Observatoire du Monde Cybernétique

Lettre n°28 – Mai 2014

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

[Europol] Blackshades : opération d'envergure mondiale contre les cybercriminels

Europol et Interpol ont annoncé, le 19 mai, l'interpellation de 100 personnes - dont 26 en France selon le parquet de Paris - dans le cadre d'une opération visant le *malware* Blackshades. Ont participé à l'opération les Pays-Bas, la Belgique, la France, l'Allemagne, le Royaume-Uni, l'Italie, le Canada, le Chili et la Suisse.

Blackshades est un logiciel malveillant permettant de prendre le contrôle à distance de l'ordinateur de la victime. Objectif : collecter les données s'y trouvant, transformer l'ordinateur en "zombie" afin de constituer un botnet, ou chiffrer certains dossiers du disque dur.

[Usine-Digitale] Nouveau plan de l'ANSSI pour développer l'offre française de cybersécurité

L'ANSSI a dévoilé quelques-unes des mesures de son nouveau plan cybersécurité, dont l'objectif est de développer le marché français à hauteur de 20% par an et d'accroître de 30% les exportations des entreprises françaises de ce secteur.

Le plan prévoit en outre la création d'un label France, et d'un second appel à projets afin de financer le développement de nouveaux produits et services de cybersécurité français. Est également prévue la création d'un forum d'industriels ayant un rôle de veille sur les appels d'offres internationaux et de partage des bonnes pratiques.

[SC Magazine] Piratage d'eBay : les autorités européennes de protection de données lancent des investigations

Les autorités européennes de protection de données ont décidé d'investiguer les conséquences du piratage d'eBay qui eut lieu le 21 mai dernier [eBay]. Cette intrusion aurait mis en danger les données de plus de 145 millions d'utilisateurs dans le monde.

[ComputerWeekly] Le gouvernement britannique publiera en juin un manuel de cybersécurité destiné aux entreprises

Le gouvernement du Royaume-Uni publiera, le 5 juin prochain, un manuel d'orientation et de certification en cybersecurité nommé *« Cyber Essential Scheme »*. Ce document spécifiera des standards de cybersécurité et les étapes à suivre pour les atteindre. L'objectif est que les entreprises puissent comparer leurs niveaux d'hygiène informatique et de cybersécurité avec ce que le gouvernement considère comme acceptable.

[Tbray] Selon l'IETF, "la surveillance de masse est une attaque contre Internet"

Au vu des révélations sur les programmes de surveillance à grande échelle utilisés par les Etats-Unis et le Royaume-Uni, l'*Internet Engineering Task Force (IETF)* a acté le fait qu'il s'agissait « d'une attaque contre Internet ». L'IETF estime donc qu'il faut y opposer une réponse technique [RFC 7258], de même qu'une réaction au niveau politique. L'idée n'est pas de rendre la surveillance impossible, mais de faire en sorte que cette dernière devienne suffisamment coûteuse pour que la surveillance de masse soit délaissée au profit d'une surveillance ciblée [voir également : Bortzmeyer].

[SCMagazine] Le FBI souhaite acheter des *malwares* au gigaoctet

Dans une annonce en ligne en date du 12 mai [FBO], le FBI a indiqué souhaiter acheter des *malwares* afin d'aider à ses enquêtes. Le fournisseur bénéficierait d'un contrat d'un an avec le FBI, renouvelable quatre fois, et devrait être en mesure de transférer 30 à 40 gigaoctets de *malwares* chaque jour.

L'affaire des implants de la NSA : des conséquences majeures sur les ventes des constructeurs

Dans son dernier livre, *« No Place to Hide »*, Glenn Greenwald soutient que la NSA a intercepté de manière régulière des équipements réseaux entre l'usine et le client final, afin d'y installer des outils de surveillance (implants) [The Guardian]. Suite à ces révélations, le Directeur Général de Cisco a exprimé, par courrier, son inquiétude au Président américain B. Obama quant aux méthodes de la NSA [Re/code]. Ces allégations d'espionnage seraient la cause directe, selon Chambers, de la réduction des ventes de 27% au Brésil et de 28% en Russie enregistrées au 1er trimestre 2014 [Forbes].

