Observatoire du Monde Cybernétique

Lettre n°36 – Décembre 2014

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

[industrie-techno] Airbus de l'énergie, institut cybersécurité : l'innovation franco-allemande vue par Geneviève Fioraso

Lundi 8 décembre s'est tenu le 5ème forum de la coopération franco-allemande en recherche qui a lieu tous les trois ans depuis 2002. Geneviève Fioraso, secrétaire d'Etat à l'Enseignement supérieur et à la Recherche, a pu y rappeler l'importance de la cybersécurité dans le secteur du numérique. Ce secteur fait en effet partie des pistes à privilégier dans le cadre de la recherche commune aux deux pays. Ce partenariat pourrait se renforcer par la création d'un Institut de recherche franco-allemand en cybersécurité co-localisé à Sarrebruck et Nancy.

[Security Defense Business Review – repris par RPDefense] Interview de Guillaume Poupard, directeur général de l'ANSSI

Neuf mois après sa nomination au poste de directeur général de l'Agence nationale de la sécurité des systèmes d'information, Guillaume Poupard revient sur les évolutions récentes ayant touché l'Agence. Le Directeur rappelle que l'institution est en évolution et en adaptation permanente face aux menaces. L'objectif principal pour cette année 2015 : assurer l'élaboration de règles de sécurité pour les OIV dans le cadre de la LPM.

[NextInpact] Le décret de l'article 20 de la LPM publié : on fait le point

C'est pendant les fêtes de Noël qu'a été publié le très attendu décret d'application de l'article 20 de la loi de programmation militaire. Il s'agit de l'ancien article 13 qui, durant les discussions au Parlement, avait fait l'objet de vives critiques quant au respect de la vie privée, certains dénonçant la création d'un « big brother à la française ». Selon ce texte, c'est le « groupement interministériel de contrôle » placé auprès du Premier ministre qui recevra les données fournies par les opérateurs et hébergeurs. Au nombre des informations concernées : date, horaire, durée de chaque communication, identifiants de connexion, géolocalisation des communications, noms, prénoms, adresse postale, email, pseudonymes, numéros de téléphone ou encore références aux transactions et paiements. Enfin, la question de l'accès en temps réel aux réseaux des opérateurs qui suscitait de vives polémiques est désormais réglée. Les autorités administratives n'auront pas d'accès direct aux réseaux, ce qui rassure la CNIL qui indique que de telles dispositions interdisent « toute possibilité d'aspiration massive et directe des données ».

[Assemblée nationale] Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2014

La délégation parlementaire au renseignement a remis son rapport le 18 décembre dernier. Ce rapport relatif à l'activité de la délégation pour l'année 2014 évoque le champ « cyber » à plusieurs reprises, notamment concernant la recherche opérationnelle et le développement du « cyber-renseignement », ou en référence à la nomination du préfet cybersécurité Jean-Yves Latournerie, dont la nomination est toutefois jugée trop tardive.

[NextInpact] L'Élysée va consacrer 520 000 euros à la sécurisation de ses systèmes informatiques

Conformément au projet de loi de finances de 2015, plus de 500 000 euros devraient être alloués à la sécurisation des systèmes informatiques de l'Elysée. Pour protéger ses infrastructures régulièrement sous le feu d'attaques informatiques, la présidence de la République a notamment comme projet de se doter d'un data center sécurisé.

[Journal du net] Intelligence économique : quel avenir pour le secret des affaires ?

La proposition de loi datant du 16 juillet dernier sera prochainement débattue devant le Parlement. Ce texte prévoit de consacrer le principe de « secret des affaires » selon lequel « nul ne peut obtenir une information protégée au titre du secret des affaires en violation des mesures de protection prises pour en conserver le caractère

non public, ni utiliser ou communiquer l'information ainsi obtenue ». Si le texte est adopté, il sanctionnerait de 3 ans d'emprisonnement et de 375 000 euros d'amende l'atteinte au secret des affaires. Ce texte trouverait à s'appliquer dans certains cas de cybercriminalité.

