Nominum, une entreprise à éviter de loin

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 23 septembre 2009. Dernière mise à jour le 4 octobre 2009

https://www.bortzmeyer.org/nominum-a-eviter.html

La société Nominum, qui vend des logiciels DNS, s'était déjà fait connaître par des discours marketing douteux <http://www.nominum.com/news/articles/2008/nominum_dns_protects_120_print.html> sur ses concurrents, notamment ceux utilisant du logiciel libre. Elle franchit un nouveau pas, avec l'interview / publireportage de son marketroïde Jon Shalowitz en "*Why open-source DNS is 'internet's dirty little secret'* " <http://news.zdnet.co.uk/itmanagement/0,1000000308,39760362,00.htm?s_cid=260>.

Aujourd'hui que Microsoft proteste de son amitié pour le monde du logiciel libre, et qu'Apple la ferme prudemment, Nominum prend le relais de SCO en assumant le rôle du méchant, qui crache son venin sur le principe même du logiciel libre, comparé au "*malware*".

Bien sûr, comme tant de commerciaux, Jon Shalowitz est un ignorant complet et n'a même pas pensé que tout le monde testerait immédiatement les serveurs de Nominum pour voir quels logiciels ils utilisent :

```
% dig +short NS nominum.com
ns1.nominum.com.
ns2.nominum.net.
ns3.nominum.com.

% dig +short @ns1.nominum.com CH TXT version.bind.
"Nominum ANS 3.0.1.0"
% fpdns ns1.nominum.com
fingerprint (ns1.nominum.com, 64.89.228.10): Nominum ANS

% dig +short @ns2.nominum.net CH TXT version.bind.
"9.3.5-P2"
% fpdns ns2.nominum.net
fingerprint (ns2.nominum.net, 81.200.68.218): ISC BIND 9.2.3rc1 -- 9.4.0a0
```

Eh oui, un des serveurs DNS de Nominum utilise BIND, archétype du serveur DNS en logiciel libre. (Les deux autres utilisent ANS, "*Authoritative Name Server*", l'un des principaux produits de Nominum.)

Depuis que cette information a été publiée, le serveur a changé. Difficile de dire s'il a vraiment été remplacé ou bien si un technicien de Nominum a utilisé la directive `version` du bloc `options` pour changer le nom sous lequel BIND s'annonce...

Autre cas où Nominum dépend de logiciel libre, son site Web :

```
% telnet www.nominum.com http
Trying 67.192.49.178...
Connected to www.nominum.com.
Escape character is '^]'.
HEAD / HTTP/1.0
Host: www.nominum.com

HTTP/1.1 200 OK
Date: Wed, 23 Sep 2009 10:20:28 GMT
Server: Apache/2.0.52 (Red Hat)
X-Powered-By: PHP/4.3.9
...
```

Pour une société qui prétend que son logiciel est sécurisé, utilisable industriellement, etc, cela fait drôle d'utiliser PHP, dont on n'avait jamais entendu dire qu'il était spécialement durci... (En outre, si le numéro de version est correct, la version de PHP date de 2004, ce qui montre un certain sens du conservatisme.)

On pourrait continuer à l'infini à se moquer de Nominum et de la nullité de ses équipes commerciales, dont l'aggresivité essaie de masquer la perte de part de marché actuelle. Mais il est probable que le discours de Nominum ne vise pas à convaincre les lecteurs de ce blog, ni les habitués du logiciel libre <http://lwn.net/Articles/353879/>, ni même d'ailleurs aucun technicien connaissant ne serait-ce qu'un tout petit peu le DNS. Leur propagande est conçue pour une population de PHB, qui ignorent tout du logiciel libre, qui les inquiète. Ceux-ci sont rassurés que quelqu'un ose tenir un discours de guerre froide, avec la reprise d'arguments moyen-âgeux, comme le fait que la non-distribution du code source permettrait à Nominum de mettre en œuvre des protections originales contre les vulnérabilités du DNS.

Tiens, à propos de cet argument (Nominum cite la faille Kaminsky <https://www.bortzmeyer.org/comment-fonctionne-la-faille-kaminsky.html>, en oubliant qu'elle les avait obligé, eux aussi, à mettre à jour en urgence leur logiciel <http://www.nominum.com/asset_upload_file741_2661.pdf>), est-il vrai ? Beaucoup pensent que Nominum ne fait que bluffer, qu'il n'existe aucune protection particulière contre l'empoisonnement de cache dans CNS ("*Caching Name Server*", l'autre produit de Nominum). Mais il y en a bien une (merci à Paul Vixie pour son rappel à ce sujet), CNS essaie de se connecter en TCP s'il reçoit des réponses dont le "*Query ID*" ne correspond pas (ce qui peut indiquer une tentative d'empoisonnement). Cela n'a évidemment rien de « secret » contrairement à ce que raconte le menteur en chef de Nominum, puisque n'importe quel gérant de zone peut voir (par exemple avec tcpdump) les machines CNS essayer en TCP, simplement en tentant d'empoisonner sa propre zone.

Les serveurs de Nominum, à part qu'ils sont privateurs, sont-ils meilleurs ou au moins comparables aux serveurs en logiciel libre comme Unbound, NSD ou PowerDNS ? Impossible de le dire : lorsqu'il y a des tests comparatifs de logiciels DNS, Nominum refuse systématiquement de prêter une copie d'ANS ou de CNS pour les essais. Ou alors, ils imposent des contraintes comme l'impossibilité de rendre compte

publiquement des résultats sans leur autorisation expresse. Donc, on ne peut rien dire, Nominum n'a pas assez confiance dans ses logiciels pour les comparer aux autres.

Devant la pluie de critiques qui s'est abattue sur Nominum à cette occasion, un chef plus haut placé a fini par comprendre l'erreur commise et a opéré un tournant à 180° dans un article sur CircleID <http://www.circleid.com/posts/20090930_nominum_ceo_commercial_vs_open_source_let_customers_choose/> où il abandonne toutes les attaques contre le logiciel libre. Voilà des gens qui n'ont pas de fierté : on attaque méchamment puis, lorsque les victimes font trop de bruit, on s'enfuie en prétendant n'avoir jamais voulu cela.

Mais il y a bien plus grave que ces attaques anti-pingouins. Nominum, on l'a vu, ne cherche pas à convaincre les porteurs de T-shirts IETF. Nominum vise les messieurs sérieux, ceux qui sont haut placés dans les entreprises ou les gouvernements. Et, à ceux-ci, Nominum ne se présente pas simplement comme un fournisseur de logiciels DNS, mais comme une entreprise de filtrage et de censure <http://www.darkreading.com/securityservices/security/showArticle.jhtml?articleID=220100568>: « "*Since the first step of any Internet request is a DNS look-up, the name service is a natural position to deploy technology asserting manageable controls over the complexities and threats of today's Internet.*" ».

Pas étonnant, donc, que Nominum cherche en ce moment à convaincre le gouvernement français de l'intérêt de ses produits, au moment où l'une des pistes suivies pour la loi LOPPSI est l'installation obligatoire de serveurs DNS censeurs chez les FAI.

D'autres bons articles sur Nominum :

— "*PowerDNS competitor Nominum lauds its closed source credits !*" <http://bert-hubert.blogspot.com/2009/09/powerdns-competitor-nominum-lauds-it.html>,
— Discussion sur Slashdot <http://tech.slashdot.org/story/09/09/23/1555245/Nominum-Calls-Open
— et une sur LWN <http://lwn.net/Articles/353879/>.