Le conflit sino-américain s'intensifie par une cascade de réactions, suite à la mise en accusation de présumés hackers chinois par le *Department of Justice (DoJ)* américain

Le Département de la Justice américain a annoncé, le 19 mai, l'inculpation de cinq officier de l'Armée populaire de libération chinoise pour « *piratage informatique* » et *« espionnage économique »* [The Guardian]. Selon l'acte d'accusation, les cinq officiers membres de l'Unité 61 398 du troisième département de l'APL auraient, entre 2006 et 2014, collecté des données secrète appartenant à des entreprises américaines du secteur énergétique ou de la métallurgie.

Comme l'a justement rappelé Eric Holder, procureur général des Etats-Unis et responsable du DoJ, *« cette affaire d'espionnage industriel présumé perpétré par des membres de l'armée chinoise représente les premières poursuites jamais engagées à l'encontre d'un acteur étatique pour ce type de piratage »*.

La réaction chinoise fut rapide : après s'être retirée du groupe de travail sino-américain sur la cybersécurité [Bloomberg], la Chine a interdit Windows 8 sur les terminaux gouvernementaux [ZYCG] et a annoncé, le jeudi 22 mai, qu'elle établirait un *« cybersecurity vetting system »* pour tous les produits IT entrant sur son territoire. Objectif : éliminer tout soupçon d'espionnage et d'activité de surveillance [PCWorld]. Cette annonce a été suivie de mesures concrètes, le gouvernement chinois ayant expressément demandé aux banques domestiques de remplacer leurs serveurs IBM par une marque locale [Bloomberg]. Il aurait également ordonné à ses entreprises publiques de ne plus faire appel aux services des principales entreprises de consulting américaines (McKinsey, Boston Consulting Group, Bain & Co). Ces entreprises étant soupçonnées de fournir des informations sensibles au gouvernement américain [Forbes].

Le gouvernement américain étudierait pour sa part la possibilité de restreindre l'émission de visas afin d'empêcher certains *hackers* chinois de participer aux conférences « Black Hat » et « Def Con ». Cette action, qui s'inscrirait ainsi dans le droit fil d'une stratégie de pression sur la Chine [The Guardian], n'a toutefois pas été confirmée par les organisateurs des évènements concernés [Zdnet].

[RT] Le FBI sur les traces de hackers russes : le *Department of Justice* (*DoJ*) est prêt à agir

Diverses rumeurs font état d'une prochaine offensive menée par le *Department of Justice (DoJ)* américain, à travers la formulation d'accusation visant des *hackers* russes. Ces derniers, tout comme les cinq officiers chinois, devraient être accusés de cyberespionnage économique sur le fondement des investigations menées par le FBI.

[Cicero] La Suède n'invite pas E. Snowden à la « Stockholm's Internet Freedom Convention »

Le gouvernement suédois, organisateur de la *« Stockholm's Internet Freedom (SIF) Convention »* - rendez-vous européen réunissant les cyber-activistes - a décidé de ne pas inviter Edward Snowden, ni aucun de ses confidents (le *hacker* Jacob Appelbaum, ou encore les journalistes Glenn Greenwald et Laura Poitras). Ce qui a déclenché une vague de protestation au sein de la communauté des hactivistes qualifiant cette

décision d'« absurde », la SIF 2014 ayant comme principale thématique la cyber-surveillance.

[The Verge] La Chambre des Représentants des Etats-Unis réduit la marge de manœuvre de la NSA

La Chambre des Représentants des Etats-Unis a voté, jeudi 22 mai, le *« US Freedom Act »*. Le contenu de la loi réduit la marge de manœuvre de la NSA sur la surveillance des appels téléphoniques à travers l'analyse systématique des relevés téléphoniques des clients des grandes entreprises de télécommunications américaines. La NSA ne pourra entrer en possession de ces relevés qu'après une période de 18 mois. Si l'Agence veut obtenir ces documents plus tôt, elle devra justifier sa demande auprès de la Cour de Justice Américaine et se contenter de recherches par mots-clés. La Chambre a toutefois rajouté un amendement qui réduit considérablement l'efficacité de la loi, étendant les modalités de recherche aux adresses (email, comptes en ligne, adresses physiques) et appareils (ordinateur, portables, etc.).

