RFC 6561 : Recommendations for the Remediation of Bots in ISP Networks

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 20 mars 2012

Date de publication du RFC : Mars 2012

https://www.bortzmeyer.org/6561.html

Une des plus grosses menaces sur la sécurité de l'Internet réside dans les zombies, ces machines Windows contaminées par du logiciel malveillant et qui obéissent désormais à un maître qui leur ordonne, selon sa volonté, de lancer une dDoS, d'envoyer du spam, etc. Ce RFC documente le point de vue d'un gros FAI, Comcast, sur le problème. La partie que je trouve la plus riche est celle sur le difficile problème de la **notification** des utilisateurs.

Il n'existe pas de solution miracle contre les zombies. C'est comme cela que je lis ce document qui, malgré son nom, propose peu de remèdes. Et certaines des solutions relèvent plus d'une logique « business » (se débarrasser d'un problème) que d'une volonté d'améliorer l'Internet (le document se réclame du MAAWG, cartel de gros opérateurs très tentés par le nettoyage civilisateur).

Le RFC commence par un peu de terminologie (section 1). "*Bot*" est l'abrévation de "*robot*" et désigne dans ce RFC un zombie, une machine qui n'obéit plus à son propriétaire légitime mais au « maître des zombies » ("*bot master*"), qui les contrôle à distance. Le logiciel qui transforme une innocente machine en zombie a typiquement été installé en trompant l'utilisateur (« *"Click here to install over 200 000 HOT pictures of REAL CHICKS!"* »), ou bien en profitant d'une faille de sécurité de ses logiciels, ou encore en essayant plein de mots de passe jusqu'à en trouver un qui marche. Le RFC note qu'il existe des gentils robots (par exemple pour interagir automatiquement sur les canaux IRC) mais qu'il ne se consacre qu'aux méchants, aux robots malveillants. Petite colère au passage : le mot anglais "*malicious*" veut dire « malveillant » et pas « malicieux » comme on le voit souvent stupidement traduit.

Les "*bots*" sont ensuite regroupés en bandes, les "*botnets*", un groupe de zombies obéissant au même maître. Les activités des "*botnets*" sont très variées, envoi de spam, de spim, de spit, dDoS, hébergement de relais ou de sites de hameçonnage, hébergement de contenu illégal, fraude aux clics, etc.

Pendant longtemps, le protocole de communication favori des "*bot herders*" (ceux qui créent les "*botnets*" et les entretiennent) était IRC (RFC 1459 [1]). Muni d'une seule machine maître (le C3C, "*Command and Control Center*"), le "*botnet*" était assez facile à neutraliser : une fois le maître déconnecté, les zombies ne savaient plus quoi faire. Aujourd'hui, les "*botnets*" sont plus perfectionnés : utilisation de protocoles plus variés (HTTP, plus discret et moins filtré, a remplacé IRC), souvent en pair à pair, le tout largement chiffré.

Quelles sont les conséquences des actions du "*botnet*" ? Pour les victimes (ceux qui reçoivent le spam ou qui sont attaqués par déni de service), elles sont évidentes (pour le spam, voir « "*Spamalytics : An Empirical Analysis of Spam Marketing Conversion*" <http://www.icir.org/christian/publications/2008-ccs-spamalytics.pdf> »). Pour l'utilisateur de la machine, c'est surtout la consommation de ressources, qui diminue les performances attendues. Mais pour le FAI, ces zombies ont aussi un coût : capacité réseau utilisée mais aussi atteinte à la réputation du FAI. Ses adresses IP courent un risque élevé de se retrouver sur des listes noires dont il est difficile de sortir. Certaines des opérations du "*botnet*" peuvent mettre en danger des ressources Internet critiques (voir le « "*Emerging Cyber Threats Report for 2009*" <http://smartech.gatech.edu/bitstream/1853/26301/1/CyberThreatsReport2009.pdf> » et « "*Distributed Denial of Service Attacks : Explanation, Classification and Suggested Solutions*"" <http://www.exploit-db.com/download_pdf/14738/> »).

Le FAI est évidemment bien situé pour détecter la présence de "*bots*", et pour prévenir les utilisateurs. Notons toutefois que, le concept de neutralité du réseau étant tabou chez les FAI, les risques pour ladite neutralité si le FAI s'engage dans ce combat ne sont pas mentionnés dans le RFC.

