Le rapport HostExploit 2012 sur les plus grandes sources de Mal de l'Internet

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 31 octobre 2012. Dernière mise à jour le 12 novembre 2012

https://www.bortzmeyer.org/hostexploit-2012.html

Les gérants du groupe HostExploit <http://www.hostexploit.com/> compilent un rapport régulier sur les plus grosses sources de Mal de l'Internet, c'est à dire les systèmes autonomes hébergeant le plus de centres de commande de botnets, le plus de serveurs de hameçonnage, envoyant le plus de spam... Un Who's who des acteurs de l'Internet, sous l'angle négatif. Dans le dernier rapport, numéroté Q32012, on note un nouveau n° 1 de ce classement, Confluence, et l'arrivée du français OVH dans le sommet.

Avant de commenter ce rapport, il convient d'être prudent et de bien prendre connaissance de la méthodologie. Celle-ci est décrite dans une annexe au rapport (le rapport est fait en Word avec des couleurs et l'annexe en LaTeX...). En gros, HostExploit <http://www.hostexploit.com/> utilise un certain nombre de sources qui listent des adresses IP qui ont participé à des comportements négatifs, comme héberger un serveur de malware, ou bien un serveur Zeus (voir le Zeus Tracker <https://zeustracker.abuse.ch/>). De l'adresse IP, on remonte à l'AS et au pays (cette dernière information étant moins fiable). Le tout est pondéré par la taille de l'espace d'adressage annoncé par l'AS (pour éviter que les petits AS hébergant proportionnellement beaucoup de Mal ne se glissent sous la couverture du radar.)

Ces sources ne sont pas parfaites : tout n'est pas signalé, certains le sont à tort.

D'autre part, malgré mon introduction sensationnaliste, il faut bien voir que le fait qu'un AS (donc, en pratique, un opérateur ou hébergeur) soit bien placé dans la liste ne signifie pas que c'est lui qui envoie du spam ou héberge du malware. Il peut être « victime » de ses clients. Des fois, c'est même encore plus indirect : un hébergeur loue des machines, un client en prend une, son site Web se fait pirater, un serveur de hameçonnage est installé dessus et l'AS de l'hébergeur va remonter dans le classement « source de Mal ».

Alors, que contient le classement Q32012 <http://www.hostexploit.com/blog/14-reports/3540-familiar-hosts-a-open-resolvers.html> ? Ce classement est peu stable : un opérateur

envahi par des zombies va être mis sur des listes noires (et ne sera donc plus intéressant pour les maîtres des zombies) ou bien va prendre des mesures radicales (faire le ménage) et, l'année suivante, rétrogradera loin dans le classement. Cette année, l'AS 40034, Confluence, hébergé dans le paradis fiscal des Îles Vierges, arrive en numéro un du classement général (p. 9 du rapport). Coïncidence amusante, deux jours avant de lire ce dossier, je citais le cas d'un détournement de noms de domaine (l'affaire `ben.edu`), fait via une machine chez Confluence. L'AS 16276, le français OVH est numéro 4, en très nette progression. (Sur la liste FRnOG <`http://www.frnog.org/`>, le directeur d'OVH estime aujourd'hui, je cite, que « avec les differents BETA aux USA que nous avons fait entre juillet et septembre, on a eu une augmentation importante des abuses en tout genre à partir de notre reseau. en gros, les nouveaux "clients" hackers nous ont decouvert puis depuis nous commandent de services. il y a 1 mois on est arrivé au point de non retour : trop marre. et donc il y a 3 semaines on a commencé un grand nettoyage avant l'hiver mais en incluant un echange avec les clients. et si pas de reponse là on hache. vous pouvez donc lire à droite ou à gauche que "mon serveur s'est fait bloqué pour 1 spam". oui si pas de dialogue, pas de serveur. si pas d'action, pas de serveur. sur spamhaus ça sera clean à la fin de la semaine (il reste 14 alertes). et les autres rbl c'est une question de 2 à 3 semaines. » Fin de citation)

Si on regarde le type de Mal hébergé (p. 11), on note que Confluence fait surtout de l'hébergement de Zeus alors qu'OVH est nettement moins spécialisé, on y trouve de tout. Cela semble indiquer qu'il n'y a pas de choix délibéré d'OVH, ni même d'envahissement de ses serveurs par un méchant décidé : la raison du score d'OVH est plus probablement que beaucoup de ses clients sont nuls en sécurité, installent un LAMP sans rien y connaître, se font pirater via une faille PHP, et ne corrigent pas le problème même quand on leur signale.

