Réflexions pour un plan d'action contre les botnets

Éric Freyssinet

Réflexions pour un plan d'action contre les botnets

Lt-col Éric Freyssinet

Direction générale de la gendarmerie nationale, Sous-direction de la police judiciaire
35 rue Saint-Didier, F-75775 PARIS Cedex 16
eric.freyssinet@gendarmerie.interieur.gouv.fr, http://blog.crimenumerique.fr/

Résumé 90% de pourriels, des botnets toujours plus présents, des campagnes de phishing qui s'en prennent de plus en plus aux clients des institutions de tous les pays, sans discrimination. Cet article propose une réflexion sur les modes d'action possibles pour que l'ensemble des partenaires identifiés puissent travailler ensemble et de façon concertée afin non seulement de freiner, mais aussi d'identifier, d'interpeller et de poursuivre tous les acteurs qui profitent de ces schémas criminels.

Avertissement : Cet article contient volontairement un certain nombre de définitions que beaucoup de lecteurs pourront trouver superflues, mais elles ont été maintenues dans un souci de vulgarisation.

1 Introduction

Il est maintenant devenu banal d'affirmer que les botnets [1] sont l'outil le plus courant des cybercriminels. Toutefois, en dehors des cercles spécialisés, il faut bien avouer que le grand public voit les botnets comme un phénomène underground plutôt que comme une vraie tendance de fond.

Les initiatives sont nombreuses qui visent à traquer les centres de commande ou détecter les attaques. D'autres tentent une démarche plus active en incitant les fournisseurs d'accès à "débrancher" les hébergeurs malhonnêtes. Ainsi, Brian Krebs [3] est-il devenu un peu plus célèbre lorsqu'il a réussi à obtenir la fermeture de l'hébergeur malhonnête McColo, grâce à la publication dans un organe de presse grand public des résultats de travaux de recherche de différents spécialistes (dont ceux de Jart Armin et al.[1]).

Malheureusement, les botnets ressurgissent, évoluent et en réalité les véritables groupes criminels qui se sont constitués derrière, petits et grands, sont toujours là et sont rarement identifiés, interpellés et *a fortiori* poursuivis. Les compétences et les projets existent qui doivent permettre de résoudre systématiquement ce problème, mais comment les mettre en œuvre efficacement ?

1. Botnet : Réseau constitué d'ordinateurs contaminés par un logiciel malveillant – appelés alors bots – qui sont sous le contrôle d'un mécanisme de commande. Ainsi, leur maître (ou pasteur / *herder* en anglais) peut leur faire réaliser un certain nombre d'actions coordonnées malveillantes, comme la diffusion de pourriels (ou *spam*) ou des attaques en déni de service distribué

2 Les partenaires

L'action contre les botnets ne peut être qu'une affaire de partenariat. Parce que personne n'a toutes les cartes en main, mais aussi parce que des compétences existent qui doivent être exploitées.

2.1 Les partenaires classiques

Les utilisateurs d'abord sont les premiers partenaires. S'ils protègent mieux leur système d'information et développent les bons réflexes pour éviter les contaminations qui sont la première cause du développement des botnets. À leurs côtés on retrouve naturellement les développeurs et les marchands de systèmes d'exploitation et de logiciels de sécurisation.

Bien entendu, fournisseurs d'accès et hébergeurs sont des acteurs et des partenaires incontournables, aux côtés des services d'investigation. Ces derniers sont éventuellement indispensables pour légitimer certains actes tels que des coupures de service, faire le lien avec des services de police étrangers ou tout simplement s'assurer qu'une action judiciaire sera bien entreprise.

2.2 Les partenaires spécifiques

Les éditeurs de solutions de sécurité ont presque tous développé une expertise dans ce domaine et sont en tout état de cause une source d'informations incontournable. Certains travaillent effectivement de façon active sur la détection des sources de contamination, de distribution ou de commande des botnets.

Enfin, dans la lignée des premières associations créées pour lutter contre les pourriels et identifier les adresses IP ou les domaines sources de problème, de nouvelles organisations se sont créées ou les premiers se sont adaptés. Certains sont plus spéficiquement tournées vers la lutte contre le phishing [2] (Anti-phishing Working Group, Phishtank, ...), d'autres essaient d'avoir une vision plus globale.

