Botnets : illustration de nouvelles formes de criminalité organisée

Éric Freyssinet

Botnets : illustration de nouvelles formes de criminalité organisée

Éric Freyssinet

Le botnet constitue la manifestation la plus courante de la délinquance numérique sur Internet. Encore mal connu, l'étude de ces objets, la façon dont ils sont conçus, mis en place, administrés et utilisés permettent de mettre en lumière de façon très claire l'arrivée de nouvelles formes de délinquance organisée. Essayons de voir ce que l'univers des botnets et le véritable écosystème qui s'est créé autour d'eux offrent comme potentialités quant à l'identification de groupes criminels organisés : il s'agit bien d'une véritable professionnalisation de ces formes modernes de délinquance. Enfin, nous les confronterons aux définitions classiques de la criminalité organisée et conclurons à la nécessité de les faire évoluer et même d'adapter les outils utilisés pour y répondre.

1. Introduction et définitions

1.1 Les botnets

Reprenons la définition que nous avons construite sur le Wiki botnets.fr [BOT2012] :

Un botnet est un ensemble constitué par des systèmes compromis (appelés alors *bots*) qui, lorsqu'ils sont connectés à Internet, communiquent avec un système de commande et de contrôle donné.

La compromission évoquée ici est l'installation d'un logiciel malveillant, quel qu'en soit le mode de diffusion, qui directement fait communiquer le système compromis avec le système de commande et de contrôle ou entraîne l'installation d'un module qui permet cette communication.

Un botnet peut être ainsi constitué:

- d'un parc homogène ou hétérogène de machines, selon que le ou les logiciels malveillants utilisés pour le constituer sont capables de contaminer un ou plusieurs types de système d'exploitation. Il s'agit en général de postes de travail informatiques, mais il peut aussi s'agir de serveurs ou de téléphones mobiles.
- d'un nombre extrêmement variable de *bots*, qui évolue selon la connexion à Internet des machines ou la persistance de la contamination sur chaque système.

En théorie donc, une même classe de botnets pourra recouvrir plusieurs évolutions dans l'existence d'un botnet :

- selon l'évolution du système de commande (pour des raisons internes, par exemple si le développeur du système décide de le modifier ou pour des raisons externes, si des infrastructures utilisées pour le piloter voient leur fonctionnement empêché par une action judiciaire).
- selon les variantes de logiciel malveillant utilisé, qui peut permettre de construire un botnet unique ou plusieurs botnets correspondant à chaque grande version.
- selon l'organisation du botnet, qui peut être découpé en différents réseaux, utilisés pour différents usages, par exemple loués à différents clients.

1.2 Les catégories de botnets

On peut regrouper les botnets dans plusieurs grandes catégories qui vont parfois se recouvrir, les fonctionnalités étant parfois communes à différentes familles et l'intention de ceux qui les développent étant parfois multiples.