Personne ne pense bien sûr que des solutions parfaites existent : la lutte entre les "*bot herders*" d'un côté, et les FAI et les utilisateurs de l'autre, n'est pas près de se terminer. Toutefois, affirme le RFC dans sa section 2, on peut espérer limiter les dégâts et réduire la taille des "*botnets*", les rendant ainsi moins dangereux.

La section 3, consacrée à doucher les éventuels enthousiasmes, dit d'ailleurs bien que l'éradication des "*bots*" est une tâche difficile. Elle note que la seule méthode parfaite sur une machine est « Réinstallez votre système d'exploitation », un remède assez radical et donc peu susceptible d'être suivi... Et le RFC fait remarquer que même cette approche ne suffit pas (voir l'exposé « "*Persistent BIOS Infection*" <http://www.coresecurity.com/files/attachments/Persistent_BIOS_Infection_CanSecWest09.pdf> », ou le cas d'engins fermés, comme certains "*smartphones*" ou consoles de jeu, où l'utilisateur n'a même pas la liberté d'installer le système d'exploitation).

Maintenant, place à l'action. La première étape est de **détecter** les zombies dans le réseau. Cela peut se faire par l'analyse passive du trafic, ou bien par les plaintes, même si peu de FAI les traitent <https://www.bortzmeyer.org/abuse-ne-repond-pas.html>. Idéalement, ces plaintes devraient être transmises sous un format structuré, permettant leur analyse automatique, comme les formats ARF (RFC 5965) ou IODEF (RFC 7970). Le document évoque aussi la possibilité de recherches actives, comme le permet un outil comme nmap, bien que de telles recherches ne soient pas forcément légales (cela dépend du pays, note le RFC). Le RFC déconseille néanmoins ces méthodes actives, pas tant sur leur caractère intrusif que sur leur inefficacité (le "*bot*" ne va pas forcément se signaler lors du balayage).

Le RFC insiste sur la nécessité de détecter **vite**, si nécessaire au détriment de la justesse des résultats (tirer d'abord, réflechir ensuite...)

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc1459.txt

Parmi les techniques passives disponibles, le document cite aussi l'analyse des flux Netflow (RFC 3954, mais depuis remplacé par le IPFIX du RFC 5470) ou bien les méthodes à base de DNS, très à la mode en ce moment, notamment grâce au travail des chercheurs de Georgia Tech (voir par exemple David Dagon, Wenke Lee, « "*Global Internet Monitoring Using Passive DNS*" <http://www2.computer.org/portal/web/csdl/doi/10.1109/CATCH.2009.48> », "*Cybersecurity Applications & Technology Conference for Homeland Security*", 2009). Ces méthodes fondées sur l'observation du trafic DNS ont été utilisées dans le cas de Conficker (les zombies font des demandes de résolution pour les noms de domaine générés par l'algorithme de Conficker, ce dernier n'utilisant pas de noms câblés en dur, cf. l'excellent rapport « "*An Analysis of Conficker's Logic and Rendezvous Points*" <http://mtc.sri.com/Conficker/> »). Mais combien de FAI, qui n'arrivent déjà pas à fournir un service correct à leurs utilisateurs, ont les moyens, la compétence et le temps de mener ce genre d'études ?

Idéalement, le FAI devrait non seulement détecter mais également identifier l'infection spécifique, les remèdes pouvant varier.

La partie la plus intéressante du RFC, à mon avis, concerne la notification des utilisateurs. Comment les prévenir que leur machine, infectée, est devenue un zombie ? Et le faire de façon à ce qu'ils comprennent et agissent ? Toutes les techniques de communication possibles avec les utilisateurs sont soigneusement passées en revue, mais aucune ne semble parfaite.