3 Les initiatives et sources d'information

Cette section cherche à regrouper les initiatives et les sources d'information disponibles aujourd'hui. L'exercice n'est pas forcément exhaustif, ni complet, donc n'hésitez pas à contacter l'auteur pour le compléter.

3.1 Associations et autres coalitions

Plusieurs associations ou organismes collectent l'information provenant de différentes sources sur l'activité des botnets, les analysent pour les mettre à disposition du public ou de leurs membres et organisent des conférences.

(D'autres initiatives qui ne font pas de collectent pas de données mais soutiennent des initiatives intéressantes sont décrites dans l'annexe 1 de cet article).

2. Phishing : manœuvre consistant à inciter un utilisateur à fournir des données personnelles, par exemple en l'amenant sur un formulaire contrefaisant le site Web d'une banque ou d'un organisme social

Anti-phishing working group La participation à l'APWG est gratuite pour les chercheurs académiques et les représentants des services d'enquête et offre un panel d'outils et d'opportunités d'échanges d'information particulièrement riche pour aider la lutte contre le phishing.

- URL : `http://www.apwg.org/` ;
- Membres : chercheurs, professionnels, services d'enquête ;
- Outils :
  - Liste de discussion ;
  - Groupes de travail en ligne ;
  - Base de connaissances et de données sur le phishing.
- Productions :
  - Rapport trimestriel sur les tendances en matière de phishing ;
  - Étude semestrielle ;
  - Divers articles, études et recommandations.
- Conférences :
  - Counter eCrime Operations Summit (CeCOS), annuelle ;
  - eCrime Researchers Summit, annuelle.

Fondation Shadowserver Regroupant des spécialistes en sécurité informatique, Shadowserver se donne pour objectif de collecter, analyser et partager de l'information sur les logiciels malveillants, l'activité des botnets et la fraude électronique.

- URL : `http://www.shadowserver.org/` ;
- Membres : chercheurs, spécialistes en sécurité informatique ;
- Outils :
  - Liste de discussion ;
  - Base de connaissances sur les botnets, les logiciels malveillants ;
  - Collecte de données sur l'activité des botnets et des attaques.
- Productions :
  - Collection d'études sur les botnets ;
  - Distribution de rapports ciblés (par exemple, à destination du gestionnaire d'un AS [3]) ;
  - Mise à disposition de statistiques détaillées et de cartes.

Signal-spam Association française, créée en novembre 2005 sous l'impulsion de la direction du développement des médias. Elle remplit plusieurs objectifs : informer rapidement les fournisseurs d'accès à Internet des diffusions de pourriels qui les concernent (notamment lorsqu'un de leurs abonnés en est le relais), servir de relais avec les diffuseurs de messages commerciaux et participer à toutes les initiatives de lutte contre les pourriels, que ce soit par la recherche ou en donnant accès aux données qu'elle collecte aux services d'enquête.

- URL : `http://www.signal-spam.fr/` ;

3. AS : Système autonome, ensemble de réseaux IP géré par une entité, typiquement un opérateur

- Membres : chercheurs, professionnels, services d'enquête ;
- Outils :
  - Liste de discussion ;
  - Base de données sur les pourriels, alimentée par les internautes ;
  - Extensions de signalement d'un clic (pour Outlook, Thunderbird).

Team-Cymru Team Cymru est une société de services en sécurité sur Internet, à but non lucratif.
- URL : `http://www.team-cymru.org/` ;
- Outils :
  - Base de connaissances sur les botnets, les logiciels malveillants ;
  - Collecte de données sur l'activité des botnets et des attaques.
- Productions :
  - Registre de condensats (SHA1 ou MD5) de logiciels malveillants accessible par les protocoles WHOIS, DNS, HTTP ou HTTPS ;
  - Cartographie de l'activité des botnets (BATTLE, accessible uniquement aux services d'enquête officiels).
- Conférences :
  - Conférence annuelle *Underground Economy*.

3.2 Bases de données en ligne

Sans autre ambition que de mettre à disposition des professionnels, des chercheurs ou du grand public des bases de données sur l'activité des botnets et autres formes de délinquance en ligne, les initiatives ci-dessous sont particulièrement intéressantes pour qui souhaite agir dans ce domaine.

