Lettre n°56-Novembre 2016-disponible sur omc.ceis.eu

Brève du mois

« Working with the hacker community is an effective way to uncover vulnerabilities in even the most powerful organizations. Inviting the hacker community to find unknown security vulnerabilities will supplement the great work the Army's talented cybersecurity personnel are doing already », Eric Fanning, US Secretary of the Army[1].

TABLE DES MATIERES

[1] http://www.infosecurity-magazine.com/news/hack-the-army-becomes-latest-bug/

« CYBER » TACTIQUE : RETOUR SUR LES EXPERIMENTATIONS DE L'US ARMY

Quelles que soit le niveau auquel elles sont menées, les actions de lutte informatique offensive sont en général considérées comme une responsabilité de niveau stratégique. Impossible, pour autant, d'écarter ex abrupto la constitution de capacités de lutte informatique aux niveaux tactique et opératif car le numérique est présent à tous les niveaux de commandement. D'autre part, les technologies permettront peut-être demain de standardiser des capacités « cyber » adaptées à ces échelons. Tels sont les constats qui ont conduit l'US Army à lancer depuis 2015 un vaste programme d'expérimentation.

De fait, à l'instar d'une étude du Center for Strategic and International Studies et du Georgia Tech Research Institute de 2013[2], on ne peut que constater une certaine inhibition de la réflexion stratégique concernant le développement de capacités cyber tactiques. Les attaques informatiques sont considérées comme « stratégiques » par essence alors que seuls l'effet final recherché et les objectifs à atteindre devraient permettre de qualifier leur niveau. Les auteurs de l'étude déplorent ainsi que cette inhibition conduise à une logique circulaire : les capacités tactiques n'étant développées, il est inutile d'envisager leur utilisation potentielle. En conséquence, aucun besoin opérationnel n'est exprimé, ce qui rend impossible le développement des capacités adéquates. Tout ceci explique que le champ du « cyber tactique » soit aujourd'hui encore peu exploré. S'il existe bien des exercices spécifiquement consacrés à la lutte informatique, il n'existe pas ou peu d'expérimentations réalistes visant à tester l'utilisation de capacités cyber en appui à la manœuvre tactique. D'où l'intérêt du programme CSCB (Cyber Support to corp and below) lancé en juillet 2015 par l'US Army Cyber Command et la Second Army de l'Armée de terre américaine.

Le contexte

Le programme d'expérimentation CSCB répond tout d'abord à la demande du Chef d'Etat-Major de l'Armée de terre américaine, le général Odierno, de démontrer les effets cyber au niveau des corps et échelons en dessous[3]. « Si le renseignement stratégique ainsi que la défense des infrastructures critiques relèvent bien de la responsabilité de CYBERCOM, l'Army entend bien utiliser ses capacités à des fins opératives et tactiques en appui des brigades interarmes engagées »[4], explique l'auteur du blog Cybertactique.

Cette volonté s'est d'ailleurs traduite par l'intégration, en 2014, des capacités de lutte informatique et de guerre électronique au sein de l'Armée de terre sous la forme de « CEMA (Cyber Electromagnetic Activies) expeditionnary team ». Selon le Field Manual 3.38 dédié à ces activités[5], l'objectif est de synchroniser les opérations de lutte informatique, la guerre électronique et la gestion des fréquences. Il est prévu que ces équipes comptent 15 soldats par brigade, contre 4 à 6 auparavant (lesquels étaient

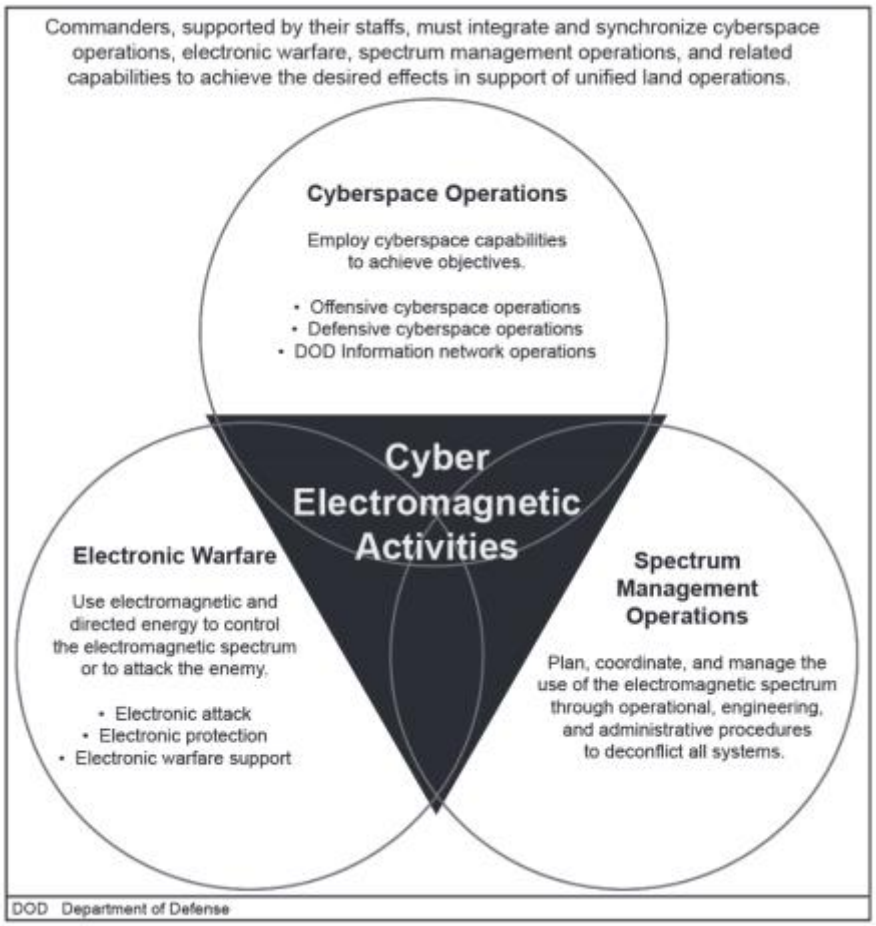
[2] Offensive cyber capabilities at the operational level. The way ahead. Septembre 2013. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130916_Leed_OffensiveCyberCapabilities_Web.pdf

