ÉRIC FREYSSINET (92) *conseiller auprès du préfet, chargé de la lutte contre les cybermenaces*

CYBERCRIMINELS : UN ARSENAL EN PERPÉTUELLE ÉVOLUTION

Les menaces de la cybercriminalité sont multiformes et changent en permanence. La lutte contre les menaces qu'elle induit passe d'abord par une connaissance intime de ce monde, par des actions tout aussi rapides que coordonnées et par un travail constant de sensibilisation des victimes potentielles.

© RAWPIXEL.COM / FOTOLIA

La forme la plus courante d'installation d'un logiciel malveillant est l'installation volontaire d'une application d'apparence banale.

LE MODE DE DIFFUSION des logiciels malveillants prend aujourd'hui plusieurs formes. La première est la propagation automatique, par la découverte sur les réseaux de nouvelles machines vulnérables. On parle alors de vers qui se propagent ainsi d'une machine à une autre.

« Certains délinquants installent plusieurs logiciels malveillants à la fois »

DES LOGICIELS MALVEILLANTS QUI SE RÉPANDENT EN CASCADE

La seconde est la diffusion par pièce jointe à un courrier électronique ou en téléchargement direct depuis un site Web, la victime cliquant sur le lien de téléchargement ou la pièce jointe. C'est notamment le cas sur les plates-formes mobiles où la forme la plus courante d'installation d'un logiciel malveillant est l'installation volontaire d'une application d'apparence banale depuis un magasin d'applications. Enfin, le téléchargement au cours de la navigation (ou *drive-by download*) se déroule à l'insu de la victime lorsqu'elle utilise son navigateur Internet. Ce dernier mode d'infection est le plus courant aujourd'hui, car il touche un plus

REPÈRES

Comprendre la menace est essentiel à la lutte contre la cybercriminalité. C'est essentiel bien évidemment pour ceux qui sont en première ligne, services d'investigation ou équipes œuvrant dans le domaine de la sécurité des systèmes d'information, mais c'est tout aussi important pour les victimes potentielles, ne serait-ce que pour prévenir ces menaces. L'arsenal moderne des cybercriminels comprend un certain nombre d'outils et de plates-formes basés autour des logiciels malveillants : *botnets*, plates-formes d'*exploits*, systèmes de distribution de trafic. Un univers à explorer pour mieux l'appréhender, mieux se protéger voire participer à la lutte contre ces phénomènes.

grand nombre de victimes potentielles, mais il suppose de mettre en œuvre une infrastructure plus complexe.

LES CINQ COMPOSANTES DE L'ARSENAL CYBERCRIMINEL

Premier type d'arme utilisé : les *botnets*, réseaux de machines utilisant un programme malveillant. Une machine infectée par un de ces logiciels malveillants devient un *bot*, qui dès lors communique avec une infrastructure de commande et de contrôle permettant au maître du *botnet* de piloter l'ensemble des *bots* et de recueillir les informations confidentielles collectées.

Une telle architecture permet de combiner un grand nombre de fonctionnalités. Ainsi, les délinquants peuvent installer d'autres logiciels malveillants ou collecter des mots de passe, même si la fonction première est autre, comme l'envoi de courriers électroniques non sollicités (spam).

L'infrastructure de commande et de contrôle du *botnet* peut prendre différentes formes, des architectures centralisées (reposant par exemple sur un simple serveur Web) aux architectures décentralisées (sur le principe des réseaux pair-à-pair). Ces dernières sont les plus résilientes et sont choisies pour les *botnets* les plus aboutis et, au bout du compte, les plus difficiles à démanteler.

LES BANQUES EN LIGNE DE MIRE

Selon nos observations, recoupées par exemple par la synthèse qu'en réalise Europol, les *botnets* les plus préoccupants actuellement sont ceux qui ciblent les transactions bancaires avec un développement croissant de ceux qui s'en prennent aux terminaux de points de vente, ainsi que les *cryptolockers* (ou « rançongiciels chiffrants », qui rendent inaccessibles les fichiers personnels trouvés sur l'ordinateur et réclament le paiement d'une rançon). De même, des architectures de *botnets* sont utilisées pour la réalisation d'étapes importantes des opérations d'espionnage industriel qui ciblent de nombreuses administrations ou entreprises aujourd'hui.