FI.R.E Finding RoguE Networks est un projet mené par une coalition de trois laboratoires de recherches (Université de technologie de Vienne (Autriche), Eurecom (France), Université de Californie à Santa Barbara (USA)).
- URL : `http://www.maliciousnetworks.org/` ;
- Outils :
  - Base de données sur l'activité des logiciels malveillants.
- Productions :
  - Rapports et cartes par réseau, hôte ou pays.

Phishtank
- URL : `http://www.phishtank.com/` ;
- Membres : Opéré par OpenDNS [4], ouvert à tous ;
- Outils :
  - Base de données sur le phishing, collectées auprès du grand public (et de certains professionnels) ;

4. `http://www.opendns.com`

  - Divers formats d'exportation de la base de données (XML, CSV, JSON, PHP).
- Productions :
  - Statistiques en temps réel ;
  - Rapport annuel.

Sitevet Sitevet est un produit en libre accès de *CyberDefcon*, société animée notamment par Jart Armin. Au moment de la rédaction de cet article, le site est en version bêta.

- URL : `http://sitevet.com/` ;
- Outils :
  - Base de données sur l'activité des logiciels malveillants.
- Productions :
  - Rapports et cartes par réseau, hôte ou pays.

Sites ne fournissant a priori que de l'information statistique ou agrégée Les ressources suivantes ne fournissent pas un accès à des bases de données, mais uniquement à des informations statistiques ou des synthèses.

FireEye Security Center (`http://www.fireeye.com/securitycenter/index.html`) : ce site donne accès à différentes ressources intéressantes sur les botnets ainsi que des cartes animées sur l'évolution des botnets.

M86 Security Labs (`http://www.m86security.com/labs/`) est une société de services en sécurité informatique qui diffuse un certain nombre d'informations pertinentes sur l'état de la menace et l'activité des botnets.

Websense Security Labs (`http://securitylabs.websense.com/content/index.aspx`) présente un certain nombre de cartes, dont certaines sont produites en temps réel, des statistiques et des alertes.

3.3 DNS Blacklists et Whitelists

La RFC [5] 5782 a été publiée dans sa première version définitive en février 2010. Elle est le résultat de travaux de l'Anti-spam research group [6] visant à faire le point des pratiques en matière de mises à disposition de listes noires ou de listes blanches d'hôtes ou de réseaux supposés être des émetteurs privilégiés de pourriels, par le protocole DNS [7].

5. Requests for comments : ces documents décrivent des pratiques, des protocoles, voire des standards de l'Internet. Ils sont édités par l'Internet Engineering Task Force – `http://www.ietf.org/rfc.html`.

6. cf. Annexe 1.

7. Domain Name System : service de l'Internet fournissant une correspondance entre un nom d'hôte dans un domaine et une adresse IP.

Cette pratique ne fait pas l'unanimité dans la collectivité des spécialistes de l'Internet (voir par exemple [2]), mais peut constituer une source d'information particulièrement intéressante, notamment si on est en mesure d'agréger un grand nombre de ces sources d'information.

Ainsi, `http://dnsbl.info/` offre le moyen de consulter d'un seul coup plus de 80 listes noires. On trouve aussi sur le site personnel du chercheur Jeff Makey [8] une comparaison mise à jour chaque semaine d'un certain nombre de listes noires.

3.4 Bloggers, journalistes, chercheurs

Terminons cette revue des sources d'information par un recueil de blogs qui diffusent des alertes ou parfois des études approfondies sur les menaces criminelles sur Internet, en particulier sur celles qui concernent les botnets.

Bloggers individuels Voici quelques exemples de personnes qui diffusent de l'actualité sur les risques en ligne. Ce qui les rassemble est un engagement personnel dans la lutte contre la délinquance sur Internet, sous un angle parfois très technique ou plutôt vulgarisateur.

Jart Armin `http://jartarmin.com`, l'un des dirigeants de CyberDefcon, conférencier apprécié.

Dancho Danchev `http://ddanchev.blogspot.com/`, publie aussi une colonne chez ZDNet (`http://blogs.zdnet.com/security/`, *Zero Day*) avec Ryan Naraine.

Brian Krebs `http://www.krebsonsecurity.com/`, rendu encore plus célèbre suite à la fermeture de l'hébergeur malhonnête McColo.

