23 sept 2008

Les dénis de service

Catégorie : Sécurité Tags : misc

~~Retrouvez cet article dans : Misc 19~~

Lire ce dossier, c'est un petit peu comme choisir la pilule rouge de Morpheus. Pour l'instant vous vivez dans un monde confortable où les dénis de service sont de vieilles attaques obsolètes aux noms rigolos. Ainsi les Ping de la Mort, boink ou autres pepsi n'ont plus leur place dans la société moderne, saine et sécurisée dans laquelle nous évoluons. Dans ce cadre aseptisé les vers font office d'exutoire, tel un match de Rollerball où quelques faibles se font ramasser dans une arène circonscrite.
Lire ce dossier, c'est entrer dans une réalité peu connue et parfois effrayante : les dénis de service sont toujours présents, et plus efficaces que jamais. Et même nos anges gardiens chez les opérateurs ne peuvent pas toujours lutter contre le déchaînement d'attaques aux proportions dantesques. Les cyber-mafias s'organisent, l'extorsion est un business en pleine expansion et des réseaux entiers s'écroulent, sans explication officielle.
Mais il est encore temps, vous pouvez choisir la pilule bleue.

Historique

La genèse

« A l'origine était le ver » (HB, RSTACK Team, RMLL 2003).

Le ver de Morris

Le 2 novembre 1988, le monde électronique connaissait sa première bombe. En effet un proof of concept écrit par un certain Robert Morris Jr. mettait hors d'état de fonctionner 6.000 systèmes sur

Internet, soit environ 15% de la population « active » du réseau.
Ce ver, créé pour se propager en exploitant vulnérabilités et erreurs de configurations, ne contenait pas de charge. Néanmoins, incapable qu'il était de détecter sa présence sur un système, il ne s'est pas contenté de se reproduire sur les systèmes distants, mais également en local. La conséquence est alors évidente : à la longue des milliers de petits process tournaient sur le système cible et provoquaient le premier DoS massif de l'histoire.

Les SYNFloods

Il est difficile d'évaluer la date du premier DoS par SYNFlood. En effet, et comme nous le verrons plus loin dans ce dossier, les SYNFloods font partie des DoS par concepts. Cela signifie qu'ils sont la conséquence directe d'une erreur de spécification d'un protocole ou d'une application. UDP est spoofing ready, TCP est DoS Ready, chacun sa croix. Aussi est-il d'usage de dire que les SYNFloods existent depuis que TCP existe.

Anatomie d'un SYNFlood

Le concept a beau ne pas être nouveau, il trouve toujours des applications de nos jours. Les backbones d'opérateurs sont l'endroit idéal pour observer ces attaques d'un autre temps, qui présentent au moins l'avantage d'être aisément repérables. Dans la mesure où ils ciblent un service applicatif sur une machine donnée, les paquets caractéristiques de l'attaque auront au moins en commun une adresse IP et un port destination, libre après à l'instigateur de spoofer l'adresse IP source de ces derniers comme dans le tableau suivant, extrait d'un cas réel :

IP Source	IP Destination	Port Source	Port Destination
171.24.11.213	217.172.184.27	1142	8767
195.110.78.31	217.172.184.27	1885	8767
20.117.44.79	217.172.184.27	1185	8767
202.140.234.35	217.172.184.27	1108	8767
142.242.37.16	217.172.184.27	1784	8767
...			

Les capacités des systèmes et réseaux actuels ne font qu'accroître les capacités de nuisance de ce type d'attaques, dont les répercutions peuvent se faire sentir jusqu'aux réseaux de cœur !