Voici donc les principales techniques envisagées :

— Courrier électronique. Un des problèmes est qu'il risque de ne pas être lu immédiatement. Un autre est qu'il soit classé comme spam. Enfin, les méchants peuvent essayer d'envoyer de faux messages pour brouiller les pistes (du genre « Nous avons reçu notification d'une alerte de sécurité sur votre compte, connectez-vous à http://igotyou.biz/phishing.asp pour indiquer vos coordonnées »...). Ce dernier point est notamment développé en section 9 : il est très difficile d'imaginer un système de notification qui ne puisse **pas** être détourné par les hameçonneurs.
— Appel téléphonique. Ils coûtent cher (il n'y a pas que le prix de l'appel, il y a surtout celui de l'employé appelant, si on choisit de faire faire l'appel par des gens compétents). Ils peuvent être considérés comme du spam (par exemple, Bouygues Telecom appelle régulièrement ses clients pour proposer des offres commerciales nouvelles et sans intérêt, et le robot humain qui appelle, avec un fort accent étranger, n'est jamais capable de répondre à la moindre question concrète : de nombreux clients raccrochent donc dès la première minute de ces spams.). Pire, si l'utilisateur utilise un système de voix sur IP sur son ordinateur, le logiciel malveillant peut décider de ne pas répondre aux appels du FAI. Et puis, le téléphone est le plus mauvais média pour donner des instructions techniques complexes.
— Courrier postal. Très cher et très lent.
— Enfermement dans un jardin clos ("*walled garden*"). L'idée de base est de configurer les routeurs du FAI pour détourner automatiquement tout le trafic en provenance du "*bot*". Les communications avec le port 80, celui de HTTP, sont alors transmises à un site Web portant le message de notification et les instructions pour remédier au problème. Le jardin peut être totalement clos ou bien laisser passer vers certains services externes (un exemple typique étant Windows Update). La méthode est très brutale mais efficace : l'utilisateur ne peut pas ne pas voir les messages et, en attendant, le "*bot*" ne peut plus faire grand mal. Mais, en raison de sa brutalité, elle soulève bien des problèmes. Par exemple, les services autres que le Web (pensons à la voix sur IP) sont coupés, sans avertissement possible. Si le FAI s'est trompé (et que la machine n'était pas réellement infectée), le client va être furieux, et à juste titre. On risque de devoir donc laisser passer certains services par la porte du jardin, et la maintenance de la liste de ces services va être coûteuse. Le FAI doit aussi décider sur quels critères il laissera l'utilisateur sortir du jardin clos. Sur sa simple parole ou bien après un examen (forcément très intrusif) de la machine (d'autant plus que l'utilisateur typique a plusieurs machines derrière le routeur NAT...) ? Et faut-il faire passer un test de Turing aux demandeurs pour vérifier que c'est bien l'utilisateur et pas le "*bot*" qui demande l'ouverture du jardin clos ?

— Messagerie instantanée. C'est rapide et simple. Ce serait sans doute la méthode idéale si tous les utilisateurs utilisaient un tel service et y étaient connectés en permanence. Et il y a le risque de spim.
— SMS. L'utilisateur lira probablement le message, et en peu de temps. Cela suppose que le FAI garde trace des numéros de téléphone de ses clients et que ceux-ci ne considèrent pas le message comme du spam. En outre, les contraintes de taille du SMS posent un drôle de défi au rédacteur du message.
— Le RFC mentionne aussi la possibilité d'utiliser un canal public pour les notifications, par exemple d'utiliser un haut-parleur dans une gare ou un café pour crier « Votre attention, s'il vous plait, nous venons de découvrir que la machine `18:03:73:66:e5:68` est infectée par un logiciel malveillant. Son propriétaire est prié de la désinfecter de toute urgence. » Cela peut être utile dans ces environnements, où l'administrateur du réseau n'a pas de lien particulier avec ses utilisateurs et ne sait pas comment les contacter.

À noter que toutes ces méthodes ne produisent pas de bons résultats au cas, le plus fréquent aujourd'hui, où les adresses IP sont partagées. Dans une entreprise de 500 personnes, montrer la notification aux 500 utilisateurs alors que seul l'administrateur système peut agir est probablement contre-productif. Si le FAI connaît les coordonnées dudit administrateur, il vaut certainement mieux lui écrire directement.

Cette discussion (section 5) des difficultés à attirer l'attention de ses propres clients sur un problème sérieux est la plus concrète du document. Mais elle pose plus de questions qu'elle n'apporte de réponses. Vous vous demandez peut-être quelle solution a finalement retenue Comcast ? Décrite dans le RFC 6108, elle consiste à modifier le contenu des pages Web vues par l'utilisateur pour y insérer une fenêtre-polichinelle d'avertissement.