Blogs d'entreprises

Avert Labs (Mc Afee) `http://www.avertlabs.com/research/blog/`

Hostexploit (CyberDefcon), Jart Armin `http://www.hostexploit.com/`

M86 Security Labs `http://www.m86security.com/labs/traceblog.asp`

Panda Labs `http://pandalabs.pandasecurity.com/`

RSA FraudAction Research Lab `http://www.rsa.com/blog/blog.aspx?author=RSAF`

Secure Works `http://www.secureworks.com/research/blog/`

8. `http://www.sdsc.edu/~jeff/spam/Blacklists_Compared.html`

Viruslist (Kaspersky Lab) `http://www.viruslist.com/en/analysis`

Websense `http://securitylabs.websense.com/content/blogs.aspx`

4 Propositions pour un plan d'action

Une fois ce tour d'horizon réalisé, force est de constater que les sources d'information et les partenaires potentiels sont multiples, mais qu'il semble manquer une vision d'ensemble et peut-être une véritable réflexion stratégique au niveau mondial.

En témoigne la variété des acteurs qui semblent faire la même chose. En témoigne aussi le peu d'affaires qui conduisent réellement à l'identification et l'interpellation de groupes criminels. Ainsi, si on peut se féliciter de l'affaire McColo, ou de l'interpellation des gestionnaires du botnet Mariposa, beaucoup des criminels courent encore et plus surprenant encore, beaucoup de serveurs diffusant des logiciels malveillants ou servant à commander des botnets restent en ligne pendant de nombreuses semaines sans être inquiétés.

4.1 La multiplicité des acteurs criminels

La délinquance massive sur Internet s'est beaucoup éloignée du modèle traditionnel de la cyberdélinquance où l'on voyait un seul *cracker*, éventuellement membre de plusieurs communautés virtuelles développer ses outils, choisir ses cibles et mener à bien des attaques.

Ainsi, on pourra retrouver, selon les cas, les acteurs suivants :

- Le codeur de bots : celui qui développe les logiciels malveillants ;
- Le codeur de système de commande : celui qui développe le système de commande ;
- Le marchand de botnets, soit prêt à l'usage et en location, soit en kit à déployer soi-même ;
- Le pasteur de botnets qui pilote un botnet à un instant donné ;
- Un ou plusieurs hébergeurs pour diffuser les contenus malveillants ou héberger le serveur de commande, soit de façon organisée au travers des hébergeurs malhonnêtes, soit de façon subie par la prise de contrôle de serveurs ;
- Les mules : chargées de recevoir des fonds sur leur compte bancaire et de les transférer vers un intermédiaire, ces personnes sont souvent amenées à penser qu'elles ont une activité légitime ;
- Le pasteur des mules : il gère un réseau de mules et éventuellement d'intermédiaires financiers ;
- Le commanditaire : souvent un groupe criminel, qui finance les développements et la mise en place des hébergements, difficile à identifier.

On voit très nettement au travers de cette énumération que l'arrêt d'un serveur de commande ou d'une équipe de mules, pour être efficaces, devront absolument avoir pour objectif d'identifier un des acteurs clés, tels que codeurs, pasteurs, hébergeurs malhonnêtes ou commanditaires.

4.2 Prévention

Les actions de prévention sont comme toujours indispensables pour diminuer l'impact des activités malhonnêtes.

Sensibilisation L'éducation des utilisateurs doit manifestement faire des progrès. Certainement dès l'école, mais aussi dans l'entreprise.

Il faut dire que les logiciels de navigation ou de courrier électronique se sont aujourd'hui multipliés sans qu'une démarche réellement concertée n'ait été mise en place pour afficher les avertissements ou les informations de sécurité d'une manière semblable, ce qui n'aide pas beaucoup les internautes.

Mesures techniques Outre ces efforts dans le dialogue avec le public, un certain nombre de mesures techniques sont mises en avant par de grands acteurs (SPF [9] ou DKIM [10] par exemple), dont la généralisation peut certainement améliorer la sécurité dans le réseau.

4.3 Détection

Il faut avouer qu'en termes de détection, les sources d'information existent, sont animées par de nombreux professionnels, comme nous l'avons évoqué dans la 3^e section ci-dessus.

