l'Ecole Militaire, le premier symposium académique national de recherche en cyberdéfense a eu lieu le 18 septembre 2013. Cette rencontre avait pour objectif de réunir les acteurs, nourrir le débat et ouvrir la réflexion sur la cyberdéfense incluant aussi bien les thèmes de la stratégie, des sciences humaines et sociales, du droit ainsi que des relations internationales.

[Le Figaro] Arnaud Montebourg et Fleur Pellerin visitent les locaux de Cassidian

Lundi 16 septembre 2013, Arnaud Montebourg, ministre du Redressement productif, et la ministre déléguée à l'Économie numérique, Fleur Pellerin, ont visité les locaux de Cassidian à Élancourt où 2000 ingénieurs travaillent sur des projets liés à la défense, la sécurité et la cybersécurité. Point d'orgue de la visite, une démonstration d'intrusion informatique et le déclenchement des moyens pour la détecter, l'observer et la neutraliser.

[LMI] France : le numérique – et la cybersécurité – pour réindustrialiser le pays

François Hollande a présenté le 12 septembre 2013 ses plans pour réindustrialiser la France. Le projet, baptisé « Nouvelle France Industrielle », s'articule autour de 3 axes : la transition énergétique, l'économie du vivant et les nouvelles technologies. Le numérique obtient une place de choix avec près de 14 projets liés aux nouvelles technologies. Parmi ces plans d'actions, on retrouve les sujets inclus dans les investissements d'avenir au sein du FSN (fonds pour la société du numérique à hauteur de 150 millions), l'Internet des objets, le big data, le cloud, le calcul intensif et enfin la cybersécurité.

[France3] La Bretagne au cœur de la cyberdéfense française

L'université de Bretagne Sud a ouvert à Vannes une formation spécialisée en cyberdéfense, pour former en alternance des ingénieurs dont le profil intéressera aussi bien le monde civil que militaire. Cette formation unique en France vient confirmer l'orientation vers l'ouest de la cyberdéfense française, puisque plusieurs centres s'y trouvent, dont la DGA Maîtrise de l'Information près de Rennes, qui a annoncé un doublement d'effectif d'ici 2017.

[LExpansion] Cybersécurité : les ministres interdits de smartphones

L'Express s'est procuré une note de Jean-Marc Ayrault adressée à tous les ministères, dans laquelle il leur est suggéré d'abandonner leurs smartphones et tablettes grands publics pour les communications sensibles, par souci de confidentialité. Il leur est conseillé de se tourner vers des terminaux sécurisés (notamment ceux proposés par Thales), ou d'installer des outils de sécurisation validés sur leurs smartphones actuels. Cette note vient en réponse aux multiples affaires d'espionnage récemment révélées.

[Wired] Le FBI a hacké des serveurs situés en France pour diffuser un spyware

Le FBI a admis avoir secrètement pris le contrôle de Freedom Hosting en juillet dernier, afin d'y implanter un spyware. Freedom Hosting héberge en France des pages web destinées au réseau d'anonymisation Tor. Le FBI souhaitait ainsi démanteler une filière d'utilisateurs de sites pédophiles. L'agence fédérale exploitait une faille dans Firefox intégrée au Tor Browser Bundle. Elle lui permettait de capturer l'adresse MAC des visiteurs du site et ainsi les identifier. TorMail fait partie des services contaminés.

[Slate] Vupen, « l'entreprise française qui bosse pour la NSA »

La société française Vupen a signé un contrat d'un an avec la NSA, offrant à l'agence un accès total à se base d'exploits. Bien que la NSA affirme ne se servir de ces failles qu'à des fins défensives, beaucoup sont convaincus que l'agence s'en sert de manière offensive, pour obtenir l'accès à des réseaux étrangers. Les régulateurs européens

prévoient d'établir des restrictions sur ce type de contrats.

[Le Figaro] La traque des cyber-djihadistes s'intensifie

Un fondamentaliste a été écroué pour apologie et provocation au terrorisme sur Internet. La DCRI, avec le Parquet de Paris, ont lancé une traque contre ceux qui utilisent la Toile pour diffuser ces idées.