[FranceInter] Les cyberattaques dans le transport maritime

Dans un communiqué publié le 20 août 2014, le Bureau Maritime International a démontré que les infrastructures maritimes seront de plus en plus touchées par les cyberattaques. Aujourd'hui il est possible pour un pirate informatique de détourner des informations, de prendre le contrôle d'un navire ou même de son système d'armement. En 2011, l'Agence européenne de cybersécurité a publié un premier rapport européen sur la cybersécurité maritime. Elle évoquait déjà les menaces qui s'amplifiaient. La même année, le port d'Anvers avait été piraté par un cartel de drogue. Pour contrer les menaces informatiques, l'école navale, Telecom Bretagne, DCNS et Thales se sont associés pour créer, avec le soutien de la région Bretagne, une chaire de cyberdéfense des systèmes navals.

[Europa.eu] Premier dialogue entre l'UE et les Etats-Unis sur le cyberespace

À l'occasion de la réunion inaugurale du dialogue UE-États-Unis sur le cyberespace qui s'est tenue le 5 décembre 2014, les représentants des deux parties se sont rencontrés à Bruxelles pour discuter de plusieurs aspects du cyberespace liés à la politique étrangère. Au programme : la sécurité internationale dans le cyberespace ; l'évolution de la gouvernance de l'internet en 2015 ; la promotion et protection des droits de l'homme en ligne ; la cybersécurité ; la cybercriminalité.

[RT] Une cyberattaque sur une usine de métaux allemande aurait infligé de sérieux dommages physiques

Dans un récent rapport, le BSI allemand confirme qu'une cyberattaque menée contre une usine métallurgique aurait causé d'importants dommages matériels. L'attaque, trouvant son origine dans un email piégé et du social engineering, aurait causé la défaillance de plusieurs composants qui ont empêché l'arrêt contrôlé d'un haut fourneau, endommageant l'infrastructure. Le rapport précise que les attaquants maitrisaient les processus de production et de contrôle industriels.

[Bloomberg] 2008 : un pipeline turc aurait explosé suite à une cyberattaque

Initialement attribuée au PKK, l'explosion qui a touché l'oléoduc TBC, reliant l'Azerbaïdjan, la Géorgie et la Turquie, aurait en réalité été provoquée par une cyberattaque, selon une enquête publiée par Bloomberg. Si elle est confirmée, cette information viendrait bouleverser la notion de cyberguerre, rendant bien plus probable les effets matériels d'une cyberattaque.

[Citizenlab] Des cyberattaques ciblent les opposants de Daesh

Dans ce rapport diffusé par CitizenLab, John Scott-Railton et Seth Hardy décrivent une cyberattaque qu'ils estiment « probablement » liée à Daesh. Pour appuyer cette hypothèse, ils diffusent une liste d'indicateurs de compromission. L'attaque aurait ciblé un groupe de détracteurs syriens de Daesh (RSS ou Raqqah is being Slaughtered Silently). L'objectif de ces cyberattaques serait de localiser le groupe d'opposants.

[SC] Le Danemark lance sa stratégie de cybersécurité

Le plan de cybersécurité du Danemark propose 27 initiatives réparties en 6 domaines clés. Parmi ces propositions : renforcer les secteurs de l'énergie et des télécommunications, renforcer la formation et l'entrainement et promouvoir les partenariats internationaux.

[Le Point] Nucléaire : la Corée du Sud teste la sécurité de ses centrales après une cyberattaque

Victime d'une récente cyberattaque (vol de données), l'opérateur des centrales nucléaires sud-

coréennes Korea Hydro and Nuclear Power (KHNP) a lancé un exercice visant à tester ses capacités de réponse. Le scénario prévoit que l'auteur de la cyberattaque publie sur Twitter des plans et des manuels de deux réacteurs ainsi que des informations personnelles sur quelques employés de l'opérateur.

[WashingtonPost] La Corée du Nord appelle les Etats-Unis à des investigations conjointes dans l'affaire Sony

La Corée du Nord, qui menace les Etats-Unis de « sérieuses conséquences » si ces derniers poursuivent leurs fausses accusations, propose aux américains de mener conjointement l'enquête dans l'affaire du piratage de Sony. Cette proposition fait suite à la récente affirmation du FBI accusant la Corée du Nord d'être à l'origine du piratage de Sony, grâce à des preuves collectées jugées concluantes.