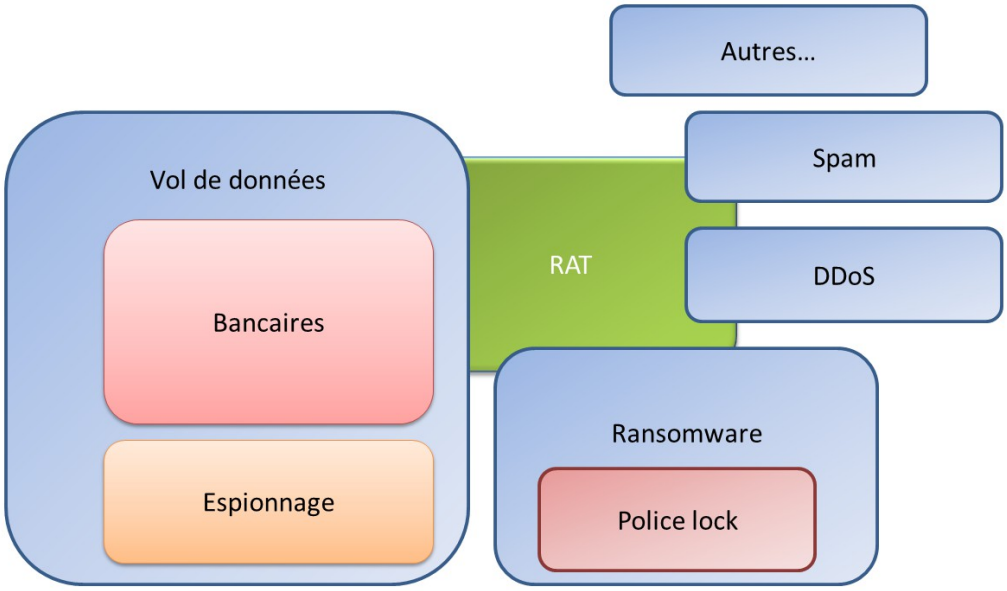

Fig. 1 : Les différentes catégories de botnets

- Vol de données :
  - Données bancaires (numéros de carte bancaire, identifiants de compte bancaire en ligne, détournement de session de connexion à un compte bancaire en ligne, etc.) ;
  - Espionnage d'informations confidentielles ou sensibles ;
- Le spam ou courrier électronique non sollicité, qui ne se limite pas à la prospection commerciale illégale tel que l'encadre la loi pour la confiance dans l'économie numérique mais peut relayer différents messages malveillants ou tentatives d'escroquerie par exemple ;
- Les attaques en déni de service distribué (DDoS = *distributed denial of service*) qui ont pour objectif de rendre inaccessible une connexion ou un serveur sur Internet et qui sont grandement facilitées par l'utilisation d'un botnet qui peut rassembler plusieurs centaines de milliers de machines ;
- Les rançongiciels dont le principe est de bloquer l'utilisation de l'ordinateur (ou du téléphone) de la victime et réclamer le paiement d'une rançon, avec la variante particulièrement prisée ces deux dernières années qui consiste à se faire passer pour un message légitime d'un service de police et réclamer le paiement d'une amende ;
- Les RAT (*remote administration trojans*) dont la particularité est de regrouper en un seul outil tout un tas de fonctionnalités qui pourraient ressembler à un outil d'aide à distance, mais qui permettent en réalité de réaliser de nombreuses actions malveillantes : activation de la caméra vidéo, enregistrement de copies d'écran, copie de fichiers, enregistrement de mots de passe, etc... Ils sont autant utilisés par des entreprises d'espionnage que par de jeunes délinquants à la recherche de sensations fortes – certains publient des enregistrements vidéo de leurs exploits sur Internet où ils se moquent de leurs victimes qu'ils surprennent dans leur initimité ;
- Enfin, d'autres usages plus spécifiques sont rencontrés mais sont plus isolés (comme le cas de Sality décrit plus bas).

1.3 Comment les botnets sont diffusés et administrés

Les grandes étapes de la vie d'un botnet sont les suivantes :

- le développement des programmes informatiques (le virus ainsi que le logiciel qui va permettre au serveur de commande et de contrôle de fonctionner) ;
- la diffusion du virus – et donc la contamination d'un nombre suffisamment important ou ciblé de machines ;
- l'installation du serveur (ou de l'infrastructure dans les cas plus complexes) de commande et de contrôle ;
- la gestion et le suivi du botnet, l'envoi de commandes ;
- la fin de vie du botnet qui passe parfois par sa désinstallation sur l'ordinateur des victimes ou sur les serveurs de commande et de contrôle.

La phase de diffusion du virus est une des plus importantes et peut mettre en œuvre, voire combiner différentes méthodes :

- l'installation directe ou par ruse (certains ont laissé traîné des clés USB sur les parkings de certaines entreprises dans le but d'y installer des virus par l'action maladroite d'employés) ;
- l'envoi de pièces jointes piégées par courrier électronique (on parle de spear phishing lorsque cette opération cible une personne ou un groupe de personnes bien spécifique, notamment pour les opérations d'espionnage) ;
- la contamination par l'exploitation de vulnérabilités lors de l'utilisation d'un protocole de communication Internet et en particulier au travers des navigateurs Web : les victimes sont dirigées par des liens, de fausses bannières publicitaires ou du code malveillant inséré frauduleusement dans des sites Web légitimes vers des sites Web particuliers, les plates-formes d'exploits (voir le paragraphe suivant).

1.4 Les plate-formes d'exploits

Les plate-formes d'exploits sont donc des sites Web dynamiques permettant de tester un certain nombre de vulnérabilités[1] sur les machines qui les visitent. Elles disposent d'une interface de commande dans laquelle en général chaque client (ici un délinquant) dispose d'un identifiant et peut gérer lui-même ses campagnes de contamination. Pour chacune d'entre elles il dispose d'une URL[2] dédiée sur laquelle il va chercher à diriger le trafic des futures victimes (cette URL contient un paramètre spécifique à la campagne de diffusion d'un virus particulier). On a donc ici trois acteurs immédiats : celui qui développe et commercialise le logiciel, celui qui administre un serveur, le tient à jour et enfin celui qui loue ces ressources auprès de ce dernier. Parfois les rôles peuvent évidemment coïncider au sein des mêmes équipes.

La plus connue de ces plates-formes est peut-être Blackhole Exploit Kit mais il en existe plus d'une vingtaine d'autres. [PAR2012] présente une table des capacités de chacune d'entre elles : elles se distinguent en particulier par l'intégration de méthodes permettant d'exploiter un maximum de vulnérabilités dans les logiciels les plus courants. En général ce sont les navigateurs Web qui sont ciblés (Internet Explorer, Chrome, Firefox, ...), des composants additionnels (en particulier Adobe Flash, Adobe Acrobat Reader ou encore Java), voire les systèmes d'exploitation eux-mêmes. Tout comme les virus c'est le plus souvent Microsoft Windows qui est ciblé, mais d'autres systèmes d'exploitation sont parfois concernés.

1.5 Confrontation de la notion de criminalité organisée aux enjeux de la cybercriminalité.

Avant de montrer plus concrètement les formes de criminalité organisée rencontrées, revenons rapidement sur les bases juridiques qui s'appliquent en France. Dans [ZEK2007], le constat est assez négatif quant à l'adaptation des outils de la criminalité organisée aux défis de la délinquance informatique. Quelques remarques sur l'adéquation des définitions juridiques :

- la notion de délit en réunion ne s'applique à aucune des infractions spécifiques à la cybercriminalité ;
- la circonstance aggravante de la bande organisée peut parfois être retenue, par exemple pour les infractions d'escroqueries ;
- l'association de malfaiteurs est pleinement applicable ; ainsi l'article 323-4 du code pénal réprime spécifiquement la participation à une association de malfaiteurs visant à commettre des délits d'atteinte aux systèmes de traitement automatisé de données ;
- au titre de l'article 706-73 du code de procédure pénale on peut appliquer des possibilités supplémentaires en matière d'outils d'investigation spécifiques à la lutte contre la criminalité organisée : les crimes aggravés d'extorsion, les escroqueries commises en bande organisée, le blanchiment du produit de ces infractions ou l'association de malfaiteurs en vue de leur commission ;
- de même, on pourra parfois appliquer l'extension de ces dispositions spécifiques tel que le prévoit l'article 706-74, à savoir la compétence des juridictions interrégionales spécialisées ou l'ordonnance de mesures conservatoires permettant de préserver les biens d'un suspect en vue du paiement d'amendes ou de réparations aux victimes.