[Slate] USA Freedom Act : la Chambre des Représentants des Etats-Unis interdit à la NSA de s'immiscer dans l'élaboration des standards de chiffrement

La Chambre des Représentants des États-Unis a interdit à la NSA de s'immiscer dans l'élaboration des standards de chiffrement. Ces standards, précédemment établis par le *National Institute of Standards and Technology (NIST)* et la NSA, sont intégrés par les agences gouvernementales et les sous-traitants afin de sécuriser leurs échanges d'informations sur le web. Le vote du texte [USA Freedom Act] survient 8 mois après que le New York Times a accusé la NSA de profiter de sa position pour exploiter les failles au sein de protocoles de chiffrements.

[Wired] La Darpa utilisera Oculus à des fins militaires

La Darpa a lancé un projet de R&D dans le but d'intégrer la technologie Oculus Rift dans les opérations de lutte informatique. Objectif : simplifier la visualisation des données et flux réseaux afin d'augmenter la flexibilité opérationnelle des *hackers* militaires du USCYBERCOM. La Darpa n'a pas indiqué quand cette technologie sera opérationnelle.

[The Intercept] Les Bahamas demandent aux Etats-Unis de s'expliquer sur l'opération SOMALGET

Les autorités des Bahamas ont demandé aux États-Unis des explications sur l'opération SOMALGET, pilotée par la NSA [The Intercept]. En effet, si le gouvernement de l'archipel a bien permis à la *Drug Enforcement Agency (DEA)* de mettre en place l'enregistrement des conversations téléphoniques de narcotrafiquants, elle n'a en aucun cas autorisé la NSA à enregistrer la totalité des appels téléphoniques émis depuis ou à destination des Bahamas. Les États-Unis n'ont pas encore donné suite à cette demande, mais assurent les Bahamas qu'ils *« valorisent leur relation »*.

[WikiLeaks] L'Afghanistan serait le deuxième pays ciblé par l'opération SOMALGET, selon WikiLeaks

L'Afghanistan serait le deuxième pays ciblé par l'opération d'enregistrements et d'écoutes téléphoniques opérée par la NSA, et baptisée SOMALGET. Cette information a été révélée par WikiLeaks, vendredi 23 mai. Il est important de rappeler que Glenn Greenwald avait décidé, lundi 19 mai, de ne pas divulguer cette information, jugeant qu'elle risquerait de mettre en péril la vie d'innocents. Julian Assange, qualifiant cette décision de « censure », s'engagea à dévoiler le nom du pays espionné sous les 72 heures [CS Monitor]. Il faut toutefois souligner qu'Assange n'a pas fourni de documents sources *(leak)* étayant sa déclaration, contrairement à toutes les révélations jusque-là issues d'Edward Sowden.

[eMarketer] La région d'Asie Pacifique enregistrera, dans les quatre prochaines années, la plus forte progression d'utilisateurs Twitter

Selon eMarketer, la région d'Asie Pacifique enregistre la plus forte progression d'utilisateurs

Twitter. Il est estimé qu'en 2018, 40% des utilisateurs viendront d'Asie. Ce pourcentage pourrait augmenter significativement si la Chine se décidait à lever l'interdiction visant le réseau social.

[Prachatai] Plus de 100 URLs bloqués en Thaïlande depuis la proclamation de la Loi Martiale

En Thaïlande, depuis l'imposition de la Loi Martiale le 20 mai, plus de 100 URLs ont été bloqués. Depuis décembre 2011, ce nombre s'élève à 22 000. La censure du Web thaïlandais est opérée par le *Cyber Security Operation Center*. Cet organisme gouvernemental exige des fournisseurs de services Internet une coopération totale afin d'étouffer toute activité révolutionnaire sur le web.

[Zeenews.india.com] Le Japon veut renforcer sa cybersécurité

Le Japon a annoncé son intention de renforcer son rôle en matière de cybersécurité. Cette annonce s'inscrit par ailleurs dans une volonté plus globale d'assurer le succès des Jeux Olympiques de Tokyo, prévus pour 2020.

[CCDCOE] L'exercice international de cyberdéfense « Locked Shields 2014 »

L'exercice Locked Shields qui réunit plus de 300 participants de 17 Etats a démarré le 21 mai. Pendant deux jours, 12 équipes défensives ont affronté une équipe offensive. Locked Shields est un exercice annuel organisé par le Centre d'Excellence de cyberdéfense de Tallinn.