[3] https://www.army.mil/standto/archive_2015-07-16/

[4] http://cybertactique.blogspot.fr/

[5] http://fas.org/irp/doddir/army/fm3-38.pdf

principalement des planificateurs intégrés aux états-majors), et comprennent à la fois des capacités de lutte informatique, de guerre électronique, de renseignement, d'opérations d'information et de gestion des réseaux. Un changement que la général Frost, en charge des opérations à l'Army Cyber Command, qualifie de « sismique » pour faire face à la mutation de l'environnement informationnel. « L'environnement informationnel est en train d'exploser. Les soldats ont besoin de savoir comment naviguer dans cet environnement », explique-t-elle.[6]



Autre évolution notable : la mise à jour de l'Army Regulation 525-15[7], désormais intitulée « Software reprogramming for cyber electromagnetic activities », pour intégrer une dimension numérique. Il s'agit désormais de développer des équipements de guerre électronique reprogrammables intégrant des bibliothèques de menaces, des capacités de détection, de préparation et d'exécution de missions couvrant aussi le champ cybernétique.

[6] https://www.army.mil/article/165494

[7] http://fas.org/irp/doddir/army/ar525-15.pdf

Les expérimentations

En 18 mois de « wargames » et d'entrainement, le programme CSCB a permis d'expérimenter le déploiement de « CEMA expeditionnary teams » au sein de nombreuses unités de l'US Army, qu'il s'agisse de brigades d'infanterie légère, de troupes aéroportées, de brigades mécanisées ou bien encore de régiments de rangers. Pour le général Nakasone, le patron de l'Army Cyber Command (ARCYBER), l'objectif est clair[8] : "I'm going to come back to the Department of the Army with a recommendation". Il s'agit donc d'analyser le fonctionnement et les résultats des unités pour pouvoir améliorer les tactiques et techniques, ainsi que les plans, les politiques et les doctrines en se focalisant d'abord sur le niveau brigade. L'enjeu est de taille : réussir l'intégration des capacités et effets cyber aux niveaux tactique et opératif et définir ce que seront les opérations de demain, et en déduire les besoins en termes de compétences, d'équipements, d'organisation et de procédures.

Pour réussir cette mission, l'ARCYBER s'appuie sur le National Training Center de Fort Irwin (NTC, Californie), dédié aux unités blindées et le Joint Readiness Training Center de Fort Polk (JRTC, Louisianne), destiné aux unités d'infanterie. Pour ce faire, les deux centres ont créé avec l'aide de l'ARCYBER une réplique en miniature d'un environnement numérique d'un petit Etat-nation afin de permettre aux « CEMA expeditionnary teams » d'exercer leurs talents en matière de « situational awareness », de protection des réseaux, d'opérations d'information et de lutte informatique offensive.

Côté NTC, la 2ème brigade blindée « Stryker » a ainsi conduit en janvier 2016 un premier exercice. Si les détails sont classifiés, quelques éléments du scénario ont transpiré[9] : une vidéo émise par un drone montre au PC brigade la présence d'un radar de conduite de tir dans un camp de réfugiés. Le commandant de la brigade doit donc choisir entre une frappe classique, au risque de causer de nombreuses pertes humaines, et une attaque de guerre électronique visant à désactiver le radar, tout le débat étant de savoir si l'effet pouvait être produit dans les temps impartis compte tenu de la chaine de commandement et des éventuelles difficultés techniques. En juillet et août 2016, c'est la 1st Armored Brigade qui est engagée dans l'exercice Climactic[10]. Au total 40 à 45 « cyber soldats » lui sont attachés avec la répartition suivante : une « defense support team » de 4 ou 5 soldats dédiés à la protection du réseau de la brigade ; 4 « weapon teams » de 2 ou 3 soldats chacune déployées auprès des différentes compagnies ; une composante « guerre électronique » de 2 soldats par unité ; quelques spécialistes positionnés au niveau de l'état-major de la brigade, notamment un « information operation planer » pour les opérations d'information. Là aussi, peu d'informations précises sur l'exercice lui-même, si ce n'est que l'une des « weapon teams » déployées sur un poste d'observation a pu, grâce à des équipements mobiles, couper les communications d'un C2 ennemi et permettre à l'unité de manœuvrer en conséquence.

Côté JRTC, un premier exercice a été mené avec la 3ème brigade de la 25th Infantry division, qui a été suivie en juin 2015 par un ranger régiment, puis en novembre 2015 par la 1ère brigade d'infanterie et la 82ème division aéroportée.