On a donc une couverture juridique partielle des pratiques cybercriminelles. En réalité, nous allons voir, au travers de quelques exemples concrets que non seulement les infractions spécifiques à la cybercriminalité ne sont pas forcément ciblées par les outils procéduraux de lutte contre la criminalité organisée, mais peut-être faudrait-il revoir la définition ou l'interprétation qui permet d'appliquer ces circonstances, certaines formes d'organisation étant particulièrement modernes et difficiles à mettre en évidence de prime abord.

2. Quelques cas concrets récents

Les botnets constituent un terrain particulièrement riche pour l'observation d'interactions entre personnes qui se coordonnent et se rendent des services pour la commission d'infractions. Analysons quelques exemples récents et leurs caractéristiques organisationnelles et parfois quasi-professionnelles.

2.1 KoobFace

Commençons par un exemple original. Apparu en 2008, KoobFace est un ver[3] dont la particularité est qu'il utilise des comptes de réseaux sociaux pour se propager, d'où son nom construit d'après Facebook. Parmi ses autres particularités, il utilise un réseau de commande et de contrôle basé sur un protocole pair à pair – donc non centralisé – et cible aussi bien les ordinateurs fonctionnant sous Microsoft Windows que MacOS X ou encore Linux. Une fois installé sur la machine victime, il collecte des identifiants de connexion à différents services sur Internet, installe d'autres virus et participe au réseau pair à pair de commande et de contrôle.

Selon différentes sources, dont la société Facebook qui cherche à les faire tomber, il serait le projet de cinq habitants de Saint-Petersbourg en Russie. Ainsi, en janvier 2012, la société Sophos publiait une synthèse des découvertes réalisées sur cette équipe [SOP2012]. Il est intéressant de souligner que beaucoup des informations sur les suspects ont été trouvées sur des réseaux sociaux. Leurs activités seraient hébergées derrière plusieurs sociétés légalement établies à Saint-Pétersbourg et en République Tchèque : c'est dans les registres officiels qu'une partie de l'information sur ce groupe a pu être découverte.

On a donc ici un botnet assez complexe, qui serait construit et géré par une petite équipe qui s'est révélée relativement facile à identifier et les noms des suspects ont été rendus publics... ils n'ont toutefois pas encore été interpellés.

2.2 Les botnets bancaires

ZeuS était peut-être le plus célèbre des botnets bancaires, mais il existe une variété assez impressionnante de botnets dont la vocation est de détourner des données bancaires : Citadel, Gozi, SpyEye, Tilon ou encore Carberp sont quelques-uns des noms rencontrés. Ceux qui les développent sont particulièrement inventifs : non seulement ils sont capables de copier des mots de passe d'accès à des comptes bancaires ou des numéros de cartes bancaires, mais ils interagissent avec le navigateur de l'ordinateur infecté, dans lequel ils remplacent à la volée le programme légitime qui sert à afficher le contenu (HTML, JavaScript) téléchargé depuis le site bancaire, par du code malveillant, pour s'attaquer à la sécurité des claviers virtuels ou encore passer des ordres de virement au travers de la connexion établie par l'utilisateur légitime. Ainsi, Amit Klein décrit dans [KLE2012] comment le botnet Tatanga se déjoue des protections par mot de passe à usage unique en faisant réaliser au consommateur des opérations qui semblent lui être demandées par sa banque.

Il s'agit souvent pour les groupes qui utilisent ces botnets de cibler différentes banques, dans différentes régions du monde. On peut certainement supposer que certains développeurs se sont spécialisés dans la conception des fichiers de configuration qui permettent de capturer grâce à l'insertion de code Javascript les identifiants de connexion bancaire ou d'interagir dynamiquement avec la session de l'utilisateur. Ils commercialisent certainement ces fichiers à des groupes exploitant des botnets bancaires différents. Ces fichiers de configuration sont en général téléchargés dans un fichier texte et ils sont vraisemblablement interchangeables ou facilement réadaptables (certains réutilisent par exemple le format de fichiers de configuration mis en place pour ZeuS/SpyEye, comme le démontrent [BOU2012] et [BOU2012-2]).

2.3 Le cas Citadel

Citadel est un exemple de botnet bancaire dont l'utilisation réelle et le comportement de ses diffuseurs est intéressant à étudier. Dans [FRE2012] nous faisions le point sur l'avènement d'un nouveau botnet dont la commercialisation se développait alors. Les observateurs avaient identifié plusieurs caractéristiques intéressantes de ce botnet ciblant d'abord les clients de banques en ligne : des messages publicitaires sur les forums criminels, des horaires de bureau pour les équipes en contact avec leurs clients (entre 10h00 et 0h30 les jours de semaine), des mises à jour hebdomadaires et de nombreuses options vendues séparément du produit basique. Dans un papier plus récent [KES2012], Limor Kessem souligne par exemple une nouvelle fonctionnalité permettant au maître d'un botnet d'ouvrir jusqu'à cinq comptes pour des prestataires externes qui développeraient et implémenteraient pour lui des scripts spécifiques selon ses cibles.