[Reuters] La France veut réguler les géants du Web

Fleur Pellerin a appelé l'Union européenne a réguler les géants de l'Internet (Google, Facebook, etc) afin de limiter leur monopole sur le commerce et les services en ligne.

[DhNet] Belgique : 20 M€ seront nécessaires pour mettre en œuvre une stratégie de cybersécurité

Selon le secrétaire d'Etat à la Fonction publique belge, Hendrik Bogaert, 20 M€ seront nécessaires pour mettre en œuvre la stratégie de cybersécurité du gouvernement fédéral adoptée en décembre 2012. Cette somme pourrait être répartie sur 4 ans.

[Le Monde] Belgacom dépose une plainte après l'intrusion de ses systèmes par la NSA

L'opérateur téléphonique belge Belgacom, acteur majeur des télécommunications en Afrique et au Proche-Orient, a déposé une plainte pour accès non autorisé à son système informatique interne. Les intrusions, très techniques, semblent avoir eu pour but d'intercepter des communications. La NSA est soupçonnée par le gouvernement belge.

[Yle] Le chef du renseignement européen appelle à plus de moyens pour lutter contre la cybercriminalité

Parlant de la situation en Finlande, le chef du centre de renseignement de l'UE a affirmé que plus de pouvoir devrait être donné aux autorités pour lutter efficacement contre la cybercriminalité.

[IIPDigital] Sécurité : des ministres européens et hauts responsables américains renforcent la coopération

Le secrétaire à la sécurité intérieure des États-Unis, Rand Beers, a rencontré ses homologues du Groupe des six (G6) les 12 et 13 septembre, pour discuter des efforts transatlantiques relatifs à plusieurs enjeux dont la cybersécurité.

[Livemint] L'Inde et le Royaume-Uni vont collaborer sur la cybersécurité

Le Royaume-Uni a annoncé son intention d'ouvrir un CERT avant la fin de l'année 2013. Ce CERT-UK travaillera en collaboration étroite avec le CERT indien (CERT-IN).

[The Hill] Etats-Unis : le Sénat prépare CISPA 2

La commission du renseignement du Sénat américain est en train de préparer une nouvelle loi qui serait l'équivalent du CISPA cybersecurity bill, afin d'encourager le partage d'informations entre les entreprises et l'administration fédérale.

[TheDailyDot] Une possible intrusion de la NSA dans le réseau Bitcoin

Suite aux multiples révélations sur la surveillance opérée par la NSA, beaucoup ont craint que Bitcoin fasse l'objet d'une surveillance particulière en raison des suspicions d'autres agences américaines (notamment le FBI) sur l'usage de cette crypto-monnaie. Une altération des procédés cryptographiques de Bitcoin est peu probable, mais la NSA et le FBI auraient déjà déployé un filtre permettant de suivre plusieurs types d'échanges frauduleux. Ces suspicions sont renforcées par le fait que l'algorithme employé par Bitcoin (SHA-256) a été créé par la NSA.

[RTNews] L'Argentine et le Brésil nouent une alliance de cyberdéfense contre l'espionnage américain

Les ministères de la Défense d'Argentine et du Brésil ont noué une alliance pour améliorer mutuellement leurs capacités de cyberdéfense, suite aux révélations sur l'espionnage des Etats-

Unis en direction des pays d'Amérique latine. Un sommet bilatéral de cybersécurité sera tenu avant la fin de l'année 2013, et le Brésil formera en 2014 des officiers argentins à la cyberdéfense.

[Channel News Asia] L'ASEAN salue la création d'un groupe pour lutter contre la cybercriminalité à Singapour

La neuvième rencontre ministérielle de l'ASEAN sur le crime transnational a salué la création à Singapour d'un groupe de travail luttant contre le cybercrime. Ils ont déclaré que cela fournirait une plateforme de discussion régionale pour discuter d'une stratégie contre la cybercriminalité.

[RTNews] La Chine pourrait lever la censure d'Internet au sein d'une nouvelle zone de libre échange

Afin de mieux servir les investisseurs étrangers au sein de la prochaine zone de libre-échange à Shanghai, les autorités chinoises envisagent d'y lever la censure sur les réseaux sociaux et les sites de presse internationale. La Zone de Libre-Echange de Shanghai, qui ouvrira le 29 septembre 2013, deviendrait ainsi un refuge de liberté sur Internet.