---

[8] http://breakingdefense.com/2016/11/army-wargames-hone-battlefield-cyber-teams/

[9] http://smallwarsjournal.com/jrnl/art/cyber-support-to-corps-and-below-digital-panacea-or-pandora%E2%80%99s-box

[10] http://breakingdefense.com/2016/06/offensive-cyber-comes-to-the-street-fight/

Quels enseignements ?

Certes, ces expérimentations sont sans doute une manière pour l'US Army de relancer les programmes de guerre électronique sous couvert de « cyber ». La plupart de ces programmes ont, en effet, été abandonnés par l'US Army après la fin de la guerre froide. Aucun brouilleur offensif ne sera ainsi mis à disposition des unités avant 2023, l'Armée de terre dépendant aujourd'hui d'équipements prêtés par d'autres forces, comme les avions Growler de la Navy[11]. Mais c'est aussi pour l'US Army un moyen de consacrer le lien fort existant entre capacités de lutte informatique et capacités de guerre électronique, surtout aux niveaux tactique et opératif. Avec le développement des réseaux sans fil (WiFi, WiMax, mesh networks, réseaux d'objets connectés…), la frontière entre les deux types de capacités n'a jamais été aussi floue, nombre de cibles « cyber » étant atteignables par des moyens de guerre électronique.

Cette évolution obéit donc aussi et surtout à une nécessité opérationnelle. Comme le soulignent Andrew Metcalf et Christopher Barber[12], le terrain a changé : « Aujourd'hui, avec quelques échecs notables, nous menons un combat cinétique contre un adversaire qui n'est pas pleinement préparé à exploiter la dépendance américaine à l'égard des technologies de l'information. Les militaires américains ne peuvent pas compter sur le fait qu'une telle dynamique soit toujours vraie à l'avenir ». Le retour des Etats-puissance et la crise ukrainienne ont sans nul doute contribué à cette prise de conscience…

Les expérimentations ont ainsi permis de montrer l'intérêt « d'une combinaison au niveau tactique des effets défensifs, offensifs et informationnels », commente l'auteur du blog Cybertactique[13]. « En outre, une « capacité de proximité », capable de prendre en compte l'environnement informationnel numérique (réseaux sociaux, activités en ligne...) couplée avec une capacité d'analyse multi-capteurs a démontré son utilité notamment en matière de ciblage et d'évaluation de l'atteinte des objectifs par la force. » En d'autres termes : les effets « cyber » peuvent être compris et exécutés comme les autres effets. Il est donc indispensable d'intégrer le « cyber » à tous les échelons, du stratégique au tactique. « Nous voulions créer un autre tuyau d'orgue appelé CEMA, mais c'est une mauvaise habitude bureaucratique. Cyber et guerre électronique ont besoin d'être intégrées au sein de chaque composante, qu'il s'agisse d'artillerie, de manœuvre terrestre ou de logistique, dans un plan cohérent. Et cette intégration est le travail des chefs », explique le colonel Jerry Turner de la 2ème Stryker Brigade[14]. « Le réseau est une plateforme de combat, et nous devons la traiter comme telle », poursuit la général Frost. « Ce n'est pas un service, c'est une plateforme de combat qui nous permet de concevoir et d'exécuter nos opérations ».

Quels défis ?

Au-delà de ces premiers enseignements, l'intégration d'une capacité « cyber » au niveau tactique soulève un certain nombre de défis :

- Comment concilier le temps opérationnel avec le rythme des opérations de lutte informatique, telles qu'on les conçoit aujourd'hui, c'est à dire au niveau stratégique ? Alors que le temps opérationnel est particulièrement fugace, les opérations cyber nécessitent souvent des horizons temporels de plusieurs semaines avec un fort besoin de renseignement et d'anticipation, par

[11] http://breakingdefense.com/2015/07/armys-electronic-warfare-cupboard-is-bare-no-jammer-until-2023/

[12] http://smallwarsjournal.com/jrnl/art/tactical-cyber-how-to-move-forward

[13] http://cybertactique.blogspot.fr/

[14] http://breakingdefense.com/2016/11/army-wargames-hone-battlefield-cyber-teams/

définition impossible à satisfaire au niveau tactique. La Cyber Kill Chain définie par Lockheed Martin (reconnaissance, weaponization, delivery, exploitation, installation, command & control et action) doit donc être la plus comprimée possible.

- Comment prévoir et mesurer les effets de l'opération offensive menée au niveau tactique et s'assurer que ces effets soient bien maitrisés ? Difficile en effet, compte tenu de l'interconnexion des réseaux, de garantir qu'une attaque sur telle ou telle cible n'aura pas de répercussions non souhaitées sur d'autres systèmes numériques, d'autant que la notion de rayon d'effet physique n'est pas applicable.

- Comment assurer une « situational awareness » efficace de l'espace numérique afin d'éviter les « tirs » fratricides ? Difficile de représenter un environnement particulièrement mouvant. D'autant que l'environnement numérique doit aussi être superposé à l'environnement physique pour permettre au chef d'avoir une « common operational picture » globale.

