Un « Internet-Draft » résumant ce que peut faire un FAI contre les zombies

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 5 octobre 2009

https://www.bortzmeyer.org/bot-remediation.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.

Il n'existe pas de solution miracle contre les zombies. C'est comme cela que je lis l'"*Internet-Draft*", draft-oreirdan-mody-bot-remediation, intitulé « "*Remediation of bots in ISP networks*" » mais qui, malgré son nom, propose peu de remèdes. ("*Bot*" est l'abrévation de "*robot*" et désigne un zombie.)

Cet "*Internet-Draft*", qui est devenu un RFC de « bonnes pratiques » quelques années plus tard (RFC 6561 [1]), est écrit par des employés de Comcast et résume l'état actuel de l'art, vu du point de vue du FAI. Celui-ci, étant donné sa position, est bien placé pour identifier les machines de ses clients qui sont devenues des zombies. Mais que peut-il faire ?

Le document explique bien le problème, ainsi que la manière de détecter les zombies (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> ; 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). Il insiste sur la nécessité de détecter **vite**, si nécessaire au détriment de la justesse des résultats (tirer d'abord, réflechir ensuite...)

Parmi les techniques disponibles, le document cite Netflow (RFC 3954) 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). Mais combien de FAI, qui

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6561.txt

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 ?

Le document rend aussi un hommage obligatoire à la nécessite de préserver la vie privée des utilisateurs, sans trop s'attarder sur comment concilier surveillance rapprochée et respect de la vie privée.

La partie la plus intéressante du document 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 ? Le problème est d'autant plus complexe que 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 »...)

Toutes les techniques de communication possibles avec les utilisateurs sont soigneusement passées en revue, mais aucune ne semble parfaite. Les appels téléphoniques coûtent cher (le courrier papier encore plus), les messages peuvent être ignorés, couper l'accès pour que l'utilisateur appele est violent, quoique efficace, etc. Cette discussion des difficultés à attirer l'attention de ses propres clients sur un problème sérieux est la plus concrète et certainement la plus intéressante du document. Le RFC 6108, publié plus tard, présente une solution possible.

La seule section qui aie un rapport direct avec le titre, sur les remèdes est, par contre, très courte, peut-être à juste titre, étant donné la difficulté à traiter les zombies : « Réinstallez votre système d'exploitation » est un remède assez radical et donc peu susceptible d'être suivi...

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