[Le Monde ; Silicon] Sous la menace, Sony Pictures renonce à la sortie de « The Interview »

Après les menaces d'attentat terroriste dans les cinémas diffusant le film The Interview du studio hollywoodien proférées par le groupe de hackers Guardians of Peace, Sony a annoncé que le long-métrage ne sortirait pas le 25 décembre aux Etats-Unis. Les Anonymous ont également pris part aux débats, reprochant à Sony de céder face aux menaces, et menaçant à leur tour la firme de diffuser le film The Interview. *« Nous ne pouvons pas avoir une société dans laquelle un dictateur peut commencer à imposer une censure ici aux Etats-Unis »*, ont-ils affirmé. Notons que le film a toutefois été diffusé par streaming après le 25 décembre.

[Reuters] Obama ne considère pas le piratage de Sony comme un acte de guerre

Dans une interview accordée à CNN, le Président américain a déclaré ne pas considérer le piratage de Sony comme un acte de guerre, mais comme un acte de « vandalisme ». La réponse apportée sera « proportionnée ». Les Etats-Unis sont en effet directement concernés, les studios Hollywood étant détenus par la firme japonaise Sony. Autre réponse des Etats-Unis : remettre la Corée du Nord sur la liste des Etats favorisant la montée du terrorisme.

[Engadget ; Yahoo!] Coupures d'Internet en Corée du Nord

Selon Dyn Research, Internet aurait été coupé en Corée du nord pendant 9 heures et 31 minutes le 23 décembre dernier. Certains experts ont d'ailleurs estimé qu'il s'agissait d'une riposte américaine, la coupure étant probablement due à une série d'attaques en déni de service. Le 27 décembre, ce sont les réseaux Internet et mobiles (3G) qui ont cette fois été coupés. Ces attaques n'ont toujours pas été attribuées.

[ICANN] L'ICANN ciblée par des attaques de spear phishing

Par un communiqué publié sur son site, l'ICANN annonce avoir été victime d'une attaque de spear phishing. Si une quantité importante de données à caractère personnel, d'identifiants et de mots de passes ont été subtilisés, les fonctions critiques telles que l'Internet Assigned Numbers Authority, qui gère les espaces d'adressage IP, n'auraient pas été touchées.

[ENISA] L'agence européenne de cybersécurité diffuse son programme d'entrainement

Sur son nouveau site enisa.europa.eu/activities/cert, l'ENISA diffuse une série de documents supports des entrainements et cours prodigués par l'Agence. Les documents sont classés par centres d'intérêt et sont librement téléchargeables.

[USNews ; Cylance] L'Iran, une menace grandissante

Depuis l'affaire Stuxnet, l'Iran aurait renforcé ses capacités en matière de cybersécurité. Si bien que le FBI alerte aujourd'hui sur la menace que peut désormais représenter ce pays. Le FBI a en effet transmis à certaines entreprises américaines une note détaillant les modes opératoires des pirates

iraniens. Le Royaume-Uni, la France, l'Allemagne, l'Inde ou encore Israël feraient partie des victimes identifiées. Cela fait écho au récent rapport diffusé par Cylance sur l'opération Cleaver, levant le voile sur certaines opérations d'origine iranienne.

[Arstechnica] 12 millions de routeurs privés et professionnels vulnérables

Des vulnérabilités critiques touchant 12 millions de routeurs de particuliers et professionnels permettraient aux pirates informatiques, depuis n'importe où dans le monde, d'intercepter la totalité du trafic y transitant.

[The Hill] Le Sénat américain vote un texte sur le rôle du DHS en matière cyber

Le texte approuvé par le Sénat vient codifier le rôle du Department of Homeland Security en matière de cybersécurité. Le département dispose désormais d'une autorité claire afin de mener à bien sa mission et ses partenariats avec le secteur privé.