Mais comment imaginer que les services de police de tous les pays soient en mesure d'appréhender l'ensemble de ces sources d'information ? Il est absolument nécessaire d'explorer deux pistes de recherche pour leur rendre ce travail plus accessible :

- la généralisation d'un format d'échange de données standardisé, tel que l'IODEF [11] et les extensions proposées pour le phishing [12] ;
- la création d'outils permettant de synthétiser l'ensemble des sources d'information existantes pour les rendre exploitables par les services de police d'un pays ou un opérateur pour son propre réseau.

4.4 Réaction

Plusieurs acteurs doivent donc agir de façon concertée, pour mitiger l'effet d'un logiciel malveillant ou d'un serveur de commande de botnets, collecter des preuves et finalement interpeller les criminels.

---

9. Sender Policy Framework : consistant à publier dans les enregistrements DNS les serveurs autorisés à émettre du courrier pour un domaine donné, RFC 4408, `http://www.openspf.org/`

10. DomainKeys Identified Mail : norme d'authentification du domaine de l'expéditeur d'un courrier électronique consistant à introduire des signatures cryptographiques, RFC 4871, `http://www.dkim.org/`

11. Incident Object Description Exchange Format, RFC 5070, `http://tools.ietf.org/html/rfc5070`

12. `https://datatracker.ietf.org/doc/draft-cain-post-inch-phishingextns/`

On a vu que les acteurs criminels sont multiples et n'ont pas tous la même importance dans l'organisation de ces activités. Ainsi, de la même façon que pour les affaires de contrefaçon de cartes bancaires, il est indispensable de remonter à la source (souvent localisée dans des pays de l'ancienne Europe de l'est), la France, comme beaucoup de ses partenaires, n'est souvent que l'hôte de ces activités et doit avoir une action de collecte et d'analyse de preuves.

L'action typique, par exemple sur un serveur de commande de botnet, pourrait donc se dérouler en 5 temps :

1. Détection ;
2. Coordination : avec les opérateurs concernés et les partenaires de confiance étrangers ;
3. Opération policière et technique coordonnée ;
4. Analyse des preuves collectées ;
5. Partage de l'information.

La coordination est nécessaire pour éviter que l'action dans un pays nuise à des enquêtes se déroulant dans un autre pays. Toutefois, elle ne doit pas empêcher un coup d'arrêt contre un phénomène qui aurait pris une ampleur trop importante dans un pays donné. Cette coordination est aussi nécessaire pour permettre aux opérateurs, notamment les hébergeurs, de préserver un certain nombre de preuves en amont avant qu'elles n'aient pu être supprimées. Si le cadre juridique le permet le service d'enquête peut éventuellement mettre en place une opération de surveillance ou d'interception de communications sur le serveur. C'est peut-être le temps le plus complexe et pour lequel il n'existe pas réellement d'instance chargée de l'animer au niveau européen ou mondial.

L'opération policière est assez simple, elle consiste à saisir le serveur et ainsi interrompre au moins temporairement son activité. L'action technique à mettre en œuvre par les opérateurs nationaux ou internationaux associés remplit plusieurs objectifs :

- si c'est légalement ou contractuellement possible bloquer toute action du botnet sur le réseau, pour empêcher notamment son rétablissement trop rapide ou détecter ses tentatives de rétablissement ;
- informer si possible les usagers comme participant à leur insu au botnet pour les inciter à décontaminer rapidement leurs systèmes.

Le partage de l'information, permet éventuellement de réamorcer le plan d'action à l'étape 1 ou l'étape 2 ou de l'enclencher dans d'autres pays. Le ficher d'analyse Cyborg d'Europol devrait être un des vecteurs privilégiés de cet échange d'informations (notamment parce qu'il offre un cadre juridique adapté).

Bien entendu ce schéma est à adapter en fonction des situations (serveur de commande bien localisé ou bien distribué grâce à l'utilisation de noms de domaine multiples ou d'autres techniques furtives, action contre une équipe de mules, démantèlement d'une diffusion importante de bots chez un opérateur, etc.).

5 Faire évoluer la législation

Plusieurs mesures d'ordre législatif ou réglementaire sont peut-être nécessaires pour améliorer l'efficacité de tels projets.

5.1 De la neutralité des réseaux

La neutralité nécessaire des réseaux par rapport aux messages échangés, aux protocoles utilisés ou à l'accessibilité des services ne doit pas être un obstacle à des mesures proportionnelles et temporaires permettant de limiter ou empêcher la propagation ou le fonctionnement d'un botnet.