[Gulf Daily News] Le Parlement du Bahreïn examine une loi sur la cybercriminalité

Le Parlement du Bahreïn est en train d'examiner un projet de loi sur la cybercriminalité renforçant les peines en cas de mauvais usage de sites Internet et des réseaux sociaux.

[AllAfrica] Nigeria : 3ème Conférence Mondiale sur la Cybersécurité

700 participants étaient attendus le 17 septembre au Nigeria pour la 3ème conférence mondiale sur la cybersécurité, en tête desquels figurent la première dame nigériane Patience Jonathan et l'ancien premier ministre israélien Ehud Barak. Des représentants de l'UIT et de la Banque Centrale Nigériane étaient également présents.

[All Africa] Tanzanie : une loi sur la cybercriminalité en préparation

La Banque de Tanzanie est en train de travailler avec le gouvernement à la préparation d'une nouvelle loi pour créer un cadre légal pour les transactions financières électroniques et pour mieux lutter contre la cybercriminalité.

[BBCNews] L'explosion des connexions sur Tor serait causée par des cybercriminels

Depuis le mois d'août, le réseau Tor constate un bond considérable dans le nombre de ses connexions quotidiennes, passant de 500 000 à 1,5 M en une semaine, et jusqu'à 3 M aujourd'hui. Alors que les premières suppositions faisaient état de connexions de citoyens d'Etats censurant Internet, plusieurs analyses viennent plutôt avancer l'idée de cybercriminels exploitant Tor pour contrôler un large botnet.

[ArabianBusiness] Ouverture du premier Centre de Cyberdéfense du Moyen-Orient

Le premier centre de cyberdéfense du Moyen-Orient a ouvert, à Dubaï. Développé par McAfee, sa mission sera de centraliser des informations sur de potentielles menaces, leurs origines et leurs motivations, mais également toutes les données pouvant aider les gouvernements, institutions et entreprises à anticiper et répondre aux cyberattaques.

[Out-Law] Directive NIS : problème de clarté des définitions

Un rapport du Parlement européen a mis en évidence le manque de clarté de la directive NIS quant aux définitions de la cybersécurité et des termes associés, ce qui poserait problème aux entreprises qui y sont soumises.

[CSIS] Les capacités cyber offensives sur le plan opérationnel

Le Centre d'Etudes Stratégiques et Internationales (CSIS) a publié une étude intitulée « Offensive Cyber Capabilities at the Operational Level: The Way Ahead », dans laquelle est envisagé l'avenir des opérations cyber offensives de l'armée américaine. Ses auteurs ont souhaité déplacer la réflexion des approches défensives vers une meilleure exploitation des capacités cyber à des fins offensives, et se sont interrogés sur la nécessité pour la Défense américaine d'y consacrer un effort plus important.

[VirtualStrategyMagazine] Une étude montre que les cyberattaques changent selon le secteur visé

Une étude menée par la société Proofpoint révèle que le volume des cybermenaces change selon les secteurs visés. Ceux les plus communément associés aux cyberattaques (gouvernements, banques et haute technologie) sont en fait moins menacés que les secteurs moins envisagés (pharmaceutiques, commerce, logement et assurances). Cependant, les premiers secteurs nommés sont davantage la cible d'attaques concentrées.

[Bloomberg] La cybercriminalité russe est-elle vraiment en baisse ?

Un rapport de la société Group-IB fait état d'une réduction de 11% de la taille du marché de la cybercriminalité russe entre 2011 et 2012, passant de 1,19 milliard de dollars à 1,07 milliard. Malgré la position privilégiée de cette société en Russie, ses chiffres nourrissent des doutes, puisqu'ils conforteraient Group-IB dans son travail avec la police russe.

[SydneyMorningHerald] L'Australie est le relais principal des cyberattaques vers l'Asie

Alors que la cybercriminalité opère un glissement d'ouest en est, l'Australie devient un carrefour d'opérations majeur pour les pirates. Un rapport constate qu'en 2013, 32% des attaques ciblées ont impliqué des serveurs australiens. Les ordinateurs australiens infectés servent ainsi d'intermédiaire « sécurisé » entre le pirate et sa cible asiatique. Ce chiffre place l'Australie en tête, suivie de la Corée du Sud (15%) et l'Allemagne (9%).