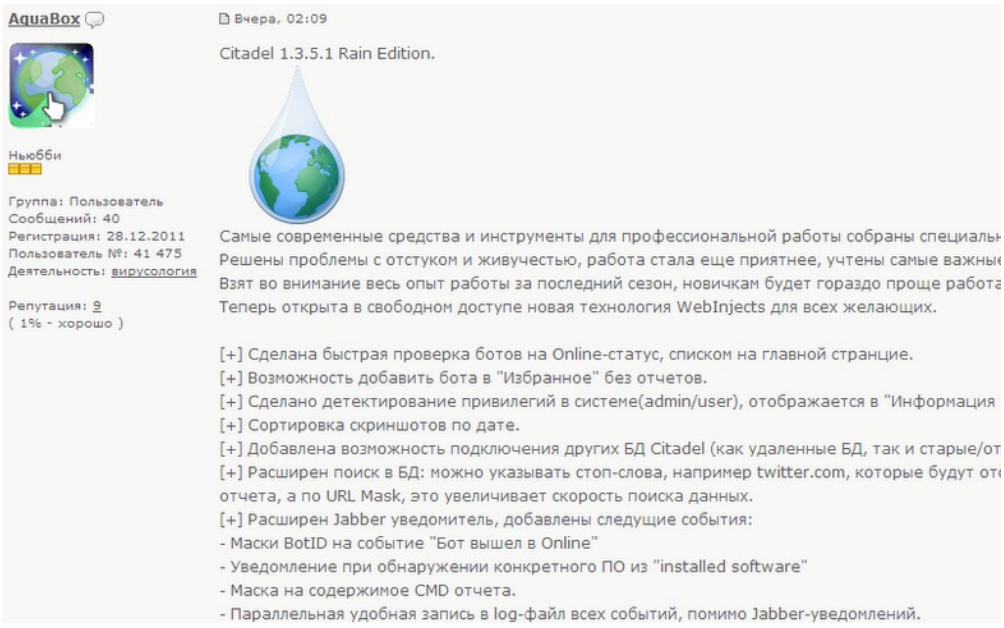

Fig. 2 : Annonce en octobre 2012 de la toute dernière version du botnet Citadel sur un forum cybercriminel – Copie d'écran par @Kafeine

En plus d'être une trousse à outils particulièrement développée, Citadel se fait remarquer pour être un des modes de diffusion privilégiés du rançongiciel Reveton (voir plus bas le paragraphe sur les rançongiciels) lorsqu'il cible des victimes américaines dans différentes messages d'alerte diffusés par le FBI [ICC2012].

On note donc ici une organisation quasi-professionnelle et l'utilisation des codes et des pratiques de l'univers du commerce classique : publicité, contact privilégié avec le client et gestion d'un service après-vente.

2.4 Utilisation du botnet Sality pour scanner l'Internet

Sality est un autre de ces botnets trousse à outils. Il serait apparu des 2003 en Russie et reste toujours très présent sur Internet. Dans un article publié récemment [DAI2012], des chercheurs ont démontré qu'en février 2011, sur une période de 12 jours, le botnet Sality avait été utilisé pour explorer de façon relativement discrète 3 millions d'adresses IP[4] à la recherche de serveurs de téléphonie sur IP, vraisemblablement à la recherche de vulnérabilités exploitables. Les personnes qui gèrent le botnet ont-elles vendu ce service à un client ? Ou l'ont-elles fait de leur propre initiative pour revendre ensuite les résultats ou bien les utiliser par elles-mêmes ?

En tout état de cause, la démonstration de cet usage permet de souligner la variété des usages quasi professionnels des botnets aujourd'hui.

2.5 Les botnets spécialisés dans le spam

Ils sont les plus connus et peut-être ceux qui concernent le plus d'internautes : nous recevons tous du courrier électronique non sollicité et une grosse partie de celui-ci provient de botnets. Ils ont pour noms Mega-D, Rustock ou encore Waledac. Leur fonctionnement est parfaitement professionnalisé, que les activités dont ils assurent la promotion soient à la limite de la légalité ou complètement illégales.

Ainsi, *Reactor Mailer* était le produit phare de la société Elphisoft et se présentait comme un réel service de distribution commerciale de courriers électroniques. Son argumentaire publicitaire présentait sa technologie sous le titre : « Mass Mailing Cluster System Reactor Mailer ».