Selon les pays, des adaptations juridiques sont peut-être nécessaires pour permettre de telles mesures et surtout, elles doivent absolument être encadrées par des bonnes pratiques, éventuellement être menées sous l'autorité d'un organisme officiel (par exemple l'ANSSI en France) et réalisées en totale transparence vis à vis des usagers.

5.2 De la définition du pourriel

Autant tout le monde s'entend pour dénoncer les courriers électroniques non sollicités, autant notre législation est peut-être encore inadaptée. Ainsi, plusieurs dispositions se conjuguent pour permettre la lutte contre les pourriels et notamment :

- La collecte illicite de données personnelles (loi informatique et libertés) ;
- L'escroquerie et l'atteinte aux systèmes de traitement automatisé de données, pour cibler les tentatives de phishing ;
- La diffusion de messages commerciaux non sollicités (loi pour la confiance dans l'économie numérique).

Toutefois, cette combinaison laisse quelques trous dans la raquette. Ainsi l'envoi de courriers électroniques non sollicités, lorsqu'ils n'ont pas de caractère commercial, n'est pas forcément immédiatement identifiable comme une action illicite. De même, l'infraction prévue par la loi pour la confiance dans l'économie numérique en matière de spams n'est qu'une contravention.

Il pourrait donc être intéressant d'envisager :

- l'extension de la notion de courriers électroniques non sollicités aux situations de la loi pour la confiance dans l'économie numérique aux messages non commerciaux ;
- la création d'un délit de diffusion de pourriels au-delà d'un certain seuil de gravité, sans qu'il soit besoin de prouver la collecte illicite de données personnelles.

5.3 Du secret de l'enquête

Pour ce dernier sujet, nul besoin d'une évolution législative, mais peut-être faudrait-il développer un cadre de bonnes pratiques entre services d'enquête,

opérateurs et magistrats pour autoriser l'échange d'informations qui normalement relèvent du secret de l'enquête pour permettre l'action concertée des différents acteurs.

En revanche, il convient peut-être d'autoriser les agences chargées de la coopération policière (Europol, Interpol) à partager certaines informations mises à disposition par les États-membres avec des groupes d'intérêt de confiance (telles que les organisations évoquées précédemment). En pratique, si l'on prend le cas du fichier d'analyse Cyborg géré par Europol, chaque service de police partageant des informations pourrait autoriser au cas par cas la mise à disposition de ces données (notamment les données techniques) avec des partenaires extérieurs.

6 Conclusion

Répétons-le : il est indispensable que l'action purement technique soit coordonnée avec l'action policière et l'action judiciaire. Sans cela, les véritables criminels qui sont à la source des activités les plus lucratives ne seront jamais identifiés et interpellés et continueront de rétablir leur activité sans être réellement inquiétés.

On a vu que l'affaire est particulièrement complexe, les acteurs encore peu coordonnés et qu'il faut chercher un mode d'action adapté à chaque situation.

Comme dans toute situation, il faut se laisser la possibilité de faire des erreurs ou de commencer par des actions plus simples, mais il ne faut pas perdre de vue l'objectif plus global.

L'auteur tenait à partager sa réflexion dans le but de recevoir tous les commentaires utiles à son enrichissement, aussi n'hésitez pas à lui écrire !

Références

1. Armin, J., et al. : McColo – Cybercrime USA. Hostexploit.com. 2008 version 2.0. `http://hostexploit.com/downloads/view.download/4/14.html`
2. Bortzmeyer, S. : RFC 5782 : DNS Blacklists and Whitelists. 19 février 2010. `http://www.bortzmeyer.org/5782.html`
3. Krebs, B. : Host of Internet spam groups is cut off. The Washington Post. 12 novembre 2008. `http://www.washingtonpost.com/wp-dyn/content/article/2008/11/12/AR2008111200658.html`

---

7 Annexes

7.1 Annexe 1 - Associations diverses

Dans cette annexe sont regroupés les acteurs qui n'offrent pas de sources de données directement utilisables.

Anti-spam research group L'activité de ce groupe n'est pas exceptionnelle en tant que tel, aucune activité spécifique n'est rapportée depuis 2004. En revanche, on peut supposer que ses listes de discussion restent actives et permettent à des chercheurs d'échanger sur leurs sujets d'intérêt communs.