« Ne téléchargez plus TrueCrypt » : le célèbre logiciel de chiffrement mis à mort

Le mercredi 28 mai, le célèbre logiciel de chiffrement de disque dur TrueCrypt a vu la page d'accueil de son site officiel [truecrypt.sourceforge.net] remplacée par du texte invitant ses utilisateurs à ne plus télécharger le logiciel. La nouvelle page d'accueil indique que le développement de TrueCrypt est arrêté, et invite les internautes à utiliser le système de chiffrement Microsoft : Bitlocker.

Ces changements, jugés peu cohérents par la communauté d'experts en sécurité informatique, ont pour effet de jeter le discrédit sur l'outil jusque-là plébiscité. Aucune explication n'a pour le moment été apportée par l'équipe officielle de développeurs du logiciel.

Le site affiche encore le message suivant : *« ATTENTION : Utiliser TrueCrypt n'est pas sûr, il peut contenir des failles de sécurité non-comblées »*.

[Legalis] Données personnelles : la directive européenne s'applique à Google Inc.

Dans un arrêt du 13 mai, la CJUE s'est prononcée pour l'application de la directive européenne sur la protection des données à caractère personnel à Google Inc. La cour a rejeté le raisonnement selon lequel Google Spain n'intervient pas sur le moteur de recherche, géré par Google Inc. aux Etats-Unis. Elle considère que l'activité publicitaire de Google Spain est indissociable du moteur de recherche, qui rend économiquement viable la première.

Cet arrêt donne en outre la responsabilité aux moteurs de recherche d'arbitrer entre d'un coté les articles 7 et 8 de la Charte des droits fondamentaux (respectivement respect de la vie privée et familiale et protection des données à caractère personnel), et de l'autre coté *« l'intérêt prépondérant dudit public à avoir [...] accès à l'information en question ».*

[Atos] Atos prévoit d'acquérir Bull pour créer un leader européen dans le Cloud, la Cybersécurité et le Big Data

Atos et Bull ont annoncé conjointement le 26 mai leur projet d'acquisition du dernier par le premier. Atos, entreprise internationale de services en technologie de l'information, prévoit de créer une entité Big Data et Cybersécurité sous la marque Bull, alors que la filiale Cloud d'Atos, Canopy, se verra renforcée des équipes de Bull dans le domaine.

[GSM] Cybersécurité : partenariat stratégique entre Alcatel-Lucent et Thales

Thales et Alcaltel-Lucent ont conclu un partenariat stratégique qui prévoit l'acquisition par Thales des activités Services de Cybersécurité et Sécurité des Communications d'Alcatel-Lucent. L'objectif stratégique de ce partenariat est, pour Alcaltel-Lucent, d'offrir des solutions de bout en bout pour la sécurisation des réseaux de télécommunications, alors que Thales souhaite accroître ses activités de cybersécurité et de consolider l'expertise de ses équipes.

Les accords définitifs ne sont pas encore signés, et il faut encore attendre la consultation des instances représentatives du personnel et l'obtention des autorisations préalables pour que le partenariat devienne effectif.

[SC Magazine] Cisco rachète l'entreprise d'analyse de malware ThreatGRID

Le développeur de solutions réseaux Cisco a annoncé son intention d'étendre son portfolio cybersécurité (baptisé AMP pour *Advanced Malware Protection*) en rachetant la société ThreatGRID. ThreatGRID, spécialiste de l'analyse des *malwares*, développe des solutions sur site et dans le Cloud de détection de *malware* et de renseignement des menaces cybernétiques.

[ZDnet] Surveillance des réseaux : Dyn fait l'acquisition de Renesys

Dyn, société spécialisée dans l'IaaS, a racheté pour un montant non divulgué la société Renesys. Renesys, spécialiste de la supervision en temps réel du trafic, possède une technologie d'identification de routage efficace à travers des conditions réseaux changeantes, technologie qui intéresse particulièrement Dyn afin de l'intégrer dans ses plateforme de gestion du trafic et des messageries.

[GSM] Facebook et F-Secure s'associent pour protéger les utilisateurs du plus grand réseau social au monde

Facebook va utiliser la technologie de F-Secure pour offrir un scan de *malware* directement dans le navigateur. Ce service sera activé pour tous les utilisateurs de Facebook dont le compte a été temporairement gelé en raison d'une activité suspecte potentiellement liée à une infection par *malware*.