L'ENISA publie son rapport sur les incidents de l'année 2012

Le 20 août 2013, l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) publiait son rapport annuel sur les incidents majeurs survenus en 2012[1]. L'ENISA a pour missions d'assurer un niveau élevé de sécurité des réseaux et systèmes d'information, de favoriser l'échange de bonnes pratiques et de faciliter les contacts entre les institutions et les entreprises. Elle intervient en tant qu'experte auprès des autorités nationales et des institutions de l'Union européenne. Acteur incontournable, l'ENISA a vu, en juin dernier, son mandat prolongé de sept ans et ses devoirs renforcés, quelques mois après la publication par l'Union européenne de sa stratégie pour la cybersécurité[2].

L'objet de ce rapport annuel est de présenter les **incidents majeurs dans le domaine de la cybersécurité** qui ont émaillé l'année 2012, leur impact et leur origine. Ces rapports annuels sont généralement suivis de recommandations à destination des autorités nationales afin qu'elles renforcent la cybersécurité des infrastructures concernées.

Un système européen de notification

Le rapport annuel publié par l'ENISA est le fruit d'un **mécanisme européen de notification** issu de la réforme du cadre légal pour les communications électroniques de 2009 (Paquet télécom 2009) qui a introduit l'article 13a sur la sécurité et l'intégrité des réseaux et services publics de communication électronique. Cet article établit un système de notification : les fournisseurs de services ou administrateurs de réseaux doivent notifier les failles majeures de sécurité à leur autorité nationale qui doit alors en informer l'ENISA. Si celles-ci affectent plusieurs Etats membres, l'autorité nationale compétente devra les signaler aux autres agences nationales. De plus, chaque année, les autorités nationales doivent présenter un rapport à l'ENISA et à la Commission européenne sur ces incidents. Afin d'assurer une harmonisation des notifications, le Groupe d'experts 13a, composé de représentants des autorités nationales compétentes, a publié un guide de notification[3] et en 2012 l'ENISA a développé une téléprocédure (appelé CIRAS) visant à permettre aux autorités nationales de remplir plus facilement leurs obligations.

Seules les **atteintes à l'intégrité des réseaux et systèmes d'information les plus graves** devront être communiquées aux autorités nationales de régulation. L'ENISA a ainsi établi des critères pour permettre aux fournisseurs de service de déterminer s'ils se trouvent dans une situation les obligeant à informer les autorités de l'incident. Ceci implique donc que le rapport annuel ne constitue pas une analyse exhaustive de tous les interruptions des communications électroniques et ne permet pas d'avoir une vue globale de celles-ci. De plus, tous les secteurs ne sont pas soumis à cette obligation de notification, seuls les incidents

[1] ENISA, *Annual Incident Reports 2012. Analysis of Article 13a annual incident reports*, août 2013, 25 p., disponible sur http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2012

[2] UE, *Cybersecurity Strategy of the European Union : An Open, Safe and Secure Cyberspace*, 7 février 2013, disponible sur http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

[3] ENISA, *Technical Guideline on Incident Reporting in Article 13a*, version 2.0, janvier 2013, 16 p., disponible sur https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/technical-guideline-on-incident-reporting-v-2-0

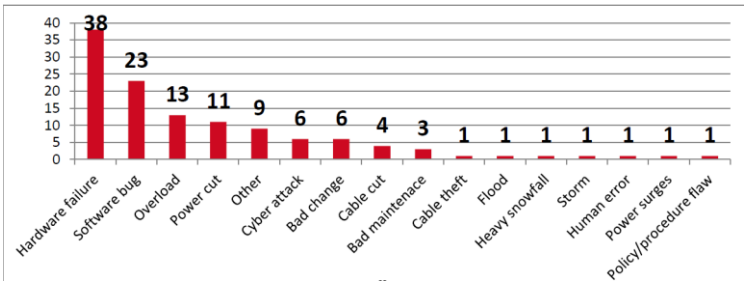
concernant la téléphonie mobile et fixe et les accès à Internet devant être signalés. Afin de les analyser au mieux, cinq causes d'interruption ont été distinguées : les phénomènes naturels, les erreurs humaines, les attaques malveillantes, les pannes des systèmes et réseaux et enfin les pannes dues à des tiers.