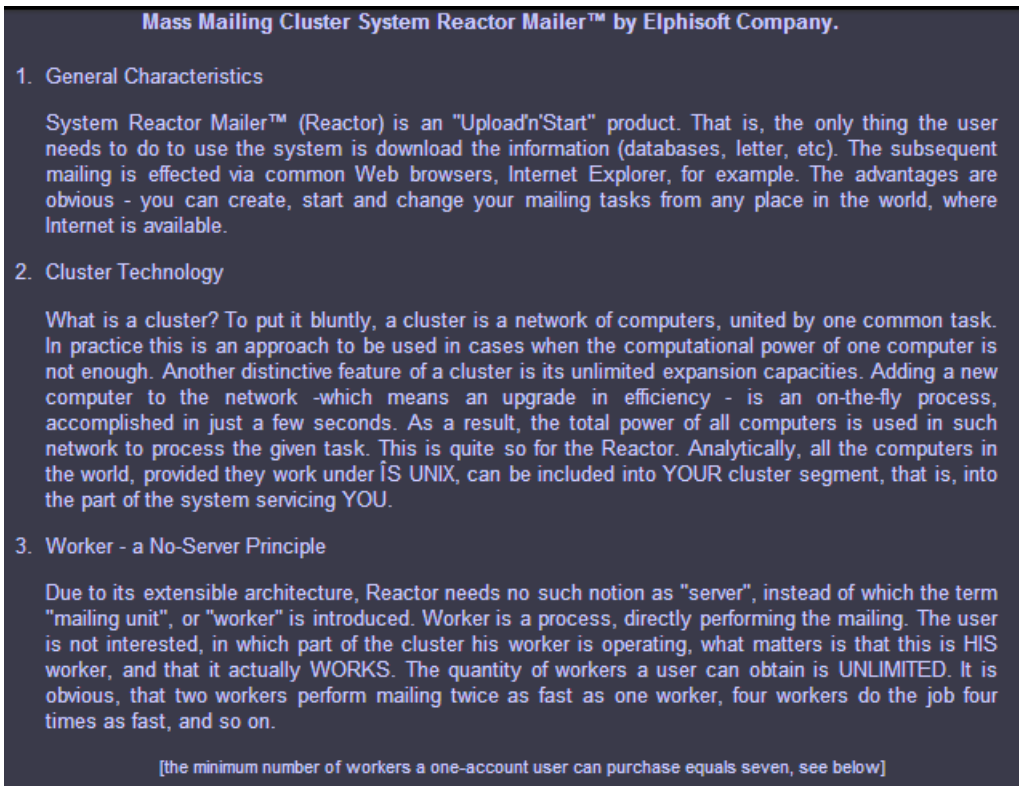

Fig. 3 : Copie d'écran de l'argumentaire commercial de Reactor Mailer, tel qu'on le retrouve encore aujourd'hui sur archive.org

Avant sa disparition en même temps que son hébergeur McColo[5], *Reactor Mailer* offrait une interface Web assez similaire en fonctionnalités à ce que mettent en place les véritables spécialistes de l'émission de prospection commerciale légale. Il était possible d'y télécharger les modèles de messages, les listes de prospects et déclencher ainsi les campagnes d'emailing. Au début Elphisoft passait vraisemblablement par des proxies (serveurs utilisés comme relais) pour diffuser son spam de façon plus discrète et efficace, puis est apparu Srizbi, un botnet permettant de distribuer plus efficacement et plus discrètement les campagnes.

Pour diffuser le logiciel malveillant de Srizbi, Elphisoft a notamment utilisé le kit d'exploits MPack [KEI2007]. Des liens vers des plates-formes d'infection MPack étaient diffusées par le botnet lui-même dans des courriers non sollicités promettant par exemple des vidéos de célébrités.

2.6 Les botnets d'espionnage

Ils défraient la chronique depuis quelques années et les éditeurs de solutions de sécurité rivalisent parfois de précipitation pour publier une nouvelle alerte sur des campagnes d'attaque en profondeur (ou autres APT) dans des réseaux d'entreprises ou d'administrations. Souvent l'objectif semble être de dérober de l'information, parfois il pourrait s'agir d'altérer le fonctionnement des systèmes. Ils s'inspirent des outils d'administration à distance malveillants (RAT) mais poussent le concept beaucoup plus loin.

Pour extraire de l'information, les campagnes découvertes révèlent à la fois une certaine ingéniosité et en même temps une très nette opiniâtreté et des moyens certainement très importants. En effet, une fois une première machine infectée dans le réseau d'une entreprise, elle est littéralement pilotée à distance par les attaquants qui cherchent à découvrir le réseau, puis de proche en proche à infecter de nouvelles machines, prendre le contrôle de serveurs gérant des domaines Windows ou encore parcourir les partages réseau. Cela suppose des équipes capables d'interagir directement avec les systèmes ciblés, de connaître différents types de systèmes ou de configuration et enfin de paramétrer finement des techniques qui pourront être adaptées à chaque type de réseau pour exfiltrer discrètement l'information.

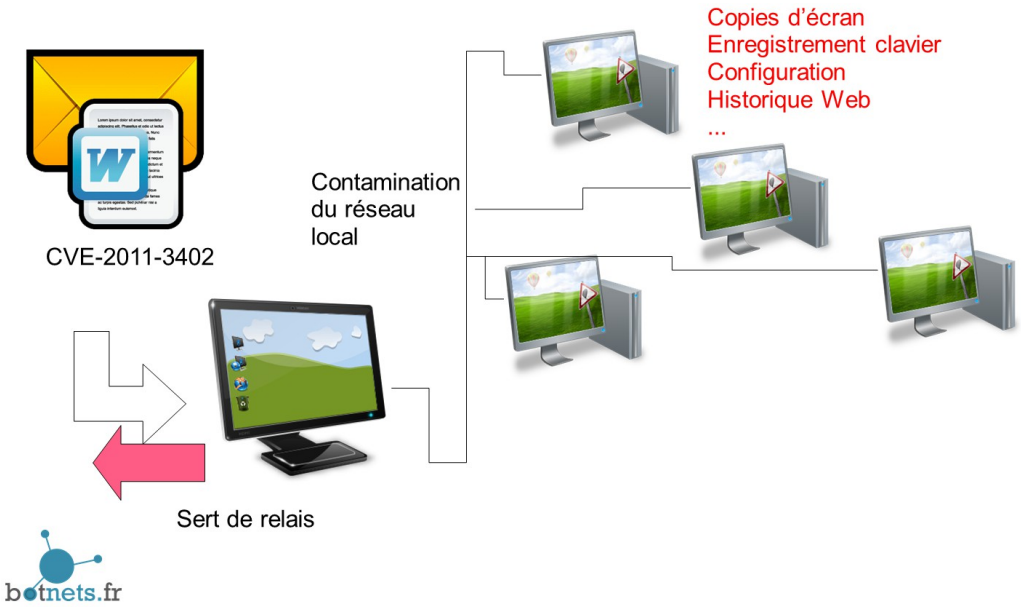

Fig. 4 : Fonctionnement de certaines attaques avec Duqu (botnets.fr d'après informations publiées par Kaspersky Lab)

Très souvent dans ce type d'attaque, les chercheurs découvrent qu'une vulnérabilité de type 0-day[6] a été exploitée : cela suppose donc aussi d'avoir les moyens d'acheter ou de rechercher ce type de faiblesse pour les exploiter sur la cible. Enfin des infrastructures dédiées sont parfois mises en place pour chacune des cibles [NAR2011].