[Infosecurity] Check Point lance son "Cyber Intelligence Marketplace"

Le CEO de check Point a annoncé le lancement de sa place de marché dédiée à la « cyber intelligence », le ThreatCloud IntelliStore. La plateforme intègre les données de ses partenaires iSight, CrowdStrike, IID, NetClean, PhishLabs, SenseCyy et ThreatGRID. Les clients devraient ainsi pouvoir sélectionner les informations selon leurs besoins.

[ANSSI] L'ANSSI publie un guide de bonnes pratiques sur l'acquisition et l'exploitation des noms de domaine

Avec ce guide, l'ANSSI souhaite offrir *« des recommandations organisationnelles, juridiques et techniques pour choisir un prestataire, enregistrer son domaine et sécuriser son hébergement »*.

[Livre] "No place to hide" de Glenn Greenwald

Le journaliste Glenn Greenwald (The Intercepter) a publié le 13 mai son ouvrage intitulé "No place to hide" (JC Lattès, 360 p.). Greenwald fut le dépositaire des documents soustraits à la NSA par Edward Snowden. Dans cet ouvrage, l'auteur révèle, entre autres, que la NSA placerait des backdoors (« implants ») dans des routeurs et autres matériels réseau de fabrication américaine, avant leur export à l'international [WSJ].

[Internet Governance Panel] « Towards a Collaborative, Decentralized Internet Governance Ecosystem »

Le panel sur la coopération globale de l'Internet et les mécanismes de gouvernance publie son rapport intitulé "Towards a Collaborative, Decentralized Internet Governance Ecosystem".

S'inscrivant dans le droit fil de NetMundial, le document liste les composantes essentielles d'un écosystème collaboratif et décentralisé pour la Gouvernance Internet, et propose un plan d'action pour 2017 :

- Encourager la mondialisation de l'ICANN et de la fonction IANA ;
- Faire évoluer le processus de prise de décision vers un mode plus collaboratif ;
- Renforcer le développement d'alliances pluri-acteurs

L'une des propositions majeures est la création de groupes de réflexion "décentralisés" *(DG ou distributed governance groups).*

Créé sous l'impulsion de l'ICANN en partenariat avec le Forum Economique Mondial, le Panel est présidé par le président estonien Toomas Ilves, assisté de Vint Cerf, co-inventeur du protocole TCP/IP ; il réunit des acteurs issus de la société civile, du secteur privé, de gouvernements, ainsi que quelques organisations internationales et représentants de la communauté scientifique.

[EFF] Les sociétés qui protègent le mieux les données des utilisateurs face aux demandes du gouvernement américain

L'Electronic Frontier Foundation (EFF) a publié une étude offrant un classement des sociétés qui protègent le mieux les données de leurs utilisateurs, en fonction de critères tels que l'obligation de disposer d'un mandat pour accéder aux données, l'information de l'utilisateur ou encore les litiges judiciaires opposant les sociétés à l'administration.

Selon Rainey Reitman, directeur activisme d'EFF, les révélations d'Edward Snowden ont incité nombre de sociétés à améliorer leur politique de protection des données utilisateur face à l'administration.

[ICO] L'I.C.O. publie un rapport sur les erreurs de sécurité les plus courantes

L'autorité britannique I.C.O. *(Information Commissioner's Office)* a publié un rapport de sécurité recensant les erreurs de sécurité les plus courantes au sein des systèmes d'information. Pour Simon Rice, Group Manager de l'équipe technologie d'I.C.O., le fait que ces erreurs, pourtant de notoriété publique, continuent d'apparaître au cours des enquêtes montre qu'il y a un réel besoin de continuer d'insister sur celles-ci auprès des RSI.

Les progrès dans l'identification et l'attribution des cyberattaques

Si une prise en compte grandissante des risques par les différents acteurs et la multiplication des outils défensifs contribuent à réduire les conséquences des cyberattaques, l'augmentation continue de ces dernières indique tout de même qu'une approche purement défensive ne dissuade pas les cyberattaquants de sévir. Il est ainsi indispensable d'être en mesure d'identifier les auteurs des attaques afin de permettre le déclenchement de réponses cybernétiques, politiques ou juridiques.