Analyse des incidents de l'année 2012

Dans le présent rapport, l'ENISA analyse **79 notifications d'incidents** caractérisés par une interruption des réseaux de communication électronique ou des services et qui ont eu lieu dans 18 Etats membres, neuf Etats n'ayant rapporté aucune interruption majeure et un seul n'ayant pas remis son rapport annuel. Parmi ceux qui ont été étudiés, on peut citer une tentative de vol de câbles qui a entraîné la suspension du réseau téléphonique et d'Internet pour 160 000 utilisateurs pendant 10h ou encore une série d'attaques par dénis de service distribués qui a affecté l'Internet mobile, entraînant une suspension du réseau pour 2.5 millions d'utilisateurs pendant quelques heures.

La plupart des incidents (48%) ont concerné la téléphonie ou l'Internet mobile, ce qui suggère une fragilité particulière de ces réseaux. Ce constat avait déjà été fait l'année dernière. C'est également en cas de panne de l'Internet mobile que le nombre d'utilisateurs touché est le plus important. Un point préoccupant devrait faire l'objet d'une recommandation : l'impact des pannes sur les appels d'urgence. En effet, près de 37% des incidents ont eu un effet sur les appels d'urgence à savoir l'impossibilité pour les utilisateurs d'utiliser le 112 pour appeler les secours. Il est donc impératif que ce chiffre, en augmentation par rapport à l'année 2011, diminue afin de ne pas perturber les services de secours et de limiter les risques d'atteinte à la vie humaine.

Quant aux origines des interruptions des communications électroniques, elles sont dues à 76% à des pannes des systèmes qui, cependant, sont rapidement réparées. Les composants les plus vulnérables sont les commutateurs et les registres des abonnés des opérateurs, ce qui implique là aussi des efforts particuliers à fournir en matière de résilience et de protection des infrastructures et réseaux. En revanche, dès lors qu'elles sont causées par un phénomène naturel, la durée de rétablissement du réseau est beaucoup plus longue. Le tableau suivant détaille les causes des incidents.



ENISA, *Annual Incident Reports 2012. Analysis of Article 13a annual incident reports, op. cit.*, p.13

Ce rapport se veut comme un outil à destination des institutions européennes et des Etats afin de déterminer quelles sont les mesures à prendre et quels sont les services qui devraient faire l'objet d'actions prioritaires. Christoffer KARSBERG, expert à l'ENISA, s'est félicité du peu d'incidents majeurs rapportés le document, tout en reconnaissant que les seuils établis masquaient un certain nombre d'interruptions. C'est pourquoi un débat quant à la révision de ces derniers va être engagé entre les différents acteurs, l'objectif étant d'avoir, dans quelques années, un aperçu plus précis de la situation[4].

[4] Ulf BERGSTROM, "Interview regarding the Annual major cyber incidents 2012 report according to Art 13a", ENISA, 21 août 2013, p. 4, disponible sur http://www.enisa.europa.eu/media/press-releases/chris-interview-2012-cyber-security-incidents-report

KIMSUKY

La Corée du Sud prise pour cible

Kaspersky Labs a mené à partir d'avril 2013 une enquête de plusieurs mois sur une campagne de cyberespionnage ayant ciblé des think tanks sud-coréens. Baptisée « Kimsuky », cette APT a très rapidement fait l'objet de spéculations dénuées de véritables doutes sur une implication nord-coréenne. Dans le flot de malwares quotidiennement observé, l'attention des chercheurs a été captée par des détails surprenants, quand bien même le malware initial ne présentait aucune particularité notable. Parmi ces éléments de surprise figurent le recours à un serveur mail enregistré en Bulgarie et la présence d'idéogrammes coréens dans un code de cheminement. Il aura fallu moins d'un mois aux chercheurs pour repérer le premier malware associé à cette campagne, et ensuite l'observer plusieurs mois durant.