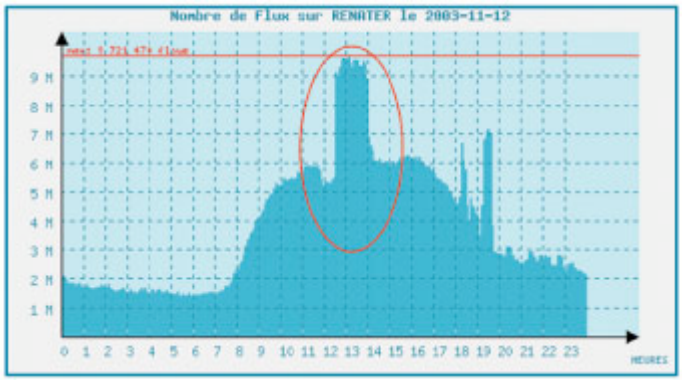

Figure 1 : Évolution du trafic lors d'une attaque par SYNFlood

Les avancées majeures

1995 : Le Ping de la Mort

Cet ancêtre célèbre, vieux de 10 ans, est le premier déni de service fondé sur des anomalies. Il consistait à envoyer des paquets ICMP Echo Request fragmentés de plus de 65.535 octets. Presque aucun stack ne résistait à la puissance de l'attaque dont les effets allaient du freeze du système pendant la durée du bombardement à l'écran bleu de la mort.
La seconde caractéristique de cette attaque est sa simplicité de mise en œuvre. En effet n'importe qui était à même de lancer ping www.pendsmoipouruncon.com -l 65510 au prompt de Windows 95 ou NT4.

Impact du ver Slammer sur RENATER

Aussi connu sous le nom de Sapphire [1], ce ver a, par sa propagation, donné naissance à l'un des dénis de service les plus importants de l'histoire d'Internet. Pour se diffuser, ce ver envoyait un simple paquet UDP à destination de centaines de milliers d'hôtes, engendrant une augmentation considérable du nombre de flux réseau et du débit. Avec les conséquences connues à ce jour : engorgement des réseaux, écroulement des routeurs, le tout aggravé par l'heure (tôt) et le jour (un samedi) de déclenchement. Le réseau RENATER a vu son nombre de flux multiplié par 20 et son débit entrant impacté lourdement. Plusieurs filtres ont été posés au long de la journée, correspondant aux paliers présents sur les graphiques.

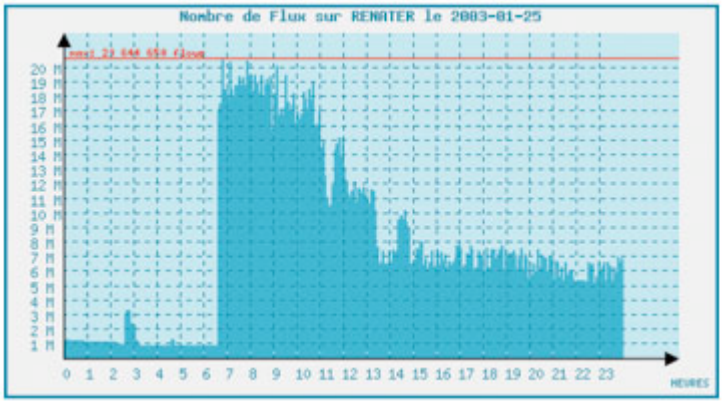

Figure 2a : Évolution de nombre de connexions sous l'effet de Slammer

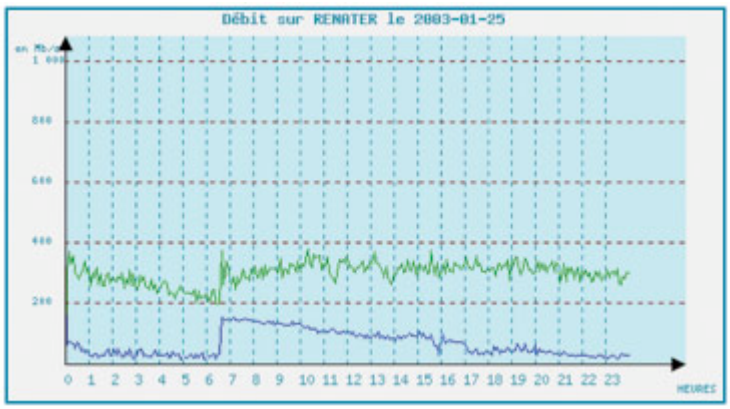

Figure 2b : Évolution du trafic sous l'effet du vers Slammer

Pour la petite histore un fabriquant de systèmes d'exploitation particulièrement vulnérable à cette attaque a développé un patch. Ce dernier protégeait de l'attaque mais plantait l'OS lorsque l'attaque était lancée depuis le système patché...
Il n'en reste pas moins que le ping de la mort a ouvert la voie à des dizaines d'autres attaques s'appuyant qui sur des paquets UDP fragmentés, qui sur des paquets dont les sources et destinations de couches 3 et 4 sont identiques et dont l'effet était mortel, au sens littéral du terme, sur les systèmes d'information.

