Compter sérieusement le nombre d'attaques informatiques ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 15 mars 2014

https://www.bortzmeyer.org/compter-attaques.html

La presse à sensation et les rapports des sociétés qui vendent de la sécurité informatique sont pleins de chiffres sur les « cyber-attaques ». Des titres comme « de 10 à 100 attaques à la seconde » ou « une cyber-attaque toutes les 1,5 secondes en moyenne » sont courants. Que signifient-ils ? Quelle est la méthodologie de mesure ? Est-ce sérieux ?

On trouve sans peine des exemples de tels articles. Par exemple dans un journal peu regardant <http://www.lefigaro.fr/hightech/2012/12/06/01007-20121206ARTFIG00569-explosion-des-cybera
php>. D'autres ont un ton plus mesuré <http://www.lepoint.fr/chroniqueurs-du-point/laurence-neuer/2013-a-l-aube-de-nouveaux-cyberdangers-19-01-2013-1617471_56.php> mais fournissent également leur lot de chiffres invérifiables. En l'absence de détails sur la définition des termes utilisés, aucune comparaison n'est possible. Un autre article de la presse à sensation <http://lexpansion.lexpress.fr/high-tech/une-cyber-attaque-toutes-les-1-5-secondes-en-moyenne_1497108.html> voit moins d'une attaque par seconde (cent fois moins que l'article cité en premier, cela donne une idée du sérieux de ces chiffres)... Certains font des jolis dessins plus sérieux <http://www.sicherheitstacho.eu/> mais ne divulguent quasiment aucun détail sur leur méthodologie. D'autres sont tellement ignorants <http://technologies.lesechos.fr/transformation-digitale/infographie-cybersecurite-les-plus-grandes-attaques-informatiques-de-l-histoire_a-37-874.html> qu'ils se trompent aussi bien sur le vocabulaire du droit que sur celui de l'informatique (en appelant « cybercrime » des délits qui ne sont pas des crimes).

Donc, première observation, les chiffres publiés ne veulent rien dire car ils ne sont jamais accompagnés d'une méthodologie, d'une description des indicateurs utilisés. D'où les variations ridicules d'un article à l'autre, et la surenchère. Par exemple, voici un extrait du journal de ce blog, où la machine 188.143.234.90 essaie successivement plusieurs attaques PHP contre le serveur (je n'ai mis qu'une partie des requêtes HTTP) :

```
188.143.234.90 - - [13/Mar/2014:03:36:14 +0000] "GET /mysql-admin/index.php HTTP/1.1" 404 281 "-" "Mozilla/4.0 (
188.143.234.90 - - [13/Mar/2014:03:36:15 +0000] "GET /PMA/index.php HTTP/1.1" 404 281 "-" "Mozilla/4.0 (compatib
188.143.234.90 - - [13/Mar/2014:03:36:15 +0000] "GET /php-my-admin/index.php HTTP/1.1" 404 281 "-" "Mozilla/4.0
188.143.234.90 - - [13/Mar/2014:03:36:15 +0000] "GET /webdb/index.php HTTP/1.1" 404 281 "-" "Mozilla/4.0 (compat
188.143.234.90 - - [13/Mar/2014:03:36:15 +0000] "GET /webadmin/index.php HTTP/1.1" 404 281 "-" "Mozilla/4.0 (com
188.143.234.90 - - [13/Mar/2014:03:36:15 +0000] "POST /cgi-bin/php?%2D%64+%61%6C%6C%6F%77%5F%75%72%6C%5F%69%6E%6
```

Comment dois-je compter ce qui est clairement une attaque ? Il est probable que `188.143.234.90` n'en voulait pas spécialement à mon blog et balayait tout simplement tout un tas de serveurs. Auquel cas, il serait logique de ne compter qu'une attaque pour tous ces serveurs. Mais, si chaque administrateur système compte le passage du bot `188.143.234.90` sur son site comme une attaque, le nombre total d'attaques sera bien plus élevé. Et, si je veux franchement abuser, je peux aussi compter chaque requête HTTP comme une attaque (il y en avait bien plus que ce que je montre ici). Comment font les organisations qui publient les chiffres que la presse reprend sans jamais enquêter, sans jamais chercher un point de vue critique ? Eh bien, on ne sait pas. La publication des chiffres n'est **jamais** accompagnée de la méthodologie et ces chiffres n'ont donc aucun intérêt.

Peut-être pensez-vous que j'ai vraiment trop abusé avec l'idée de compter chaque requête HTTP comme une attaque. Mais j'ai déjà vu cela en vrai, par exemple sur des "*firewalls*" cliquodromesques avec un bouton permettant de générer des jolis camemberts pour PHBs. Chaque paquet rejeté par le pare-feu était compté comme une attaque, ce qui permettait au PHB de se dire chaque matin qu'il avait bien dépensé son argent. (Pour les gens qui ne sont pas administrateurs système ou réseau, précisons que toute adresse IP reçoit en permanence un trafic non sollicité d'attaque ou de reconnaissance, qu'on appelle l'IBR.)