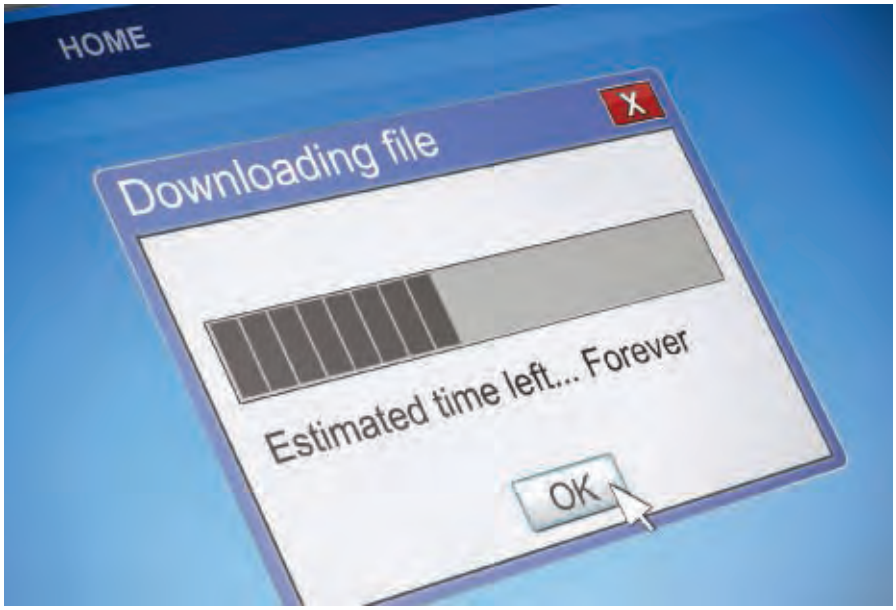
DES ACTIONS EN RÉSEAU

Autre aspect intéressant des *botnets* : les mécanismes de valorisation utilisés. Bien entendu, le maître du *botnet* cherche à commercialiser les données qu'il en tire, ou à sous-louer ses services (des attaques pour bloquer l'accès à un service par exemple). Dans d'autres cas, il peut se contenter d'administrer le *botnet* et confier le « recrutement » de victimes à des affiliés – à charge pour eux d'envoyer des spams ou de faire appel aux services d'un gestionnaire de plate-forme d'*exploit* pour infecter les systèmes de leurs futures victimes. Dans d'autres cas, le logiciel malveillant est commercialisé sous forme de kit, le développeur n'ayant alors pas à se soucier de prendre le risque de le mettre en œuvre lui-même : c'est le cas notamment de beaucoup de catégories de logiciels malveillants qui ont du succès dans la communauté cybercriminelle comme les *botnets* bancaires ou plus récemment les *cryptolockers*.

« L'Angler exploit kit générerait 60 millions de dollars par an de revenus criminels »

PLATES-FORMES D'EXPLOITS

Lorsqu'un internaute se connecte, volontairement ou à son insu, sur une plate-forme d'*exploit*, celle-ci teste un certain nombre de vulnérabilités connues en vue de les exploiter. Il peut s'agir de vulnérabilités du système d'exploitation, du navigateur Web ou encore d'extensions logicielles (extensions pour visualiser des animations, des vidéos ou des fichiers PDF par exemple).



© CREATIVE SOUL / FOTOLIA

Une machine infectée par un logiciel malveillant devient un *bot*.

La plate-forme d'*exploit* la plus célèbre était pendant quelques années le *Black Hole exploit kit*, développé et commercialisé par un citoyen russe agissant sous le pseudonyme Paunch et qui a été interpellé en octobre 2013 par la police de Moscou. La plate-forme qui tient actuellement le haut du pavé est certainement l'*Angler exploit kit*. Celui-ci générerait des revenus criminels atteignant 60 millions de dollars par an rien qu'en diffusant une campagne de rançongiciels.

LES DEALERS DU CYBERCRIME

Les systèmes de distribution de trafic (TDS) sont une catégorie de services cybercriminels qui montre la complexification de cet écosystème. Il s'agit, pour la personne qui l'administre, d'être en mesure d'offrir à ses clients du trafic garanti avec un certain nombre de caractéristiques : pays d'origine, version du système d'exploitation ou encore volumétrie. En amont, lui-même ou des sous-traitants attirent des victimes vers le TDS, puis le système réalise un tri au profit des différents clients. Sutra TDS, Kallisto TDS ou Simple TDS sont quelques-uns des noms des « produits » commercialisés pour mettre en œuvre un tel système.