La seule section qui ait un rapport direct avec le titre (section 6), sur les remèdes est, par contre, très courte, peut-être à juste titre, étant donné la difficulté à traiter les zombies. On les a détecté, on a notifié l'utilisateur, maintenant, que faire ? Le RFC suggère aux FAI de créer un site Web dédié à cet usage, où utilisateurs et administrateurs système pourront accéder à diverses documentations et outils. Les textes visant les utilisateurs sont difficiles à écrire : il faut les motiver pour agir (le "*bot*" peut être très discret, et l'utilisateur n'a alors rien détecté de problématique pour lui), sans les paniquer, et il faut expliquer rapidement car l'utilisateur ne lira pas de longs textes. Le RFC cite comme exemple d'introduction pour capter l'attention : « "*What is a bot ? A bot is a piece of software, generally installed on your machine without your knowledge, which either sends spam or tries to steal your personal information. They can be very difficult to spot, though you may have noticed that your computer is running much more slowly than usual or you notice regular disk activity even when you are not doing anything. Ignoring this problem is risky to you and your personal information. Thus, bots need to be removed to protect your data and your personal information.*" »

La tâche de désinfection peut être difficile (surtout sur des engins comme les consoles de jeu, qui ne donnent typiquement pas accès au système) et, dans tous les cas, l'utilisateur n'a en général pas de compétences techniques : les instructions de désinfection doivent donc être très concrètes et détaillées.

Donc, sous forme d'une liste, voici quelques-unes des étapes que le RFC recommande de ne pas oublier, dans les conseils donnés aux utilisateurs :

— Faites des sauvegardes de vos fichiers (un bon avis, indépendamment de l'infection par le "*malware*").
— Mettez à jour votre système ("*Windows Update*" avec Microsoft Windows, par exemple).
— Ne pas hésiter à demander l'aide d'un professionnel. Ce conseil du RFC est évidemment raisonnable (la tâche peut être trop complexe pour l'utilisateur ordinaire) mais me laisse perplexe : pour les soins aux machines de M. Toutlemonde, on trouve plein de gourous autoproclamés, dont les compétences en informatique sont en général à peine supérieures à celles de leurs clients. Ces derniers, ne connaissant pas le sujet, ne peuvent pas distinguer un vrai expert d'un Jean-Kevin Michu qui se prend pour un gourou parce qu'il a déjà installé une fois un Windows en partant de zéro. Ce problème me semble un des plus sérieux pour M. Toutlemonde « à qui faire confiance ? »

— Si l'utilisateur a l'intention de porter plainte, il faut faire l'inverse : ne **pas** nettoyer la machine mais la laisser intacte pour l'enquête (comme la scène du crime entourée du ruban jaune, dans les séries policières états-uniennes). Aux États-Unis, l'organisme national en charge est l'"*Internet Crime Complaint Center*" <http://www.ic3.gov/>. (Quel est l'équivalent en France ?) Le RFC note toutefois en termes diplomatiquement polis qu'il y a peu de chance que la police se dérange parce que M. Toutlemonde a un virus sur sa machine... (Et j'ajoute que c'est parce que la police est occupée avec des crimes plus graves <http://www.numerama.com/magazine/19648-tous-ces-delits-ju
html> comme par exemple le partage de la culture.)

Et si l'utilisateur ne peut pas ou ne veut pas réparer (section 7) ? Le RFC note que c'est évidemment un problème non-technique et a une approche très états-unienne, « "*shoot them*" » (supprimer l'abonnement et déconnecter l'utilisateur).

Le document rend aussi un hommage obligatoire à la nécessite de préserver la vie privée des utilisateurs (sections 4 et 10), sans trop s'attarder sur comment concilier surveillance rapprochée et respect de la vie privée. Un intéressant problème à la fois politique et légal. Voir aussi la section 8 sur les problèmes que pose le partage de données entre l'utilisateur, le FAI et éventuellement les autorités. L'annexe A donne une liste d'organisations privées qui peuvent être intéressés par ces données (liste de machines infectées, pour faire une liste noire, par exemple) et les publier.

À noter qu'une autre faiblesse de ce document est que, pour éviter de déchaîner les avocats de Microsoft, le fait que la quasi-totalité des zombies soient aujourd'hui des machines Windows est tout simplement absent...