- Comment faire en sorte que les unités de combat s'imprègnent suffisamment du sujet pour intégrer efficacement le cyber parmi les capacités à la disposition du chef ? Les expérimentations de l'US Army ont souligné la difficulté qu'avaient spécialistes cyber et forces conventionnelles à se parler. « Que les geeks fassent leur travail et qu'ils me laissent faire le mien » ![15], ont répondu certains commandants de brigade en se moquant du « dolphin speak » des spécialistes cyber. Bien sûr, il serait absurde de prétendre transformer tout le monde en spécialiste cyber. Il s'agit seulement de développer une acculturation mutuelle, à laquelle les expérimentations actuelles ont d'ailleurs nettement contribué.

- Comment éviter, enfin, qu'une action cyber tactique ait des conséquences non souhaitées par le niveau stratégique ? Comment faire les arbitrages entre les objectifs de terrain et les objectifs stratégiques ? « Le problème du « caporal stratégique » s'aggrave quand le fusil du caporal peut avoir des effets sur tout le globe et viser des cibles inconnues », soulignent Andrew Metcalf et Christophe Barber[16]. « Tous les planificateurs prévoyant l'emploi du cyber tactique doivent comprendre l'impact potentiel sur la situation diplomatique, informationnelle, militaire, économique, financière, renseignement et juridique ». Premier exemple : que se passe-t-il si un commandant veut empêcher un groupe d'insurgés d'accéder à un réseau social hébergé dans un autre pays ? S'il agit sur le réseau en question et non en local, le risque de violation de la neutralité d'un autre pays, et donc d'escalade, est bien réel. Deuxième exemple : faut-il « supprimer » une cible qui pourrait constituer une source de renseignement précieuse ? Certains tenants du « cyber tactique » déplorent en effet les opérations cyber soient principalement considérées pour leur intérêt pour le renseignement. Troisième exemple, enfin : l'utilisation tactique de capacités de lutte informatique offensive peut conduire à la dissémination non contrôlée de malwares informatiques. Indépendamment de la question du coût de développement de telles armes, la question est aussi de savoir s'il faut risquer, pour une opération tactique, de « griller » une vulnérabilité informatique (parfois juste un mot de passe par défaut sur un routeur) et de provoquer le développement par l'adversaire de contre-mesures, alors que cette vulnérabilité aurait pu être utilisée à meilleur escient.

Pistes de réflexion

Si l'on considère que le développement de capacités de lutte informatique tactique est inéluctable compte tenu de la digitalisation du terrain d'affrontement, ces différents défis appellent plusieurs réflexions.

[15] http://breakingdefense.com/2015/11/army-fights-culture-gap-between-cyber-ops-dolphin-speak/

[16] http://smallwarsjournal.com/jrnl/art/tactical-cyber-how-to-move-forward

- Au niveau tactique, guerre électronique et lutte informatique vont nécessairement de pair, puisque les capacités de guerre électronique sont l'un des vecteurs d'accès aux cibles « cyber ». « *Fondamentalement, il n'y a que trois vecteurs d'attaque contre les systèmes informatiques : le « close access », le « remote access » et le « wireless access* », expliquent Mickael Klipstein et Michael Senft[17]. Et seul le « wireless access » permet, au moins dans certains cas, de maitriser le rayon d'effet.

- Si les cibles ne sont pas tactiques ou stratégiques par nature, l'échelon tactique doit intégrer dans ses critères de ciblage les contraintes de temps et les capacités des modes opératoires à sa disposition. Certaines cibles, en particulier les réseaux dit « fermés », présentent ainsi l'avantage de limiter le risque de propagation non voulue des effets, même si aucun réseau n'est par définition fermé puisque le branchement d'une clé USB sur un poste isolé constitue une forme de connexion.

- Le contrôle des effets peut être obtenu par un système de combat cyber-électronique qui, à partir d'une modélisation du terrain numérique, identifie les interactions, assure le suivi de l'action et en mesure les effets. C'est tout l'enjeu du projet DARPA Plan X dont l'objectif est de construire une plateforme de combat cyber directement utilisable par les commandants de brigade. Le projet comporte ainsi un module appelé « cyber battlespace analytics » incluant la modélisation du terrain numérique et l'évaluation dynamique des dommages.

- Le risque de dissémination et de gaspillage d'un armement cyber sophistiqué peut être évité si les capacités tactiques sont principalement basées sur des moyens et outils publics. Pourquoi par exemple utiliser une solution coûteuse pour couper une liaison WiMax si un brouillage simple grâce une solution du marché à 25 $ suffit, s'interrogent Andrew Metcalf et Christopher Barber ?

- Au plan organisationnel, le choix du responsable tactique, compte tenu du temps utile imparti, ne peut être validé par toute la chaine de commandement de l'opération et nécessite de la subsidiarité. Les informations doivent cependant circuler horizontalement et verticalement, dès lors que les effets peuvent sortir du périmètre de responsabilité du responsable tactique.

- Le développement d'une capacité de lutte informatique tactique implique bien évidemment l'élaboration d'une doctrine et de règles d'engagement précises, ainsi que le développement de compétences spécifiques.

Conclusion

Actuellement, la chaine de commandement opérationnelle de cyberdéfense est unifiée, centralisée et spécialisée.