Dans une série d'attaquées similaire révélée au mois de mai 2013, les chercheurs ont découvert que le logiciel malveillant (appelé HangOver/Hanove ou Kitmos) s'installait avec un certificat de sécurité produit par une société indienne et les infrastructures permettant de gérer le fonctionnement du botnet d'espionnage étaient elles aussi liées à une entreprise indienne [NOR2013].

Il se confirme donc de plus en plus que ce type d'activités s'inscrit clairement dans la guerre économique entre les entreprises ou entre les États. Non seulement les groupes qui sont derrière sont très professionnels dans leur comportement, mais aussi dans leur organisation, voire leur structure juridique, avec ou sans la complicité supposée – voire la clientèle – des États qui les hébergent.

2.7 Les rançongiciels

L'observation des rançongiciels, dont vous trouverez de nombreux exemples sur le site géré par la communauté botnets.fr[7], nous a permis d'approcher une partie de la complexité des schémas collaboratifs qui se sont mis en place progressivement. On retrouve autour de ces types de botnets toutes les catégories d'acteurs. Le schéma ci-dessous synthétise nos observations, mais d'autres niveaux de complexité peuvent exister, par exemple comme autour des plates-formes d'exploits comme évoqué plus haut.

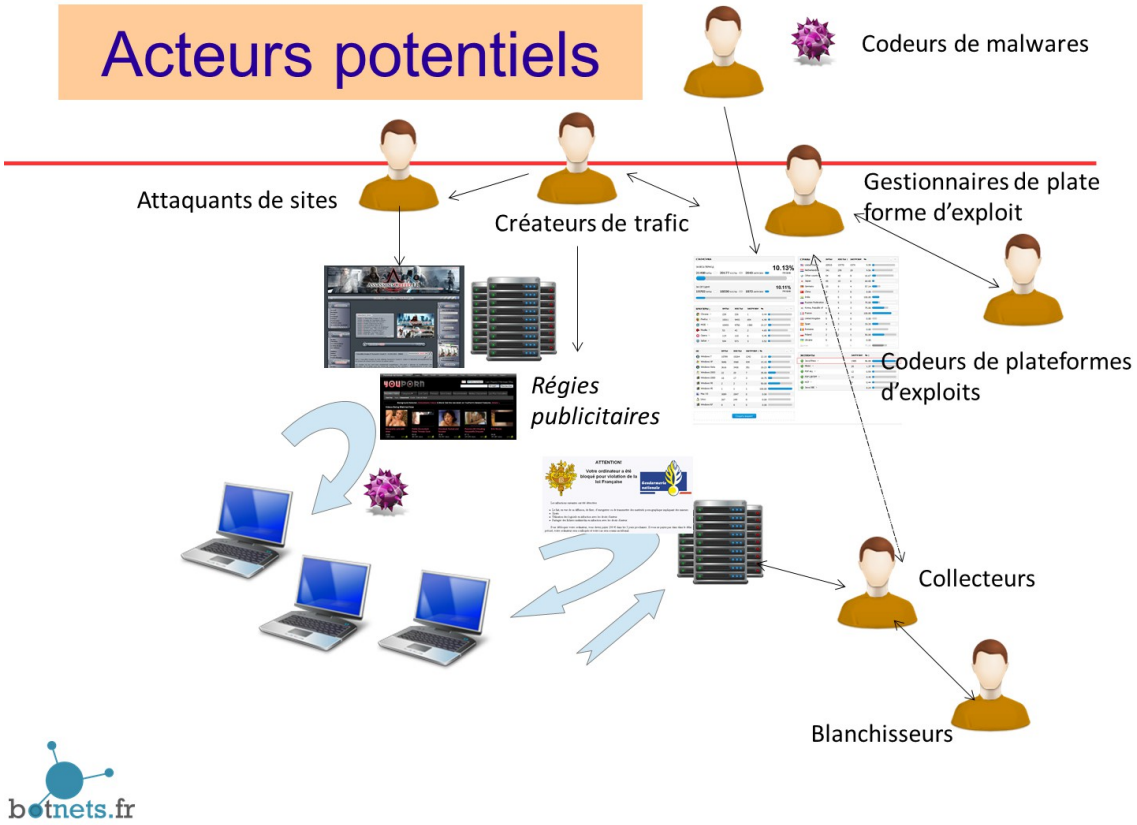

Fig. 4 : Schéma de fonctionnement des attaques de rançongiciels policiers (botnets.fr)

Ainsi, celui qui souhaite déployer une campagne pour ce type de botnets va faire appel aux prestataires suivants :