Pour autant, est-il judicieux pour une organisation de faire savoir qu'elle possède des capacités en termes d'identification et d'attribution ? Celle-ci court alors le risque de voir son efficacité réduite.

En octobre 2012, un officiel du DoD (*Departement of Defense*) indiquait, malgré la croyance communément partagée dans le cyberespace qu'il était impossible d'attribuer une attaque à un individu ou à un Etat spécifique, que son département avait investi avec succès dans le développement de cette capacité. Leon Panetta, alors ministre de la Défense des Etats-Unis, ajoutait que l'*U.S. Army* possédait dorénavant les capacités de déterminer les origines des cyberattaques[1].

Si ces annonces prennent tout leur sens suite aux révélations d'Edward Snowden, on peut se douter que ces « progrès » reposent en grande partie sur les capacités sans précédent de l'USCYBERCOM (United States Cyber Command) et de la NSA. Il convient alors de souligner les difficultés rencontrées dans l'attribution des cyberattaques mais aussi les méthodes qui pourraient permettre de surmonter ces difficultés.

Pourquoi est-il difficile de tracer la source d'une attaque ?

Contrairement au réseau téléphonique traditionnel, qui possède un système efficace d'identification et de localisation des utilisateurs lié au besoin de facturer l'utilisation du service pour chaque appel, le réseau Internet n'a pas été conçu dans l'optique d'identifier les échanges et leurs auteurs autrement que dans un but purement logistique : il s'agissait à l'origine d'un réseau gratuit à l'utilisation. De plus, étant adressé à une communauté collaborative de chercheurs, les besoins de sécurité n'ont pas été anticipés lors de la phase de spécifications d'ARPANET. Il ne s'agissait pas de protéger le réseau contre des cyberattaques internes, mais contre des attaques physique externes. La robustesse a été privilégiée au détriment de la sécurité.

Une première réponse technique : le *Single PacketBacktracing*

Le protocole TCP-IP qui permet le transport des flux de données en segmentant ces dernières sous la forme de paquets (comprenant entre autres l'adresse source, l'adresse de destination et les données elles-mêmes) n'opère pas de vérification de l'adresse source, ce qui rend aisée l'usurpation de l'adresse d'un autre ordinateur. L'usurpation d'adresse IP possède cependant un inconvénient : l'émetteur réel ne peut pas recevoir de réponse de son destinataire au cours de cette communication à sens unique.

Cette technique est employée notamment dans les attaques par déni de service (DoS) afin de cacher l'émetteur des paquets (l'attaquant) ou en se faisant passer pour la cible réelle de l'attaque (DRDoS).

[1] http://www.stripes.com/news/us-can-trace-cyberattacks-mount-pre-emptive-strikes-panetta-says-1.192789

L'objectif est de faire envoyer des requêtes par un grand nombre d'ordinateurs qui usurpent l'adresse IP de la victime. La victime recevra alors les réponses à des requêtes qu'elle n'a pas réellement émise, au risque intentionnel d'être surchargée et de ne plus être opérationnelle.

Si l'idée de tracer individuellement les paquets IP dans l'optique de contrer l'usurpation d'IP et de remonter au plus proche de la source est ancienne, plusieurs propositions plus concrètes sont apparues à partir du début des années 2000. L'idée originelle était de faire stocker par les routeurs les paquets IP en transit, afin de permettre d'être en mesure de remonter facilement et rapidement au point d'entrée sur le réseau. Cette première approche se confrontait à plusieurs obstacles, à la fois techniques (capacité de stockage et vitesse d'enregistrement) et juridiques (protection de la vie privée).

En 2001, une première approche appelée *Hash-Based IP Traceback*[2] propose de stocker uniquement des *Hashs* – c'est-à-dire des empreintes – des paquets IP transitant par les routeurs. Cette technique est au cœur du *Source Path Isolation Engine*[3] (SPIE), qui permet de répondre à l'obstacle technique de capacité de stockage et à celui juridique de préservation de la confidentialité des données.