[BlueCoat] Blue Coat dévoile les opérations du groupe Inception

Le groupe de pirates informatiques surnommé Inception par Blue Coat dans son dernier rapport serait à l'origine d'une campagne de cyberespionnage très sophistiquée. Cette campagne qui visait initialement la Russie ou ses partenaires, s'étend désormais à d'autres Etats. Les secteurs ciblés : l'énergie, la finance, mais aussi les secteurs militaire et ambassades.

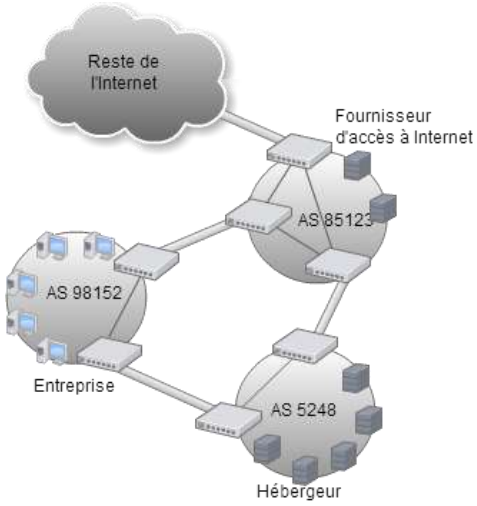
[BBC] Le Kenya démantèle un centre de cybercriminalité chinois

Le Kenya a, en coopération avec l'ambassade chinoise, arrêté 77 cybercriminels chinois. Ces cybercriminels auraient participé à des activités de piratage et de blanchiment d'argent.

.

Détournements BGP, état des lieux

Le transport des données est l'élément le plus critique de l'Internet, mais également le plus vulnérable.



L'Internet est constitué de systèmes autonomes appelés AS (pour Autonomous Systems). Ces systèmes autonomes correspondent à des réseaux qui appartiennent généralement à des fournisseurs d'accès à Internet et des hébergeurs, voire à des grandes entreprises. Les fournisseurs d'accès à Internet assignent les adresses IP à leur client, de telle façon que tout ordinateur connecté à Internet fait partie d'un système autonome.

Ces systèmes autonomes possèdent en leur sein plusieurs routeurs particuliers qui permettent leur interconnexion. Ces routeurs emploient le protocole BGP (Border Gateway Protocol) afin de s'échanger les informations de routes permettant de relier des AS distants, et ainsi permettre les échanges entre machines appartenant à des AS différents.

Malheureusement, l'échange des routes se base sur la confiance réciproque, sans aucun mécanisme d'authentification, ce qui rend le système extrêmement vulnérable : l'injection d'une route au sein de la table d'un seul routeur est susceptible de contaminer l'ensemble de la planète.

Il convient de s'attarder sur les mécanismes de définition et d'échange des routes BGP afin de comprendre comment ce protocole peut être détourné, ainsi que les risques associés à ces détournements et les solutions techniques qui pourraient permettre de les limiter ou de les empêcher.

Protocole BGP

Le protocole BGP permet aux routeurs de définir les routes à emprunter pour acheminer le trafic, en tenant compte de plusieurs facteurs, tels que la disponibilité des systèmes autonomes ou le nombre de sauts à effectuer pour atteindre la destination. Sachant que le protocole BGP ne permet pas de tenir compte de l'état de congestion d'un réseau, une préférence administrative locale peut également être inscrite par l'administrateur de l'AS.

Il existe deux versions du protocole BGP :

- Une version interne, appelé iBGP, qui relie entre eux les routeurs BGP d'un même AS.
- Une version externe, appelée eBGP, qui relie les routeurs BGP entre deux AS voisins.

Les routeurs BGP échangent leurs routes avec leurs voisins directs par un mécanisme d'annonce, de telle façon qu'une route ajoutée dans la table BGP d'un routeur se propage peu à peu dans l'ensemble du monde.

La table BGP d'un routeur associe des routes à des destinations, qui sont généralement des sous-réseaux.

