

Attaque DNS par amplification en demandant "NS."

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 24 Janvier 2009

<http://www.bortzmeyer.org/dns-attaque-ns-point.html>

Depuis au moins le 7 janvier, une série d'attaques DoS utilisant le DNS a lieu. Parfois nommée "*IS-Prime*", du nom de la première victime, cette attaque utilise une variante originale des attaques par amplification.

Le principe est que le DNS repose essentiellement sur UDP, protocole sans connexion et très vulnérable aux usurpations d'adresses IP. Tirant partie de l'absence de filtrage à la source par la grande majorité des FAI, l'attaquant envoie des paquets avec une **fausse** adresse source. Il est donc absurde de bloquer complètement ces adresses, ce sont celles des victimes, pas celles des attaquants.

L'attaque par amplification originale visait des serveurs récursifs ouverts <<http://www.bortzmeyer.org/fermer-les-recursifs-ouverts.html>>, comme le détaille le RFC 5358¹. Cette variante actuelle, compte-tenu de la diminution du nombre de récursifs ouverts, utilise des serveurs qui n'acceptent pas de faire des requêtes récursives mais acceptent de répondre à la question "NS.", c'est à dire à une demande de la liste des serveurs de noms de la racine. La liste étant assez longue, l'attaquant réussit ainsi une amplification (la réponse, envoyée à la victime, est bien plus grosse que la requête, envoyée par l'attaquant).

Un bon article de l'OARC, "*Upward Referrals Considered Harmful*" <<https://www.dns-oarc.net/oarc/articles/upward-referrals-considered-harmful>> explique pourquoi il faut configurer ses résolveurs pour éviter de répondre à ces questions "NS." (et comment le faire pour BIND).

Vous pouvez vérifier que votre résolveur est sûr en lui demandant, depuis une machine à l'extérieur de votre réseau :

```
% dig @votre-machine NS .
```

1. Pour voir le RFC de numéro NNN, <http://www.ietf.org/rfc/rfcNNN.txt>, par exemple <http://www.ietf.org/rfc/rfc5358.txt>

et vous ne devez pas avoir de réponse (ou bien une réponse courte comme REFUSED ou SERVFAIL). Vous pouvez aussi tester depuis un site Web <<http://isc1.sans.org/dnstest.html>>.

La plupart des utilisateurs de BIND voient ces requêtes dans leurs journaux :

```
/var/log/daemon.log:Jan 24 09:23:30 lilith named[31908]: client 63.217.28.226#28124: view external: query (ca
/var/log/daemon.log:Jan 24 09:23:31 lilith named[31908]: client 63.217.28.226#53227: view external: query (ca
/var/log/daemon.log:Jan 24 09:23:32 lilith named[31908]: client 66.230.160.1#1601: view external: query (ca
```

mais, si on utilise l'excellent outil de capture DNS dnscap <<https://www.dns-oarc.net/tools/dnscap/>>, on peut aussi les voir en demandant les requêtes concernant la racine :

```
% sudo dnscap -i eth0 -w ~/tmp/isprime -g -s i -x '^\..$'
...
[45] 2009-01-24 22:22:41.094184 [#1300 eth0 0] \
    [206.71.158.30].27234 [192.0.2.1].53 \
    dns QUERY,NOERROR,23839,rd \
    1 .,IN,NS 0 0 0
[45] 2009-01-24 22:22:42.251658 [#1301 eth0 0] \
    [206.71.158.30].2960 [192.0.2.1].53 \
    dns QUERY,NOERROR,41966,rd \
    1 .,IN,NS 0 0 0
[45] 2009-01-24 22:22:42.553856 [#1302 eth0 0] \
    [206.71.158.30].2204 [192.0.2.1].53 \
    dns QUERY,NOERROR,7922,rd \
    1 .,IN,NS 0 0 0
```

Un autre moyen de suivre ces attaques est d'utiliser une version récente de l'excellent dnstop <<http://dns.measurement-factory.com/tools/dnstop/>>. Avec l'option -f, on peut regarder, en temps réel, uniquement les requêtes refusées :

```
Replies: 1 new, 499 total                               Thu Jan 29 16:53:34 2009

Destinations      Count      %
-----
72.249.127.168    201    40.3
69.64.87.156     146    29.3
72.20.3.82       129    25.9
...
```

ncaptool <<https://www.dns-oarc.net/tools/ncap/>> peut également filtrer ces paquets :

```
% ncaptool -i eth0 -mg - dns qname=. qtype=ns flags\#qr
[17 pcap if eth0] 2009-01-30 14:54:34.757562000 [00000000 00000000] \
    [76.9.16.171].6448 [208.75.84.80].53 udp \
    dns QUERY,NOERROR,56008,rd \
    1 .,IN,NS 0 0 0
[17 pcap if eth0] 2009-01-30 14:55:37.391382000 [00000000 00000000] \
    [76.9.16.171].53139 [208.75.84.80].53 udp \
    dns QUERY,NOERROR,56607,rd \
    1 .,IN,NS 0 0 0
```

Dernière méthode pour regarder si une attaque est en cours, la plus "geek", due à Geoffrey Sisson, et implémentée uniquement avec tcpdump :

<http://www.bortzmeyer.org/dns-attaque-ns-point.html>

```
tcpdump -n -s 0 -vvv '  
    udp dst port 53 and  
    (udp[10:2] & 0x8000 = 0) and  
    udp[12:2] = 1 and  
    udp[20] = 0 and  
    udp[21:2] = 2 and  
    udp[23:2] = 1  
,  
# Ici, les explications de chaque ligne (sauf "udp dst port 53" qui est triviale)  
# QR = 0  
# QDCOUNT = 1  
# QNAME = '.'  
# QTYPE = NS  
# QCLASS = IN
```

Un autre logiciel qui peut être utile est en <http://www.smtps.net/pub/dns-amp-watch.pl>. C'est un petit script Perl qui analyse le journal de BIND pour dresser une liste des attaques qui ont laissé une trace dans le fichier, si votre BIND est correctement configuré pour les refuser :

```
% perl dns-amp-watch.pl  
Queries for root (probable DNS amplification attacks AGAINST these IPs  
3564 206.71.158.30  
148 66.230.160.1  
98 63.217.28.226  
51 76.9.16.171
```

Ici, on voit que la principale victime de la journée est 206.71.158.30.

Enfin, vous pouvez aider la recherche sur cette attaque en utilisant ce programme <https://www.dns-oarc.net/node/171> qui fait tourner tcpdump sur votre serveur et transmet les résultats intéressants à l'OARC <https://www.dns-oarc.net/>.

Voir aussi l'article "*DNS queries for*" <http://isc.sans.org/diary.html?storyid=5713>.
Et merci à Samuel Tardieu pour être le premier à m'avoir signalé cette attaque.