Les expérimentations menées par les Américains montrent qu'une réflexion est engagée pour décentraliser certaines actions offensives au niveau tactique. Plusieurs raisons militent en ce sens :

- Certaines actions, notamment « wireless », ne peuvent se faire « qu'au contact » ;

- L'échelon tactique peut ainsi ajouter l'effet cyber dans la gestion dynamique des différents modes d'action à sa disposition ;

[17] http://smallwarsjournal.com/jrnl/art/cyber-support-to-corps-and-below-digital-panacea-or-pandora%E2%80%99s-box

- La multiplication des techniques et outils grand public rend possible techniquement et financièrement d'en doter les unités sans risquer la dissémination d'outils d'attaques plus complexes réservés au niveau stratégique ;

- Il devrait être possible à terme de « packager » des capacités offensives pour produire à des effets standards sans ressources spécialisées ;

- L'augmentation du vivier d'experts « cyber » permettra sans doute d'en affecter aux différents niveaux de la chaine de commandement, alors qu'ils sont aujourd'hui regroupés dans des unités dédiées.

BOTNET MIRAI : QUELLES CONSEQUENCES ?

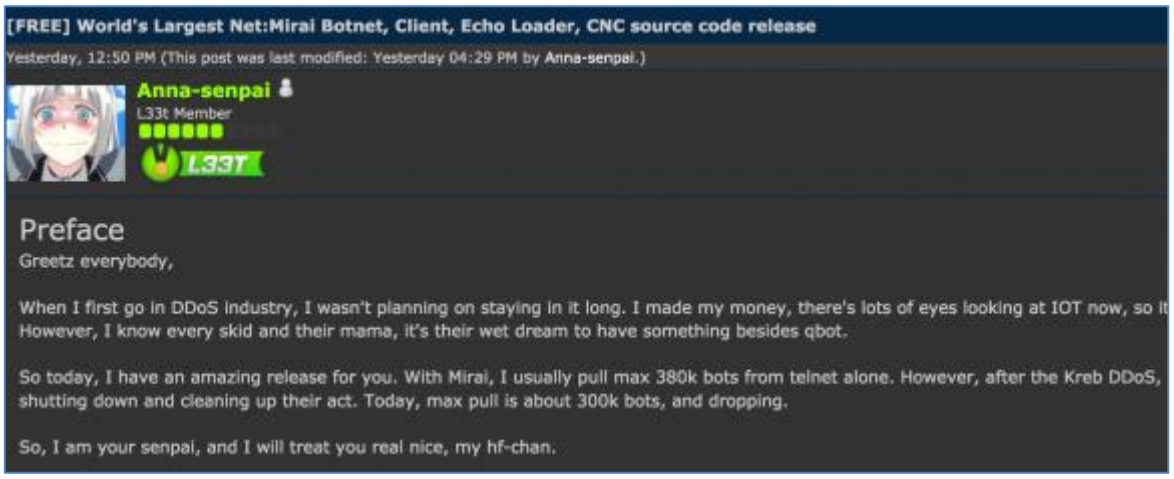
Le 13 septembre 2016, Bruce Schneier publiait sur son blog un billet intitulé « *Someone Is Learning How to Take Down the Internet* »[18]. Il annonçait qu'une entité non-identifiée testait depuis plusieurs semaines les limites de l'Internet via des campagnes de type DDoS de grande envergure. Ces dernières ciblaient précisément les principales sociétés fournissant l'infrastructure dorsale du réseau informatique mondial pour créer un potentiel blackout généralisé.

Cette annonce fut d'abord accueillie avec un certain scepticisme par le monde de la cybersécurité en raison de la solidité éprouvée des serveurs racines du DNS comme ceux fournis par VeriSign. Mais plusieurs événements exceptionnels contribuèrent à faire changer d'avis les experts : entre le 19 et le 20 septembre 2016, OVH et KrebsOnSecurity furent les principales cibles des plus importantes attaques DDoS jamais mesurées en termes d'intensité (avec des pics jusqu'à 1 Tbps) et, surtout, de mode opératoire (plus de 145 000 objets connectés piratés employés).

Plusieurs investigations révélèrent alors que ces dénis de service distribués avaient été menés à partir de botnets basés sur un malware révolutionnaire intitulé Mirai dont le concepteur publia le code source. Son objectif était que d'autres attaquants puissent déployer leurs propres botnets et couvrent en parallèle et de manière indirecte ses traces via la multiplication des origines des attaques.

Multiplication des botnets et des attaques associées

Le code source du malware Mirai a été rendu public par son créateur le 29 septembre sur le site anglophone Hack Forums dédié comme son nom l'indique au hacking. Le dénommé *Anna-senpai* accompagne le code source d'un long tutoriel expliquant pas à pas comment mettre en place un botnet basé sur son malware d'une capacité maximale de 300 000 machines zombies :