Cette approche, nécessitant d'apporter des évolutions aux routeurs, permettrait une identification quasi-instantanée, au mieux de l'attaquant, sinon du point d'entrée sur le réseau d'une cyberattaque. Elle pourrait s'inscrire dans une démarche nationale, voire transnationale, au sein d'un espace de coopération. On imagine en revanche plus difficilement une application au niveau mondial : au-delà des principes généraux relatifs à la lutte contre la cybercriminalité, il est fort peu probable que les Etats s'entendent pour financer une amélioration coûteuse de leurs infrastructures suivant une norme commune qui contraindrait d'autant leurs capacités offensives.

La technologie a cependant ses limites. Quand bien même serait identifié le poste d'origine de l'attaque (ce qui est rendu difficile par l'utilisation de proxy), la technologie seule ne permettrait pas de connaître l'identité de la personne physique contrôlant l'ordinateur qui dirige l'attaque. L'analyse automatique doit être complétée par des analyses déductives dont seuls des analystes expérimentés sont capables. Par exemple, si l'utilisation d'un botnet est à première vue un élément rendant particulièrement difficile l'identification d'un attaquant, un examen du code peut mettre en évidence qu'il s'agit d'un botnet peu répandu et ains i réduire considérablement le champ des possibles dans l'attribution de l'attaque.

La méthode InCA[4]

Une équipe internationale de chercheurs a développé un nouvel algorithme baptisé InCA (Intelligent Cyber Attribution) afin d'attribuer l'origine d'une opération, algorithme censé en outre être capable d'expliquer à l'analyse les raisons de cette attribution. Ce système est basé sur la combinaison de modélisations probabilistes, qui constituent le modèle environnemental (EM), et de raisonnements argumentés se basant sur des travaux en matière d'intelligence artificielle, soit le modèle analytique (AM).

[2] http://www.cs.cmu.edu/~srini/15-744/papers/p1-snoeren.pdf
[3] http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.12.3752&rep=rep1&type=pdf
[4] http://arxiv.org/pdf/1404.6699.pdf

Modèle EM	Modèle AM
« Le malware W et le malware X utilisent le même style de programmation. »	« Le malware W et le malware X sont liés. »
« Le pays Y et le pays Z sont en guerre. »	« Le pays Y a des raisons de lancer une cyberattaque contre le pays Z. »
« Le pays Y a investi significativement dans l'éducation en matière mathématique et scientifique. »	« Le pays Y has la capacité de lancer une cyberattaque. »

Exemples d'observations – EM vs AM

Les données contenues au sein du modèle EM se doivent d'être cohérentes, alors que le modèle AM permet l'emploi d'informations contradictoires. Au sein de ce second modèle, un processus dialectique s'enclenche entre les arguments contradictoires, aboutissant à l'invalidation de l'un d'eux sur la base d'un critère de comparaison. Ceci permet en outre d'outrepasser aisément les fausses pistes laissées par les cyberattaquants dans le but d'induire en erreur les analystes. Les informations contenues dans le modèle EM constituent un ensemble de « mondes » dans lesquels seront testés les arguments validés du modèle AM à l'aide d'une *fonction d'annotation*. Cette dernière permet, du fait de la nature probabiliste du modèle EM, d'attribuer des probabilités à différents scénarios afin d'aboutir à une attribution argumentée de l'origine d'une cyberattaque.

Cette méthode se veut être la première à associer la programmation logique défaisable (Defeasible Logic Programming[5], un système qui permet de tirer des conclusions argumentées à partir d'informations incomplètes ou contradictoires) à des informations probabilistes. Elle nécessite évidemment d'être alimentée par des données les plus exhaustives possible. Ainsi, les axes de développement déterminés par les auteurs de ce modèle sont les suivants :

- Permettre l'alimentation automatique des modèles EM et AM à partir des données collectées ;
- Permettre l'attribution des cyberattaques en temps réel ;
- Identifier les preuves supplémentaires qui doivent être collectées afin d'améliorer une requête spécifique d'attribution ;
- Permettre à l'algorithme d'être en mesure de traiter un grand volume de jeux de données.

Le développement de solutions similaires à la méthode InCA semble incontournable, tant les cyberattaques peuvent allier célérité et pouvoir de nuisance, voire de destruction. Ceci appelle bien à la création de systèmes capables de détecter les cyberattaques et d'identifier leurs auteurs pratiquement en temps réel. Un système tel que le *Source Path Isolation Engine* pourrait permettre en outre de nourrir en informations une solution de type InCA, dans le périmètre dans lequel le premier serait appliqué.