Autre cause de désaccord, comment compter les tentatives de reconnaissance, qui peuvent être malveillantes mais peuvent aussi être de la curiosité. J'ai connu un site où l'administrateur notait chaque telnet (un paquet TCP vers le port 23) comme une attaque... Et que dire alors d'un examen avec nmap qui va illuminer l'IDS comme un arbre de Noël ? Une attaque, aussi ? On voit que l'absence de définition rigoureuse permet toutes les manipulations, dans un sens ou dans l'autre. Enfin, on voit aussi des webmestres crier à l'attaque dès que leur site ralentit sous la charge. Beaucoup de site Web dynamiques sont programmés de telle façon (avec 10 000 lignes de code Java ou PHP à exécuter à chaque requête HTTP) qu'ils s'écroulent très vite dès qu'ils ont un peu de succès. Il est alors tentant d'enregistrer cela comme une attaque plutôt que de reconnaître qu'on avait mal calculé son coup...

Il faut dire que la mauvaise qualité des données n'est pas uniquement due à la paresse et à l'incompétence. Les intérêts économiques ou politiques jouent également un rôle. Il n'existe en effet pas de « chiffres officiels » sur les attaques informatiques (je ne garantis évidemment pas que des chiffres officiels seraient plus fiables...) Les données publiées dans la presse sont donc uniquement issues de dossiers de presse faits par des entreprises qui vendent de la sécurité informatique, et qui ont donc tout intérêt à produire des chiffres élevés. Comme la grande majorité des journalistes n'a ni le temps, ni les moyens, ni la volonté de creuser un peu le sujet, les grands médias ne font que reformuler légèrement ces dossiers de presse, qui leur fournissent du contenu à bas prix. Il y a donc les intérêts économiques (peindre le problème sous les couleurs les plus noires pour vendre ensuite des solutions techniques miracles) et les buts politiques (justifier des lois répressives). Les deux concourent à exagérer les chiffres, et d'autant plus facilement qu'il n'y a jamais d'enquête indépendante et de "*fact checking*".

On a donc un problème qui n'est pas très éloigné de la classique polémique sur les chiffres de la délinquance, mais avec encore moins d'indicateurs fiables. Comme le note Nicolas Caproni « les gens veulent comparer mais comme on n'aura jamais de référentiel commun, ça semble impossible ou tout du moins très imparfait ».

Bon, assez râlé, vont se dire les plus positifs de mes lecteurs, c'est facile de critiquer mais que proposes-tu ? Je n'ai hélas pas de solution miracle. Mais il n'est pas interdit d'explorer quelques pistes :

— Un représentant des forces de l'ordre m'avait dit une fois que le problème était simple : la définition d'un délit en informatique est claire, il suffit de compter comme attaque toute action illégale. Cette métrique a l'avantage d'être objective mais l'inconvénient de mener à des chiffres colossaux : chaque fois qu'un "*malware*" infecte une machine Windows, pouf, article 323-1 du Code Pénal et on a une attaque de plus pour les statistiques.

— Autre métrique à base juridique, compter le nombre de plaintes déposées. Là, c'est le contraire, on va sous-estimer le nombre d'attaques puisque la plupart ne font pas l'objet d'une plainte (je n'ai pas porté plainte pour les tentatives de `188.143.234.90`, trop cher et trop compliqué...)
— Alors, prenons une métrique moins juridique et plus opérationnelle : compter le nombre de tickets ouverts par le NOC pour incident de sécurité ? Le problème est que cela mesure l'activité du NOC, pas celle des attaquants. Si on augmente les moyens du NOC, mécaniquement, cela augmentera le nombre d'attaques.
— Bon, et le point de vue rationnel et pragmatique ? L'administrateur système, surchargé de travail, ne compte comme attaque que ce qui perturbe effectivement le service. Mais ce critère utilitariste permet quand même des faux positifs (le slashdottage, cité plus haut, compte comme une attaque puisqu'il perturbe effectivement le service) et des faux négatifs (un pirate qui ne fait que de l'espionnage passif du système se gardera bien de perturber le service et ne sera donc pas compté comme une attaque.)
— Et compter comme attaque uniquement ce qui réussit ? Le balayage par `188.143.234.90` cité plus haut est ridicule puisque cette machine n'a aucun script PHP. De même, un balayage du port 22 <`https://www.bortzmeyer.org/sshd-port-alternatif.html`> sur une machine où sshd tourne sur un autre port ne serait pas compté comme une attaque. L'inconvénient de ce critère est qu'il dépend davantage de l'activité et de la compétence du défenseur que de l'activité des attaquants.
— Bref, je ne connais pas de solution idéale. Et vous ? Je suis sûr que vous avez une idée. (Merci à Xavier Belanger pour ses suggestions.)