Vulnérabilités et techniques de détournement

Vulnérabilité des tables BGP

Les routeurs BGP établissent une session BGP en utilisant le protocole TCP sur le port 179. Les messages UPDATE, qui permettent de transmettre une liste de routes d'un routeur à un autre, sont transmis en clair. Il existe cependant des mécanismes permettant de limiter les injections :

- Le TTL security permet de s'assurer que le paquet TCP a parcouru le bon nombre de routeurs. Le TTL du paquet IP, ou Time To Live, est décrémenté à chaque saut.
- Le TCP MD5, mécanisme d'authentification basé sur un secret partagé.

Au-delà de ces premières barrières, seul le filtrage mis en place, ou non, par l'administrateur du système autonome peut permettre de rejeter une route transmise par un pair. Et c'est là que le bât blesse : les clients d'un fournisseur d'accès à Internet souhaitent transmettre à ce dernier les routes qui mènent à leur infrastructure, et ce dernier a intérêt à leur faciliter cette possibilité car cela fait partie du service vendu. Par conséquent, le filtrage est plus ou moins fort selon l'opérateur et selon le niveau du client (un client important se verra rarement appliqué un filtrage de ses routes). De l'autre côté de la chaîne, les opérateurs entre eux évitent de s'appliquer des filtres restrictifs, car cela met en péril la continuité et la disponibilité du service. Parfois, un opérateur ne filtre pas les routes à destination de son propre réseau, alors même que celles-ci lui sont transmises par d'autres AS : en effet, rien n'empêche à un routeur d'annoncer une route vers un préfixe qui ne lui appartient pas. Cette faiblesse de l'architecture ouvre la porte à deux principaux risques : le risque de détournement et le risque de déni de service.

Choix des routes BGP et risque de détournements

Le détournement BGP consiste à parvenir à faire transiter le trafic par un point que l'on peut écouter. Pour ce faire, il est nécessaire de parvenir à ajouter une ou plusieurs routes qui devront se propager entre les différents systèmes autonomes.

Détournement BGP - Vert : chemin légitime | Rouge : chemin détourné

En sus d'annoncer un préfixe qui ne lui appartient pas, un attaquant a besoin de s'assurer que la route qu'il injecte sera privilégiée par les différents AS. Deux facteurs clés sont employés :

- L'AS indique un préfixe, et donc une destination, plus spécifique que celui qui est légitime

Route légitime : 

192.168.0.1/24

Route de détournement : 

192.168.0.1/25

- Tout le trafic destiné au sous-réseau le plus petit, empruntera la route de détournement car le préfixe réseau associé à celle-ci est plus spécifique (plus le préfixe est élevé, plus la destination est précise).

- L'AS indique une route plus courte que celle qui est légitime.

Route légitime : 

Route de détournement : 

- Entre deux routes possibles pour la même destination, la préférence ira pour la plus courte.

Le risque de déni de service

L'injection de routes illégitimes peut également être employée pour perturber voire empêcher le trafic IP d'atteindre une destination.

Propagation et choix de route BGP : illustration par l'accident YouTube de Pakistan Telecom

En 2008, le Pakistan a fait les frais du mécanisme de propagation BGP. Afin de procéder à un blocage de site YouTube dans le pays, Pakistan Telecom a ajouté dans son propre AS une route pour YouTube à destination effective de null0, c'est-à-dire un trou noir (les paquets disparaissent dans le dernier routeur). Seulement, cette route s'est propagée, par le biais de l'un de ses fournisseurs qui n'effectuait pas de filtrage, à l'ensemble de la planète : rapidement, le trafic mondial à destination de YouTube était redirigé vers l'AS de Pakistan Telecom, provoquant la saturation de son infrastructure.

La route originale, annoncée par YouTube, était définie avec destination officielle : 208.65.152.0/22

- La route originelle de YouTube avait pour destination l'espace IP 208.65.152.0/22.
- 18h47 - Pakistan Telecom émet une route pour la destination 208.65.152.0/24. Le préfixe étant plus grand et donc la route plus spécifique, celle-ci est préférée.
- 20h07 - YouTube émet une route pour la même destination, 208.65.152.0/24. Problème : la route émise par Pakistan Telecom est plus courte en termes de nombre de sauts, donc c'est celle-ci qui est préférée.
- 20h18 – YouTube émet deux nouvelles routes : 208.65.153.0/25 et 208.65.153.128/25 (c'est-à-dire l'intégralité du réseau 208.65.153.0/24). Ces deux routes étant plus spécifiques, celles-ci sont préférées à la route de Pakistan Telecom.