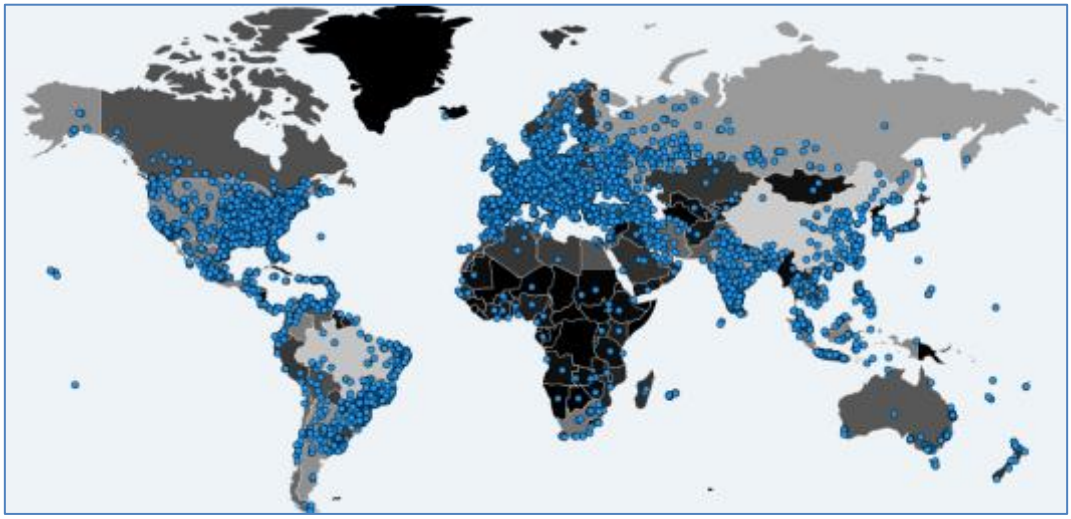
Publication du code source de Mirai et du tutoriel associé sur Hack Forums par Anna-senpai

Au plan technique, Mirai est unique en son genre tout en étant relativement simple à opérer :

[18] https://www.schneier.com/blog/archives/2016/09/someone_is_lear.html

- Dans un premier temps, le malware scanne de manière continue des adresses IP liées à des appareils IoT en recherchant des services d'administration associés (Telnet) ;
- Le malware tente ensuite d'en prendre le contrôle en tentant une authentification reposant sur une liste de couples identifiant / mots de passe par défaut ;
- Les périphériques vulnérables sont par la suite compromis par le logiciel malveillant qui les transforme en bots et les force à se connecter à un C&C. Ces mêmes périphériques suivent le même cycle d'infection en tentant de compromettre d'autres équipements IoT ;
- Le C&C peut alors être utilisé comme point de départ par un pirate pour lancer de puissantes attaques DDoS conçues pour mettre hors ligne des infrastructures robustes. D'autres fonctionnalités sont offertes comme celle de proxy ou de vecteur de spam.

Suite à cet événement, le nombre de botnets utilisant Mirai explosa. Au moment de la diffusion du code source, la société Level 3 estimait que le nombre de machines infectées par Mirai s'élevait à environ 213 000. Trois semaines plus tard, cette même société publia un nouveau rapport en évaluant la taille totale des botnets Mirai à plus de 500 000 appareils[19]. Ainsi, de multiples réseaux malveillants ont émergé dans les jours qui ont suivi. Un phénomène que deux chercheurs en sécurité informatique (*2sec4u*[20] et *MalwareTech*[21]) suivent et dont ils analysent l'ampleur sur le compte Twitter @MiraiAttacks[22] et le site web dédié MalwareTech Botnet Tracker[23]. D'après eux, la plupart des botnets suivis sont d'une taille relativement petite mais il en existe un qui se démarque de ses semblables, en ceci qu'il se caractérise par un nombre de bots supérieur à celui de tous les autres botnets cumulés[24].



Répartition des machines appartenant aux botnets Mirai

Le développement des botnets Mirai entraina également une hausse des attaques associées. Le 21 octobre 2016, le service *Dyn Managed DNS* géré par la société DynDNS fut ainsi la cible d'une attaque par dénis de

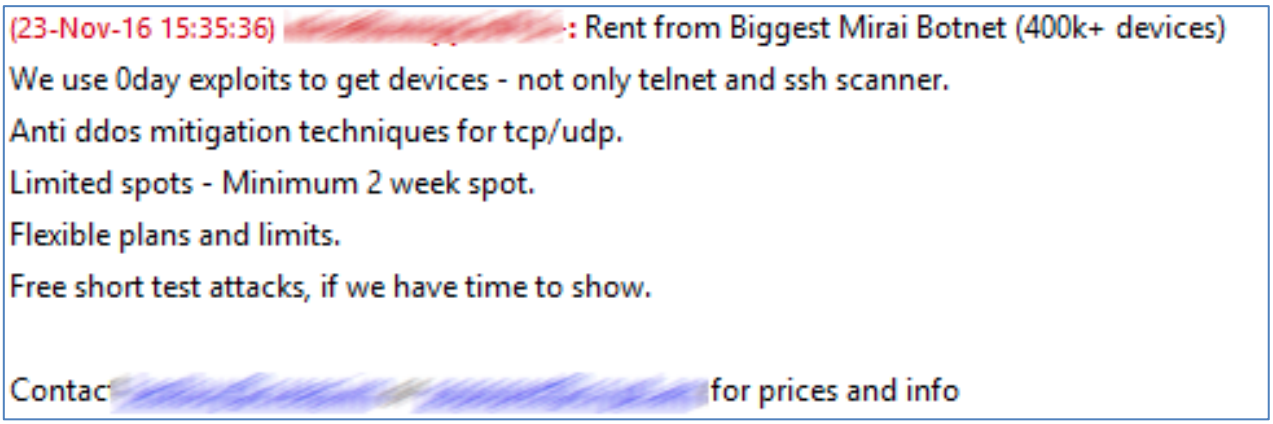
[19] http://blog.level3.com/security/grinch-stole-iot/
[20] https://twitter.com/2sec4u
[21] https://twitter.com/MalwareTechBlog/
[22] https://twitter.com/MiraiAttacks
[23] https://intel.malwaretech.com/botnet/mirai
[24] https://twitter.com/MalwareTechBlog/status/801187034672939008