- des créateurs de trafic (*traffers* dans le jargon) : ils vont attirer des visiteurs, éventuellement par types de pays, soit par injection d'IFRAMEs[8] piégées dans des bannières publicitaires ou directement dans le code de sites Web dont ils auront pris le contrôle (ou demandé à d'autres prestataires criminels d'en prendre le contrôle pour eux). Ce type de mécanisme peut fonctionner par affiliation, chaque affilié s'engageant à fournir différents types de sources de trafic. Une plate-forme intermédiaire (TDS – *traffic distribution systems* [DOS2011]) permet parfois de rediriger le trafic vers différents clients ;
- des exploitants de plates-formes d'exploits ;
- des développeurs de logiciels malveillants : dans le domaine des rançongiciels on observe actuellement beaucoup de kits à personnaliser (comme les Multi-lockers) ;
- des personnes qui vont blanchir les sommes collectées, en pratique dans ce cas racheter les codes fournis par les victimes qui ont acheté des tickets électroniques Ukash ou Paysafecard par exemple, et vont à leur tour les jouer sur des casinos en ligne ou faire des achats sur des sites de commerce électronique. A cet effet de nombreux intermédiaires se sont spécialisés dans l'achat et la revente de ces tickets en créant de véritables places de marché. On note au passage qu'une partie des personnes qui achètent ces tickets « d'occasion » ne le font pas forcément avec des intentions malveillantes mais uniquement pensant bénéficier d'un rabais sur le prix réel.

3. Conclusion

3.1 Les métiers

Dans [FRE2010] nous avions listé de façon préliminaire un certain nombre de métiers pressentis comme étant essentiels au fonctionnement des botnets. Force est de constater que cet univers est en réalité bien plus riche encore, les botnets ne pouvant fonctionner sans l'existence d'un écosystème autour.

Ces métiers criminels sont donc liés aux fonctions essentielles des botnets, mais aussi liés aux services nécessaires au fonctionnement ou à la diffusion d'un botnet. Parfois, ils pourront prendre des formes presque officielles, avec la création de véritables entreprises ou alors ils abuseront de véritables services offerts par des entreprises dont les systèmes sont mal surveillés, sécurisés ou dont les responsables sont peu

regardants sur leurs clients.

Nous avons ainsi observé dans les paragraphes précédents, en plus des pasteurs de botnets et autres codeurs : des traffers, des administrateurs de systèmes, des développeurs de fichiers de configuration, des découvreurs et des négociants de vulnérabilités 0-day ou encore de vraisemblables équipes chargées de piloter les attaques en profondeur. Si on regarde de façon plus large le paysage, on peut observer d'autres acteurs à la périphérie tels des personnes qui offrent des services de vérification de numéros de cartes bancaires pour ceux qui les achètent.

4.2 Quel impact sur l'action judiciaire et notre vision de la criminalité organisée ?

Pour les chercheurs, mais aussi pour les services de police et de justice chargés de mener des investigations, ce foisonnement et cette spécialisation des acteurs doit être considérée avec attention. En effet, il est important de comprendre quelles vont être les responsabilités des uns et des autres, mais il faudra aussi vraisemblablement adapter les méthodes.

Ainsi, ce type d'organisation crée trois types d'obstacles que l'enquête va devoir surmonter :

- une volonté manifeste de brouiller les pistes : plus il y a d'intermédiaires, plus il sera complexe de remonter la piste – cela veut dire qu'il faut peut-être ne pas toujours chercher à tirer le fil d'une affaire par une série de faits, mais prendre du recul et observer l'ensemble du phénomène ;
- les arborescences criminelles qui se forment à un instant donné peuvent changer d'heure en heure, au fur et à mesure qu'un acteur offre ses services ou fait appel à d'autres personnes, les recombinaisons sont presque infinies : peut-être faut-il parfois s'attaquer à l'un de ces métiers – et les groupes qui les exercent - plus qu'à un type de malveillance observée ;
- les rencontres entre les criminels et les affaires se font dans des espaces (des forums notamment, des contacts par des messageries instantanées) où beaucoup de services d'enquête n'ont pas légalement accès : **il est indispensable de permettre les enquêtes sous pseudonyme pour ce type d'infractions**.

Face à cette délinquance de masse qui concerne un nombre toujours plus important de victimes, peut-être faut-il changer la façon dont on recueille l'information auprès de celles-ci et ne pas forcément les soumettre à la nécessité de déposer une plainte dans les formes actuelles. En effet, ce qui intéresse les services spécialisés c'est d'avoir rapidement accès à l'information dont disposent les victimes sur les circonstances de leur mésaventure et en même temps d'en avoir une vision aussi large que possible. Cela pourrait être réalisé sur **des plates-formes de signalement en ligne**, les victimes étant éventuellement recontactées par la suite pour complément d'information ou lorsque leur situation est reliée à une enquête qui a abouti.

Enfin, les définitions actuelles de la criminalité organisée ne sont pas forcément adaptées à ce type de schémas : **on n'a pas affaire à des groupes criminels mais à un véritable écosystème criminel** et peut-être faudrait-il créer un critère supplémentaire pour la mise en œuvre des outils procéduraux dédiés à la criminalité organisée, celui d'un multiplicité d'acteurs se rendant mutuellement des services.