Des cibles stratégiques, clairement définies

Une des particularités de cette campagne est sa précision. 11 entités seulement ont visiblement été ciblées, dont 9 basées en Corée du Sud et 2 en Chine – tous des think tanks ou organisations stratégiques. Au rang de ceux-ci figurent le Sejong Institute, le Korea Institute For Defense Analyses (KIDA), le Ministry of Unification, la Hyundai Merchant Marine, mais également plusieurs ordinateurs appartenant au mouvement des supporters de l'unification coréenne.

L'intention des attaquants ne fait aucun doute, puisque leur attaque a été construite sur mesure pour leurs cibles sud-coréennes, selon des procédés particuliers.

Un mode opératoire sur mesure

En raison du degré de précision de cette campagne, les chercheurs de Kaspersky Labs n'ont pas été en mesure d'identifier la méthode de distribution du malware. Cependant, des indices leur laisse à penser qu'une campagne basique de spear-phishing aurait été utilisée. Un premier fichier introduit dans le système visé se chargeait d'en télécharger un second, ouvrant cette fois l'ordinateur au malware Kimsuky.

Une fois installé dans les fichiers temporaires, puis dans le dossier *System32*, le malware lançait plusieurs services, notamment un, essentiel, destiné à amasser des informations sur l'ordinateur infecté. Peu de programmes ont été impliqués dans l'attaque, mais chacun répondait à une fonction d'espionnage unique, ce qui a surpris les chercheurs de Kaspersky Labs. Parmi ces fonctions figurent un enregistreur de frappes, un listing des dossiers et de leur contenu, le vol de documents HWP (équivalent sud-coréen de Microsoft Word) et également le téléchargement et l'exécution à distance des pièces jointes de mails reçus (la sélection entre les documents se faisant par un système de tags).

L'analyse de cette campagne s'est trouvée renforcée par un constat confirmant la précision du ciblage des attaquants : le malware réussissait au démarrage du système à désactiver le firewall Windows (ainsi que le Security center), mais surtout les firewalls AhnLab (fournisseur sud-coréen, choisi en connaissance cause en raison de son déploiement au sein des organisations ciblées). Enfin, la communication des documents identifiés se faisait via un serveur mail bulgare, par une série d'adresses communicantes et s'authentifiant mutuellement.

Kimsuky et la Corée du Nord

Source : http://www.securelist.com/en/analysis/204792305/The_Kimsuky_Operation_A_North_Korean_APT

Bien qu'il n'y ait aucune preuve irréfutable, les liens avec Corée du Nord semblent s'établir d'eux-mêmes, en raison du choix très précis des cibles et de leurs profils stratégiques, mais également de la double-occurrence du nom Kim dans les comptes mails à l'origine de l'attaque. Les adresses IP fournissent cependant davantage d'éléments, puisqu'elles ont été retracées en Chine, dans les provinces de Jilin et Liaoning, très proches de la Corée du Nord. Les chercheurs de Kaspersky Labs n'ont pas souhaité affirmer de manière péremptoire l'origine nord-coréenne de cette campagne, ce qui n'a pas empêché plusieurs observateurs de l'assurer sans nuance[5].

Le fait que les attaquants aient ciblé les produits de sécurité AhnLab n'est pas anodin, puisque par le passé les régulateurs sud-coréens ont vivement critiqué des victimes de malware pour avoir eu recours à des solutions de sécurité étrangères. En conséquence, de nombreuses organisations se sont tournées vers les produits nationaux AhnLab, devenant paradoxalement vulnérables aux attaques ciblées sur la Corée du Sud, telles que Kimsuky.

[5] [InfoSecurity] Kimsuky - an active North Korean campaign targeting South Korea.