service massive de plus d'un téraoctet par seconde. Les dommages collatéraux furent conséquents : de nombreux sites utilisant le service, tels que Twitter, Ebay, Netflix, GitHub ou PayPal, furent inaccessibles pendant une dizaine d'heures. Le Liberia fut également paralysé par une attaque DDoS qui cibla les compagnies télécom du pays, surchargeant ainsi l'unique câble sous-marin reliant le pays au reste du réseau Internet (d'une capacité de 500 Gbps). Les 22 et 24 octobre 2016, StarHub, l'un des principaux fournisseurs singapouriens d'accès à Internet, fut touché par deux vagues de cyberattaques provenant d'appareils IoT compromis.

Diversification des services cybercriminels basés sur le code source de Mirai

La diffusion du code source de Mirai a donc permis de déployer des réseaux de machines zombies de manière simple et efficace. Face à cette « opportunité », deux types d'acteurs malveillants se sont distingués : d'un côté, les pirates qui mènent des attaques informatiques pour leur propre compte et, de l'autre, ceux qui développent leurs activités en louant une partie de leur infrastructure.

Deux personnages du monde *underground* ont ainsi récemment proposé – via une campagne de spam sur XMPP/Jabber – de louer des services d'attaques de type DDoS menées à partir de leur propre botnet basé sur le malware Mirai qui serait composé d'environ 400 000 machines zombies :



Spam diffusé via XMPP/Jabber proposant la location d'un botnet basé sur Mirai

Les deux cybercriminels derrière cette campagne, *BestBuy* et *Porpopret,* sont bien connus des communautés *underground*. Ils ont notamment commercialisé le malware GovRAT 2.0 sur le marché noir *TheRealDeal* et ont été très actifs sur le forum de piratage *Hell*. Deux journalistes du site Bleeping Computer ont réussi à échanger avec ces pirates et à obtenir plus de précisions quant à leur service de location de botnet basé sur Mirai[25] :

- Aucun minimum n'est requis en termes de nombre de bots lors du lancement d'une attaque mais cette dernière doit se dérouler au moins sur un laps de temps de 2 semaines ;
- Le prix est déterminé par le nombre de bots, la durée, le temps entre deux attaques consécutives (aussi appelé *cooldown time*) ;

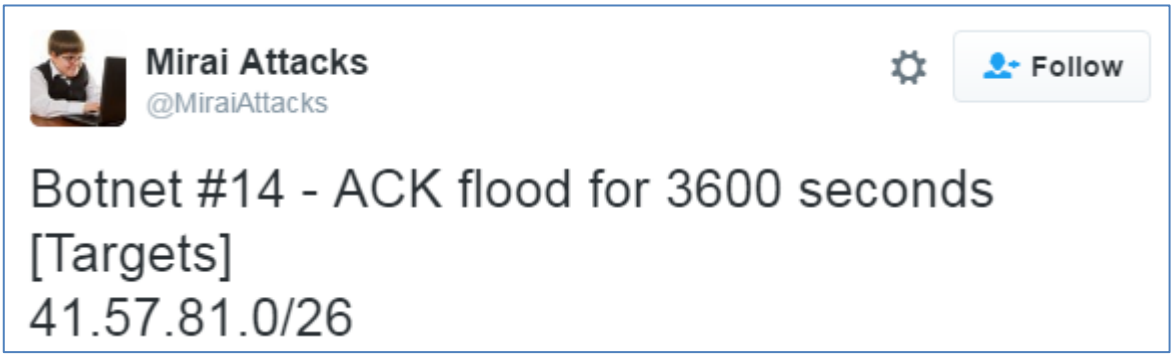
[25] http://www.bleepingcomputer.com/news/security/you-can-now-rent-a-mirai-botnet-of-400-000-bots/

- Les clients n'obtiennent de réduction que s'ils espacent la durée entre deux attaques et non sur le nombre de bots loués ;
- À titre indicatif, sur deux semaines, le prix d'une attaque menée à partir de 50 000 bots pendant une période d'une heure avec un *cooldown time* de 5-10 minutes est estimé entre 3 000 et 4 000 dollars ;
- Une fois l'accord établi entre l'acheteur et l'offreur, ce dernier fournit une URL en .onion (réseau Tor) permettant d'accéder à l'interface d'administration du botnet.

Selon le chercheur en sécurité *2sec4u*, *BestBuy* et *Porpopret* ont ajouté des fonctionnalités majeures au malware Mirai originel :

- Ce dernier se limitait à environ 200 000 machines, Internet ne disposant que d'un nombre limité d'appareils connectés proposant une administration via Telnet. En outre, le malware originel ne testait qu'une liste de 60 combinaisons identifiants/mots de passe. Les cybercriminels ont donc ajouté l'option de force brute via SSH faisant passer le botnet à environ 400 000 machines ;
- Leur malware serait capable d'exploiter des failles dites 0day. Cette hypothèse n'est cependant pas encore confirmée car aucune rétro-ingénierie n'a pu être effectuée ;
- Le botnet a la possibilité de passer outre les solutions anti-DDoS en usurpant/faussant les adresses IP de ses bots.