Éric Freyssinet, eric.freyssinet@m4x.org @ericfreyss http://blog.crimenumerique.fr/
Colonel de gendarmerie, chef de la division de lutte contre la cybercriminalité. Doctorant à l'Université Paris 6

[NOR2013] Unveiling an Indian Cyberattack Infrastructure - a special report, Snorre Fagerland, Morten Kråkvik, Jonathan Camp, Ned Moran, Norman, http://enterprise.norman.com/resource_center/unveiling_an_indian_cyberattack_infrastructure-a_special_report

[BOT2012] *Botnet*, Communauté Botnets.fr, https://www.botnets.fr/index.php/Botnet

[BOU2012] *Win32/Gataka banking Trojan – Detailed analysis*, Jean-Ian Boutin, ESET, http://blog.eset.com/2012/08/13/win32gataka-banking-trojan-detailed-analysis

[BOU2012-2] *Win32/Gataka – or should we say Zutick?,* Jean-Ian Boutin, ESET, http://blog.eset.com/2012/11/30/win32gataka-or-should-we-say-zutick

[DAI2012] *Analysis of a "/0" stealth scan from a botnet*, Alberto Dainotti, Alistair King, and Kimberly C. Claffy (CAIDA, UC San Diego) and Ferdinando Papale and Antonio Pescapè (University of Napoli Federico II), Proceedings of the Internet Measurement Conference, 14-16 novembre 2012

[FRE2012] *La citadelle du crime*, Éric Freyssinet, http://blog.crimenumerique.fr/2012/02/11/la-citadelle-du-crime/

[FRE2013] *L'écosystème des botnets : une nouvelle forme de criminalité organisée*, Éric Freyssinet, Magazine MISC n°65, Janvier/Février 2013

[ICC2012] *Citadel malware continues to deliver Reveton ransomware in attempts to extort money*, Internet crime complaint center (IC3), http://www.ic3.gov/media/2012/121130.aspx

[KES2012] *Citadel V1.3.5.1: Enter the Fort's Dungeons*, Limor Kessem, http://blogs.rsa.com/rsafarl/citadel-v1-3-5-1-enter-the-forts-dungeons/

[KLE2012] *Tatanga Attack Exposes chipTAN Weaknesses*, Amit Klein, http://www.trusteer.com/blog/tatanga-attack-exposes-chiptan-weaknesses

[PAR2012] *Common exploit kits poster*, Mila Parkour, http://contagiodump.blogspot.co.uk/2012/11/common-exploit-kits-2012-poster-based.html

[SOP2012] *The Koobface malware gang – exposed!,* Jan Drömer, Dirk Kollberg, Sophos, http://nakedsecurity.sophos.com/koobface/

[DOS2011] Web-Based Malware Distribution Channels: A Look at Traffic Redistribution Systems, Nishant Doshi, http://www.symantec.com/connect/blogs/web-based-malware-distribution-channels-look-traffic-redistribution-systems

[NAR2011] *Duqu FAQ*, Ryan Naraine, http://www.securelist.com/en/blog/208193178/Duqu_FAQ

[FRE2010] *Réflexions pour un plan d'action contre les botnets*, Eric Freyssinet, SSTIC 2010, https://www.sstic.org/2010/presentation/Reflexions_pour_un_plan_d_action_contre_les_botnets/

[KEI2007] Mpack installs ultra-invisible Trojan, Gregg Keizer, http://www.computerworld.com/s/article/9026323/Mpack_installs_ultra_invisible_Trojan

[ZEK 2007] *La notion de bande organisée en matière de criminalité informatique*, Alexis Zekri, Maxime Bernaudin et Dan Szwarc, http://www.e-juristes.org/la-notion-de-bande-organisee-en/

1 Une vulnérabilité dans un logiciel ou un matériel informatique est une faiblesse de conception ou d'implémentation qui rend possible des attaques informatiques pouvant nuire aux différents aspects de la sécurité d'un système d'information : sa disponibilité, la confidentialité des données qu'il contient ou l'intégrité de leur traitement.

2 Une URL – Uniform Resource Locator – est l'adresse d'une ressource spécifique sur un site Web, en général une page Web ou un fichier inclut dans une page, ou encore un programme qui va s'exécuter avec des paramètres pour afficher une page Web de façon dynamique.

3 Un ver est un logiciel (en général malveillant) qui se propage de lui-même d'une machine victime à une autre.

4 A chaque connexion sur Internet ou présence d'un ordinateur ou d'un serveur correspond une adresse IP (pout *Internet Protocol*), suite de chiffres qui sont indiqués aussi bien comme information sur la source ou la destination d'un paquet de données qui circulent sur Internet. Dans le protocole IPv4 (version 4) encore le plus couramment utilisé elles sont le plus souvent représentées par 4 chiffres successifs entre 0 et 255, comme par exemple 122.46.37.24 (exemple fictif). Dans les nouveaux protocoles en cours de déploiement de l'IPv6, l'adresse est de taille beaucoup plus importante pour permettre notamment d'en attribuer à un nombre beaucoup plus grand d'équipements, par exemple 2001:0db8:85a3:0042:1000:8a2e:0370:7334.

5 McColo était une société spécialisée dans l'hébergement de serveurs sur Internet, gérée par un jeune d'origine russe et installé à San Jose en Californie. Ses activités ont cessé en 2008 suite à la mise en évidence des activités essentiellement illégales que ses clients réalisaient.

6 Une vulnérabilité est dite 0-day lorsqu'elle vient d'être découverte ou révélée et qu'elle n'a pas encore été l'objet d'une mesure de correction par l'éditeur du logiciel ciblé.

7 https://www.botnets.fr/index.php/Police_ransomware Botnets.fr est un wiki collaboratif construit dans le cadre des travaux de la thèse que mène actuellement l'auteur à l'Université Paris 6 sur le sujet de la lutte contre les botnets.

8 Une IFRAME est un mécanisme permettant d'inclure dans une page Web du contenu provenant d'un autre site Web. Elle peut-être configurée pour ne pas être visible par le visiteur du site, tout en étant quand même interprétée (donc son code malveillant exécuté) par le navigateur Web.