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

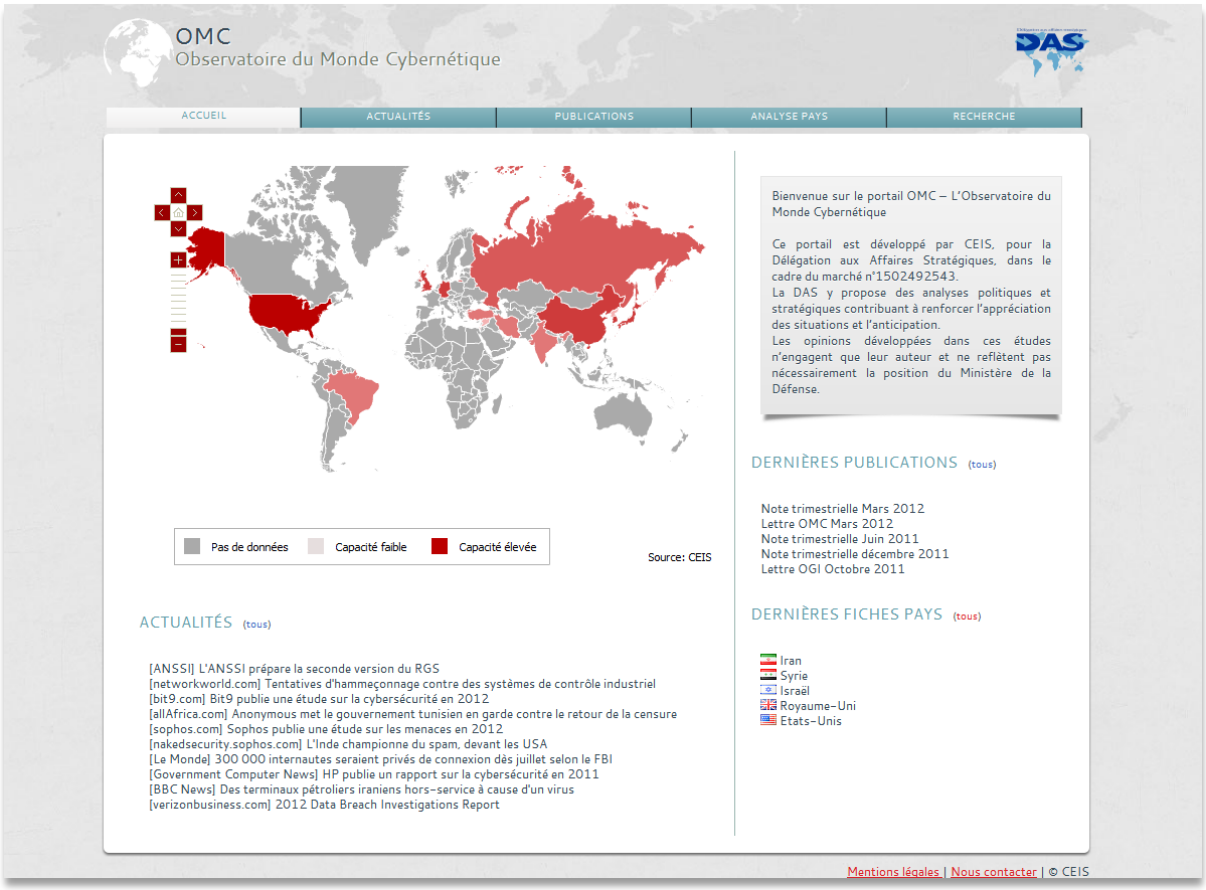


Figure 1. Page d'accueil du portail OMC - https://omc.ceis.eu/

L'accès au portail est réservé aux organisations publiques.

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

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

Mois de la Cybersécurité	Europe	Octobre
United Nations Security Council Conference on Cybersecurity	Baku, Azerbaïdjan	Octobre
Petit-déjeuner européen du FIC / Mois de la cybersécurité (EN)	Bruxelles, Belgique	15 octobre
Cyber Security Summit	Minneapolis, Etats-Unis	22-23 octobre
ICS Cyber Security Conference	Atlanta, Etats-Unis	21-24 octobre
API Cybersecurity Conference & Expo	Houston, Etats-Unis	12-13 novembre
Oil and Gas Cybersecurity Conference	Londres, Royaume-Uni	
19th Azerbaijan International Telecommunications and Information Technologies Exhibition and Conference	Baku, Azerbaïdjan	25 novembre
ASE Cyber Security Conference	Orlando, Etats-Unis	2-5 décembre

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