Le chercheur *2sec4u* pense que le botnet déployé par *BestBuy* et *Porpopret* serait celui responsable de l'attaque ayant paralysé le Liberia. Son compte Twitter @MiraiAttack – qui recense les attaques DDoS menées à partir des botnets Mirai – le répertorie sous l'appellation *Botnet #14 :*

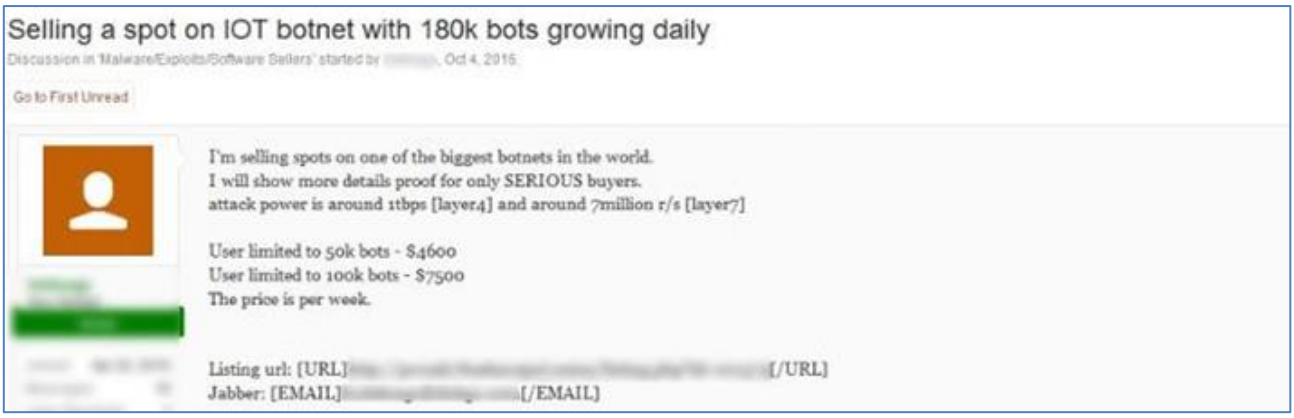


Recensement d'une attaque menée par Botnet #14 sur 41.57.27.0/26 appartenant à la société libérienne Lonestar Cell

Suite à une conversation privée avec les cybercriminels, les journalistes du site Bleeping Computer n'ont pas réussi à obtenir une démonstration des capacités du botnet. Les pirates ont cependant spécifié qu'ils avaient eu accès au code source de Mirai bien avant qu'il ne soit rendu public par *Anna-senpai*.

Outre les messageries instantanées, les cybercriminels ont également fait appel aux plateformes du Dark Web pour développer leurs activités liées au malware Mirai. Le fameux marché noir anglophone AlphaBay présent sur Tor a ainsi récemment vu l'émergence d'offres de location d'attaques DDoS reposant sur des botnets Mirai. Le 4 octobre 2016, le vendeur *loldongs* proposait par exemple dans une annonce son service de DDoS disposant d'une force de frappe de 1 Tbps (équivalent de l'attaque contre OVH) grâce à la location

partielle ou totale de son infrastructure de 50 000 (4 600 dollars) ou 100 000 bots (7 500 dollars) pour deux semaines :



Annonce du vendeur loldongs postée sur le marché noir AlphaBay

Dans une publication sur le forum annexé au marché noir AlphaBay, *loldongs* donnait plus de précisions sur son service. Il y indiquait notamment être capable de s'attaquer et de mettre à mal une cible de la taille d'OVH et avoir développé son malware à partir du code source de Mirai :

Publication de loldongs postée sur le forum d'AlphaBay

La diffusion du code source du malware Mirai a donc d'importantes répercussions en matière de cybersécurité.

Les experts de l'IoT – notamment ceux du CERT-UBIK – prévoient tout d'abord de réelles évolutions techniques, notamment sur les méthodes d'infection via les réseaux pair-à-pair (composés de caméras connectées, Digital Video Recorders et d'alarmes connectées). Ces réseaux P2P permettent à l'attaquant de cibler un ensemble d'équipements connectés. Par ailleurs, certains réseaux qui interconnectent des millions d'objets sur les serveurs reposent sur des protocoles propriétaires peu testés et peu ou pas sécurisé.

Les experts s'attendent également à l'apparition de nouveaux types d'attaques à partir des équipements IoT : les malwares seront persistants (via l'utilisation de l'espace de stockage) et non plus supprimés à chaque redémarrage de la machine. Ils seront aussi utilisés dans le cadre d'attaques ciblées (appelées

également APT), via l'exploitation de portes dérobées et de failles applicatives. Ils permettront en outre d'employer les équipements compromis à d'autres finalités, comme l'hébergement de sites malveillants ou bien la diffusion de malware.

La **Direction Générale des Relations Internationales et de la Stratégie (DGRIS)** 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 **DGRIS** a confié à **CEIS** la réalisation de 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
Direction Générale des Relations Internationales et de la Stratégie
60 Boulevard du Général Martial Valin – CS21623 – 75 509 Paris Cedex 15

CEIS
Tour Montparnasse – 33, avenue du Maine – BP 36 – 75 755 - Paris Cedex 15
Téléphone : 01 45 55 00 20
E-mail : omc@ceis-strat.com