[5] http://cs.uns.edu.ar/~ajg/papers/2004TPLPGarciaSimari.pdf

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

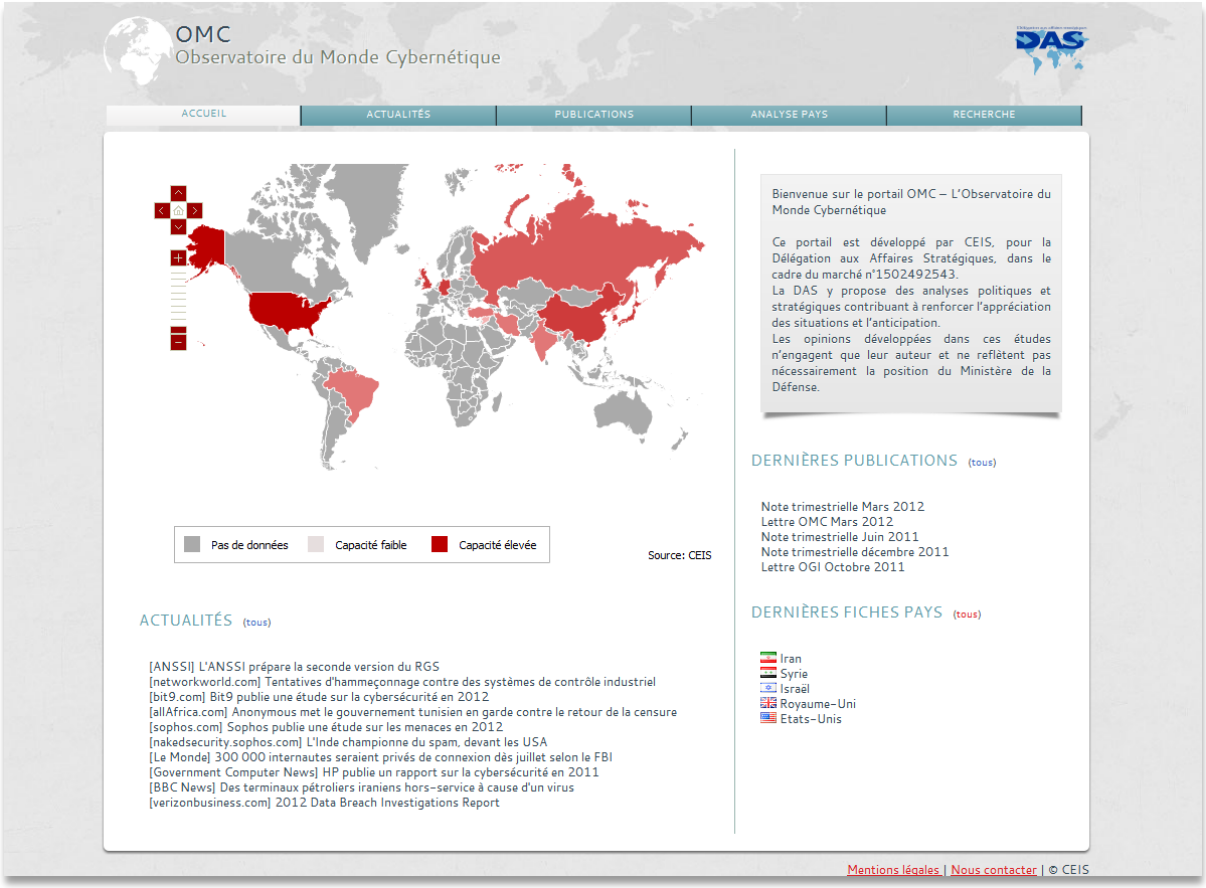

Figure 1. Page d'accueil du portail OMC - https://omc.ceis.eu/

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

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

SSTIC	Rennes	4 - 6 juin
CSO Interchange	Paris	12 juin
Université du SI	Paris	16 – 17 juin
Cyber Intelligence USA	Arlington, Etats-Unis	18 – 20 juin
« Hack In Paris »	Paris	23 – 27 juin
CLUSIF "Menaces informatiques et pratiques de sécurité en France - Edition 2014"	Paris	25 juin
Nuit du hack	Paris	28 – 29 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