- URL : `http://asrg.sp.am/` ;
- Membres : chercheurs (l'ASRG est une Internet research task force [13]) ;
- Mission : Groupe de recherche sur des outils et autres solutions techniques contre les pourriels ;
- Outils :
  - Listes de discussions ;
- Productions :
  - Wiki `http://wiki.asrg.sp.am/wiki/Main_Page`

Anti-spyware coalition L'ASC est un organisme essentiellement nord-américain, animé par le *Center for Democracy and Technology* [14].

- URL : `http://www.antispywarecoalition.org/` ;
- Membres : chercheurs, professionnels, autorités de défense des consommateurs ;
- Productions :
  - Publication de recommandations.
- Conférences :
  - Conférence publique annuelle.

Online trust alliance

- URL : `https://otalliance.org/` ;
- Membres : professionnels, services d'enquête, autres ONG ;
- Productions :
  - Publication de recommandations.
- Conférences :
  - Conférences thématiques et conférence annuelle (*Online Trust & Cybersecurity Forum*).

Messaging anti-abuse working group Si ce groupe ne semble pas produire d'informations directement exploitables à l'extérieur, il conduit la réflexion au sein de l'industrie de la communication électronique et cherche à promouvoir de bonnes pratiques (comme l'authentification des réseaux émetteurs de messages).

13. `http://www.irtf.org`
14. `http://www.cdt.org/`

- URL : `http://www.maawg.org/` ;
- Membres : professionnels (organisés en six groupes, à noter un groupe qui s'intéresse aux messages abusifs transmis sur les réseaux de téléphonie mobile) ;
- Productions :
  - Rapport semestriel sur les volumétries de messages abusifs ;
  - Études et sondages ;
  - Publication de recommandations.
- Conférences :
  - Réunion annuelle, réservée aux membres.

London action plan Il ne s'agit pas ici d'un groupe avec une activité spécifique importante, mais plus la volonté de partager un objectif commun, décrit dans les lignes directrices du plan d'action. On y retrouve d'ailleurs certaines organisations citées par ailleurs.

- URL : `http://www.londonactionplan.org/` ;
- Membres : autorités (notamment de protection des consommateurs), professionnels ;
- Mission : selon le plan, les mesures concrètes qui rassemblent ce groupe sont la sensibilisation, l'échange de bonnes pratiques, la facilitation et la mise en place de procédures de coopération, l'organisation d'opérations conjointes ;
- Conférences :
  - Conférence annuelle conjointe avec le Contact Network of Spam Enforcement Authorities (CNSA).

International botnet task force L'objectif principal que se sont donnés les promoteurs de ce projet est la formation des services d'enquête à la lutte contre les botnets. Ce groupe reste assez confidentiel dans ses activités (pas de site Web), mais les retours sont particulièrement positifs de la part de ceux qui ont pu assister aux ateliers de formation.

- Membres : professionnels, services d'enquête (co-optés) ;
- Conférences :
  - Environ deux conférences sont organisées chaque année.

7.2 Annexe 2 - Ressources sur les logiciels malveillants

Les ressources de la présente section portent uniquement sur les logiciels malveillants et ne référencent pas l'activité détaillée des botnets.

F-Secure Lab (`http://www.f-secure.com/fr_FR/security/`), portail d'information de l'éditeur F-Secure (base de données des logiciels malveillants, outils de détection en ligne, ...).

MyAvert - Avertlabs (`http://www.avertlabs.com/`), est la base de connaissances antivirale de la société McAfee.

Threatexpert (`http://www.threatexpert.com/`) est une société Irlandaise qui se propose d'analyser des logiciels malveillants et fournit une base de connaissances sur ces menaces qui indique si possible un pays suspecté d'origine.

Viruslist (`http://www.viruslist.com/fr/viruses/encyclopedia`), site d'information de *Kaspersky Lab*, présente des descriptions et analyses de logiciels malveillants.

Virustotal (`http://www.virustotal.com/`) est un service proposé par *Hispasec Sistemas* qui propose d'analyser un logiciel supposé malveillant ou un condensat d'un fichier suspect en utilisant les ressources de dizaines de produits de sécurité.

Panda Labs (`http://www.pandasecurity.com/homeusers/security-info/about-malware/encyclopedia/`) propose outre une base de connaissances sur les virus des rapports trimestriels et des monographies sur différents phénomènes.