Paradoxalement, le protocole BGP permet d'employer une technique privilégiée de lutte contre les attaques DDoS baptisée Remotely Triggered Black Hole, qui se traduit par l'envoi de paquets IP vers un « trou noir ». Il s'agit de filtrer les paquets ayant une destination ou une origine spécifiée (respectivement RTBH et Source-Based RTBH). Cela permet de faire disparaître tout ou partie des paquets d'une attaque de type DDoS.

Solutions techniques

Depuis la fin des années 90, plusieurs successeurs potentiels du protocole BGP ont vu le jour, sans pour autant être déployés : en effet, la mise en place d'une solution requiert un accord de l'ensemble des acteurs et implique l'achat de nouveaux équipements. De plus, une amélioration de la sécurité sous-entend nécessairement un risque accru d'indisponibilité des réseaux, élément clé du business des opérateurs s'il en est.

Secure BGP[1] ou S-BGP

Les travaux en vue de créer une version plus sécurisée du protocole BGP ont débuté dès 1997, avec un financement initial de la NSA. La DARPA a ensuite rejoins le financement du projet afin de permettre d'améliorer le design initial.

Les auteurs de S-BGP proposaient de mettre en place un système de triple-certificats pour lier :

- Une organisation et un liste d'espace IP (sous la forme de préfixes d'adresses). Cela permet de vérifier qu'un AS possède bien les espaces IP pour lesquels il propose des routes. Ce type de certificat serait émis par la structure qui assigne les espaces IP, c'est-à-dire l'ICANN.
- Un AS à une organisation. Ce type de certificat serait émis par une structure telle que l'APNIC, l'ARIN ou RIPE ;
- Un AS à un routeur BGP. Ce type de certificat serait émis par un opérateur réseau.

Ensembles, ces deux derniers certificats permettent aux routeurs BGP de s'authentifier l'un l'autre, et de s'assurer que l'émetteur d'une route est bien autorisé à représenter un AS spécifique. Les derniers travaux portant sur le S-BGP remontent à 2004, sans que celui-ci dépasse le stade de projet[2].

Secure Origin BGP ou SO-BGP[3]

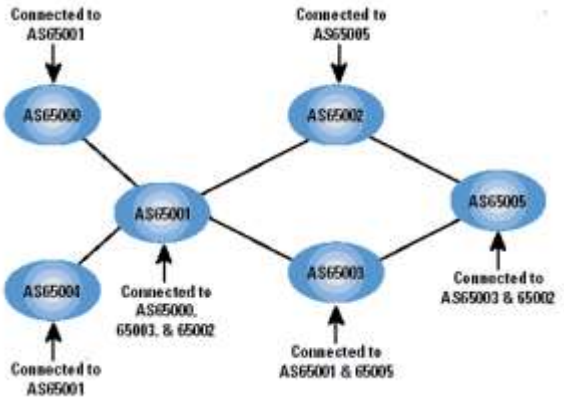
SO-BGP est une évolution sur laquelle travaille l'IETF, portée principalement par des ingénieurs de Cisco Systems. Ce protocole a été conçu afin de permettre aux routeurs BGP de répondre à deux questions :

- Est-ce que l'AS qui émet une route en direction d'une destination est bien autorisé à l'émettre ?
- Est-ce que l'AS qui émet une route possède réellement un chemin vers la destination ?