En attachant les AS à un pays (ce qui est parfois difficile, ainsi Confluence a été classé comme états-unienne malgré son adresse officielle aux Îles Vierges britanniques et, plus drôle, VeriSign a été classé aux Pays-Bas), on voit (p. 16) la Russie en numéro 1, ce qui ne surprendra guère, et le paradis fiscal de l'Union européenne en numéro 4. Grâce à OVH, la France est en huitième position.

Si on classe les AS en prenant chaque cause de Mal séparement, on voit que, pour l'hébergement de serveurs C&C, c'est l'AS 50465, IQhost, qui gagne, devant un autre russe. Pour le hameçonnage, les États-Unis prennent l'avantage avec l'AS 53665, Bodis. Confluence, on l'a vu, gagne nettement pour l'hébergement Zeus. Pour l'envoi du spam, les Indiens sont loin devant avec le record chez l'AS 55740, Tata.

Plus surprenant est le classement des AS où on trouve du malware (p. 26), car l'AS 26415, VeriSign (qui sert notamment pour les serveurs DNS racine exploités par cette société) et l'AS 15169, Google, se retrouvent dans les dix premiers. Le rapport ne propose pas d'explication. Pour Verisign, des explications raisonnables ont filtré mais rien de public encore. Pour Google, si, à première vue, dissimuler du code malveillant dans un Google document n'est pas évident (cela serait possible, via des fonctions de "*scripting*"), il y a déjà eu des rapports de hameçonnage où l'appât était un Google document, ce qui explique sans doute ce classement.

Maintenant, qu'est-ce qui devrait être fait ? Un AS a évidemment intérêt à nettoyer ces sources de Mal. Sinon, il va retrouver ses adresses IP dans plein de listes noires dont il est très difficile de sortir <`https://www.bortzmeyer.org/pas-de-listes-noires-statiques.html`>. Certains AS ont manifestement choisi de rester dans le "*business*" de l'hébergement de délinquants et se moquent de leur réputation (ils sont dans le sommet du classement depuis longtemps comme l'AS 16138, Interia). D'autres ont un problème difficile. (Ceci dit, ils pourraient commencer par traiter le courrier envoyé à abuse <`https://www.bortzmeyer.org/abuse-ne-repond-pas.html`>.) Nettoyer, OK, mais en respectant un minimum de règles. La différence de classement entre l'AS 16276 (OVH) et l'AS 14618 (Amazon), qui a un "*business model*" très proche (louer des machines rapidement et sans formalités, à des tas de clients, pas toujours compétents et pas toujours honnêtes), provient sans doute largement

d'une différence d'approche entre l'Europe et les États-Unis. Aux USA, les hébergeurs se comportent comme des cow-boys : au premier signalement de problème (même injustifié), ils coupent et on n'a plus qu'à se chercher un autre hébergeur. Le fameux premier amendement à la Constitution, censé protéger la liberté d'expression, ne les arrête pas : il ne s'impose qu'à l'État. Les entreprises privées, elles, ont tout à fait le droit de s'attaquer à la liberté d'expression. WikiLeaks, qui fut client d'Amazon avant de l'être d'OVH, en sait quelque chose.

Le rapport d'HostExploit exhorte en effet les opérateurs à « agir », à « nettoyer », mais ne fournit aucune piste en ce sens (à part un conseil implicite : « tirez d'abord et enquêtez après »).

Ah, et pour les gens du DNS, à part la curieuse place de VeriSign, une nouveauté de ce rapport est l'étude des résolveurs DNS ouverts <https://www.bortzmeyer.org/fermer-les-recursifs-ouverts.html> (p. 6). Ils sont une grande source d'ennuis, notamment par leur utilisation comme relais pour des attaques DoS avec amplification <https://www.bortzmeyer.org/dns-rate-limiting-and-attacks.html>. Mais ils ne sont pas eux-même le résultat d'un choix délibéré par un méchant : les AS qui hébergent en proportion le plus de résolveurs ouverts (7418, Terra, ou 8167, Telesc) sont largement absents des autres classements et il n'y a donc pas de corrélation entre le nombre de résolveurs ouverts et l'hébergement d'autres sources de Mal.

Merci à Daniel Azuelos et Fabien Duchene pour leurs remarques.

---

https://www.bortzmeyer.org/hostexploit-2012.html