HÉBERGEMENT : LA STRATÉGIE DU COUCOU

L'ensemble des cybercriminels utilisent les infrastructures Internet existantes pour accomplir leurs méfaits. Mais ils ont besoin de certaines qualités complémentaires pour être encore plus efficaces. Certains d'entre eux se sont donc spécialisés dans l'administration de serveurs, le détournement de serveurs légitimes ou encore la création de véritables hébergeurs à l'abri des enquêtes judiciaires (autrement appelés *bullet-proof hosters*). Ils réalisent cela en abusant leurs employeurs, en louant des services chez des hébergeurs légitimes (tous les grands hébergeurs français et européens en sont régulièrement victimes), ou encore en mettant en place des sociétés ayant pignon sur rue.

LA PISTE DE L'ARGENT

Une des catégories d'acteurs qui intéresse les enquêteurs est celle des intermédiaires financiers, c'est-à-dire l'ensemble de ceux qui permettent de blanchir les revenus de ces trafics. Certains se sont spécialisés dans le recrutement et la gestion de mules qui font transiter sur leurs comptes bancaires l'argent détourné ou réexpédient les colis. Ces activités se complexifient avec l'avènement des services de monnaie électronique. Même s'ils semblent évidents à cibler dans l'enquête judiciaire (avec l'idée de remonter la piste de l'argent), leur action constitue souvent un véritable paravent qui rend très complexe et coûteuse en temps l'identification des véritables commanditaires.

L'une des fonctions particulièrement attendues des cyberdélinquants est la possibilité de mettre en place très rapidement un serveur proche de ses victimes potentielles et d'en changer rapidement en laissant le moins de traces possibles.

« Une véritable balkanisation des acteurs, chacun s'étant spécialisé dans un rôle »

PLATES-FORMES DE MARCHÉ ET OUTILS DE COMMUNICATION

Ces activités ne pourraient se développer sans la capacité pour les cyberdélinquants de rentrer en contact les uns avec les autres. Ils se rencontrent traditionnellement sur des espaces de discussion dédiés (forums Web, canaux de discussion IRC), aussi certains d'entre eux se sont-ils spécialisés dans l'animation de tels espaces avec des fonctionnalités supplémentaires : procédure d'intégration, notation, garantie de l'anonymat, notation des services offerts par les uns et les autres, services de vérification de numéros de carte bancaire volés ou encore de logiciels malveillants pour s'assurer que le produit commercialisé n'est pas détecté par les antivirus.
Ces plates-formes de discussion sont hébergées aussi bien sur des serveurs librement accessibles sur Internet (avec un simple navigateur Web) ou uniquement *via* une connexion sécurisée par le protocole d'anonymisation Tor. Les délinquants y apprennent les méthodes, discutent les offres ou encore affichent leurs publicités.

Assez rapidement, la discussion se porte ensuite sur d'autres moyens de communication plus confidentiels, comme des courriers électroniques jetables et chiffrés ou l'utilisation de messageries instantanées. Ainsi, le logiciel de discussion interpersonnelle ICQ était très utilisé dans la première moitié des années 2000 ; il a été progressivement remplacé par le protocole Jabber/XMPP, indépendant d'un quelconque fournisseur de services et permettant d'y rajouter facilement une couche de chiffrement.

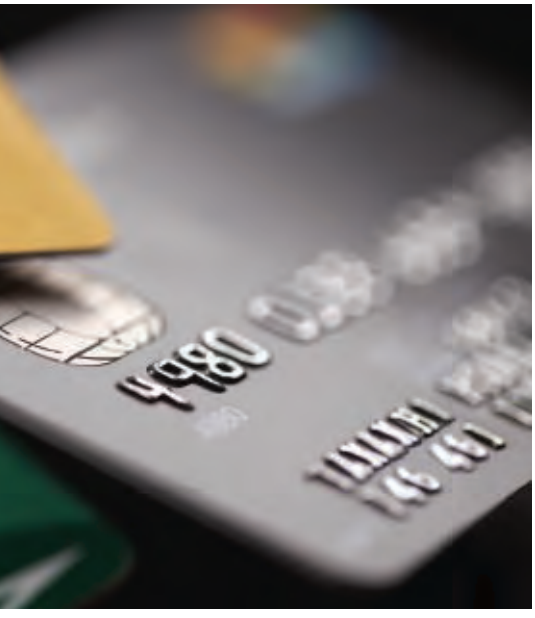
Certains délinquants offrent des services de vérification de numéros de carte bancaire volés.