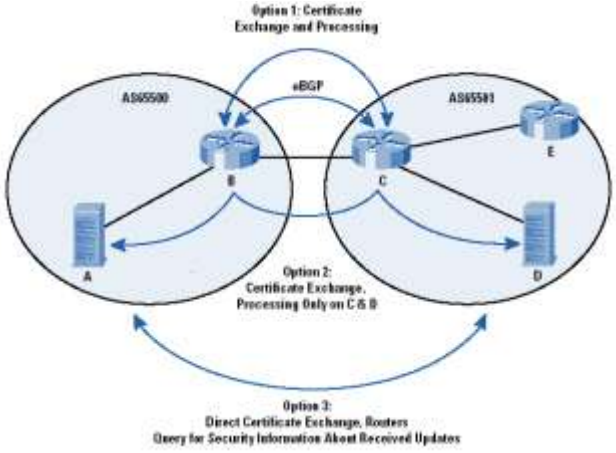
Pour y répondre, SO-BGP utilise également un système de certificats, parmi lesquels :

- Un certificat EntityCert permet de vérifier qu'un AS est bien celui qu'il prétend être ;
- Un certificat AuthCert permettrait de vérifier que l'AS a bien l'autorisation de déterminer l'aiguillage d'un espace IP ;
- Un contenant appelé PrefixPolicyCert. Celui-ci contient le certificat AuthCert, ainsi que les politiques que souhaite voir appliquer l'AS émetteur (comme par exemple une liste d'AS qui ne doivent pas faire partie du chemin menant à lui). Le problème reste bien sûr l'application ou non de ces règles par les AS les recevant ;
- Un certificat ASPolicyCert. Celui-ci contient une liste des pairs connectés à l'AS.

[1] http://users.ece.cmu.edu/~adrian/731-sp04/readings/KLMS-SBGP.pdf
[2] http://www.ir.bbn.com/sbgp/
[3] http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_6-3/securing_bgp_sobgp.html



Options de déploiement de SO-BGP



Topographie établie à l'aide de l'ASPolicyCert

Concernant le problème du déploiement, les ingénieurs à l'origine de ce projet sont conscient que la solution choisie doit impliquer un minimum de changement d'équipement et un minimum de participants.

- Option 1 : Echange et traitement direct des certificats par les routeurs (B et C).
- Option 2 : Echange des certificats par les routeurs (B et C), traitement par des serveurs internes (A et D).
- Option 3 : Echange et traitement des certificats directement par les serveurs internes (A et D). Les routeurs effectueraient des requêtes à ces serveurs pour savoir si les mises à jours reçue sont valides ou non.

Les deux dernières options permettrait de diminuer la consommation CPU et mémoire des routeurs BGP mais nécessitent un équipement supplémentaire. Cependant, laisser la charge entièrement reposer sur les routeurs nécessiterait des routeurs plus performants et serait probablement tout aussi coûteux. La technologie pour sécuriser le protocole BGP existe. Ce qui manque réellement, c'est la volonté des différents acteurs de déployer l'une de ces technologies : cela représente un investissement initial, un coût de fonctionnement plus élevé et un risque de diminution de la disponibilité du réseau. Les opérateurs étant naturellement réticents, la question reste de savoir qui, des Etats ou des entreprises, parviendra à impulser le mouvement initial. En attendant le déploiement d'une version sécurisée du protocole BGP, il existe des outils de veille permettant de détecter les incidents BGP, tel que BGPMon (créé en 2008 par l'organisation éponyme à but non lucratif). De son côté, l'ANSSI a développé son propre logiciel[4] qui décèle les conflits d'adressage à l'aide des données BGP brutes des registres Internet.

[4] http://www.intelligenceonline.fr/renseignement-d-etat/terabytes/2014/11/26/l-anssi-va-contrer-les-detournements-du-trafic-internet,108049763-ART

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

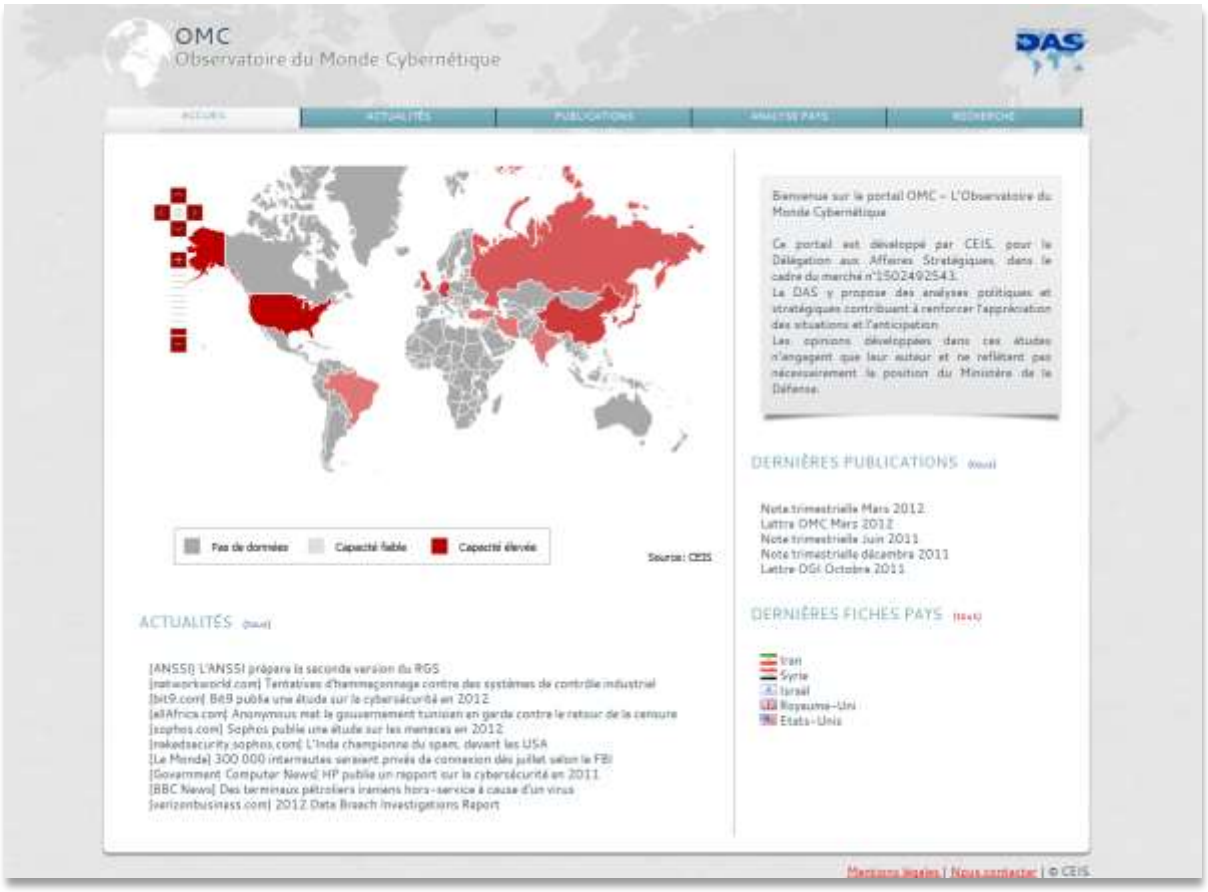


Figure 1. Page d'accueil du portail OMC - https://omc.ceis.eu/

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

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

31c3 Chaos Communication Congress	Hambourg	27 – 30 décembre
Panorama de la cybercriminalité 2014 (CLUSIF)	Paris	Janvier
CORIIN	Lille	19 janvier
Forum International de la Cybersécurité	Lille	20 – 21 janvier
9ème Université AFCDP des Correspondants Informatiques et Libertés	Paris	27 janvier
e-crime & Information Security Germany	Allemagne	29 janvier

Compagnie Européenne
d'Intelligence Stratégique

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

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

Retrouvez cette lettre et l'ensemble des articles cités sur le portail
https://omc.ceis.eu/
(Accès soumis à authentification)

La Délégation aux Affaires Stratégiques propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation.

Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la DAS a confié à la **Compagnie Européenne d'Intelligence Stratégique (CEIS)** cet Observatoire du Monde Cybernétique, sous le numéro de marché 1502492543.

Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère de la défense et des anciens combattants
Délégation aux Affaires Stratégiques
Sous-direction Politique et Prospective de Défense
14 rue St Dominique 75700 PARIS SP 07