UN ÉCOSYSTÈME EN MUTATION

L'évolution de la délinquance numérique au cours des vingt dernières années a d'abord marqué un retrait des formes classiques de criminalité organisée (structurées, stables, dont la taille est moyenne à grande) pour des formes d'organisation plus diffuse. On voit apparaître une véritable balkanisation des acteurs, chacun s'étant spécialisé dans un rôle donné, cherchant un maximum de flexibilité pour les uns ou un minimum de risques pour les autres.

« Le développement de la cyberdélinquance est en accélération »

Cette fragmentation contribue à rendre encore plus complexes les enquêtes judiciaires. Ainsi, si l'on arrive plusieurs semaines après le début d'une campagne de diffusion d'un logiciel malveillant, il est possible que le maître du *botnet* fasse appel à un TDS différent, un autre administrateur de plate-forme d'*exploit* ou un fournisseur de spam moins coûteux ou plus efficace. Et évidemment les traces des opérations correspondant aux victimes qui ont d'abord contacté les services d'enquête ont alors totalement disparu.



© SUMIRE8 / FOTOLIA

Pour cette raison, il est indispensable que la justice, les enquêteurs et les groupes de spécialistes ou entreprises spécialisées travaillant sur ce type de menaces prennent rapidement le recul nécessaire : comprendre comment les menaces sont distribuées, comment elles sont organisées et quelle est leur dynamique, sans jamais s'arrêter à une photographie dans le temps, pour être en mesure d'identifier les cibles de leur action.

Cela veut aussi dire qu'il ne faut pas forcément s'intéresser à un logiciel malveillant en particulier, mais à l'ensemble de l'écosystème qui tourne autour. Il sera parfois plus efficace de chercher à s'en prendre à une infrastructure de distribution de trafic ou une plate-forme d'*exploit* qu'à un petit *botnet* opéré par un délinquant ayant acquis un simple kit.

UNE LUTTE IMPLIQUANT DE NOMBREUX ACTEURS

Les pistes pour lutter contre ces nouvelles menaces sont complexes, mais la difficulté de la tâche rend cette complexité nécessaire. En effet, les succès sont encore trop peu nombreux et le développement de la cyberdélinquance est en accélération.

Il est d'abord important de bien comprendre les menaces, de partager cette compréhension et de prendre systématiquement le recul nécessaire pour bien comprendre l'ensemble des acteurs auxquels on peut être confronté.

Il faut être en mesure d'inventer les techniques permettant de détecter ces menaces, mais aussi d'imaginer celles qui permettront de lutter activement contre elles, par exemple identifier les faiblesses dans les infrastructures de commande et de contrôle qui pourront être exploitées.

Il est indispensable que les actions menées contre ces acteurs soient coordonnées entre les différentes parties prenantes. Aucune action technique ne sera efficace si elle n'est associée à l'identification et à l'arrestation des auteurs des méfaits, qui sans cela auront tout loisir de relancer leurs activités.

Ces actions peuvent évidemment avoir pour objectif de rendre plus coûteux le déploiement des menaces, par exemple en démantelant systématiquement les infrastructures utilisées chez les hébergeurs légitimes ou encore en informant les victimes potentielles et en les dotant d'outils permettant de détecter et nettoyer ces menaces dès qu'elles apparaissent.

Tous ont donc un rôle à jouer dans cette lutte, en particulier les acteurs de la réponse à incidents, voire de la réparation informatique, qui collectent potentiellement tous des informations essentielles sur la réalité de cette menace au contact des victimes. C'est aussi un champ d'action pour les hébergeurs, les fournisseurs d'accès à Internet et très certainement la communauté académique. Il faut souhaiter que se multiplient les initiatives leur permettant d'échanger et de se coordonner. ■

DES GROUPES CRIMINELS TRÈS ORGANISÉS

En parallèle d'un écosystème cybercriminel diffus, certains indices récents font apparaître l'émergence de nouvelles formes de groupes criminels très organisés. D'abord, on note un investissement croissant des groupes criminels organisés classiques dans certaines de ces délinquances numériques, comme lors des attaques massives contre le marché du carbone. Ainsi, de nombreux observateurs notent l'apparition de groupes très structurés, comme le groupe Carbanak qui serait derrière un détournement massif dans des banques notamment situées en Russie.

POUR ALLER PLUS LOIN

Éric Freyssinet, « Lutte contre les botnets : analyse et stratégie », mémoire de thèse de doctorat : http://blog.crimenumerique.fr/2015/11/21/lutte-contre-les-botnets/