Smurfing

A peine remis du ping de la mort et de ses petits copains, les systèmes ont dû affronter une nouvelle forme de menace : les attaques par réflexion, initiées par le smurfing. Le principe et la mise en œuvre étaient encore une fois triviaux : pinger une adresse de réseau en spoofant la source. Ainsi tous les hôtes du réseau auquel est destiné le ping répondent à la cible de l'attaque. L'absence quasi généralisée de filtrage de l'époque et la considération de ICMP comme un protocole de contrôle inoffensif permettaient d'obtenir un effet de levier considérable dont les conséquences étaient doubles. D'une part, la gestion de centaines de ICMP Echo Reply par seconde induisait une consommation de ressources processeur importante (genre 100%) et d'autre part le trafic ainsi généré saturait parfois les liens Internet qui dépassaient à l'époque rarement 256 kbps.

Les DDoS

On en parlait plus d'un an avant. Quatre mois plus tôt, un post sur Bugtraq donnait un lien sur les sources. Mais rien n'y a fait, et les 7 et 8 février 2000, Yahoo, E-bay, Amazon et des dizaines d'autres sites web de première envergure tombaient sous les coups des Trible Flood Network(2k), Trinoo et Stacheldraft. L'ère des dénis de service distribués commençait.
Outre l'affligeant constat que le domaine de la sécurité reste essentiellement un domaine dans lequel les responsables préfèrent guérir (trop tard) que prévenir, les DDoS ont prouvé que les nombreux réseaux à la sécurisation douteuse représentent un potentiel considérable en tant qu'effet de levier pour le lancement d'attaques massives. Car ces attaques ne reposaient que sur le volume. Ainsi aucun des trois sites web cités plus haut n'a été mis hors service par les dizaines de milliers de connexions qu'ils avaient à gérer. Mais ce sont les liens opérateurs qui ont été saturés, interdisant de facto toute connexion.

L'age de raison

Code Red

Les briques étaient désormais posées. Néanmoins, les techniques restaient indépendantes les unes des autres. C'est cette dernière barrière que Code Red a su faire tomber, en associant le mécanisme de propagation d'un vers à l'efficacité des dénis de service distribués. La faille Unicode de IIS 5.0 s'est donc retrouvée exploitée afin de diffuser un agent dont l'objectif final était d'établir des connexions sur le site web de la maison blanche.
Heureusement, le créateur du ver a, encore une fois, sous-évalué l'impact de sa création, et plus

particulièrement sa rapidité de propagation. Ainsi, quand il avait prévu qu'il faudrait un mois pour que le nombre d'agents dormants soit suffisant, il a suffit d'à peine une semaine, délai à l'issue duquel le ver a pu être « capturé », désassemblé et analysé. La publication rapide d'outils de nettoyage a alors permis de réduire suffisamment l'impact de l'assaut.

L'avènement du broadband

L'arrivée des liens à haut débit dans les habitations particulières est également un tournant important dans l'histoire des dénis de services. Quand il fallait avoir accès à un réseau universitaire pour pouvoir lancer une attaque efficace, une connexion ADSL peut souvent faire l'affaire. Cette révolution, couplée aux accès WiFi protégés (eh, eh) par du WEP, met à la portée de n'importe qui (ou presque) le lancement d'attaques à des débits considérables et de manière quasiment anonyme.

Les DoS aujourd'hui

Techniques actuelles

Nous sommes loin désormais des innovations technologiques de la décennie précédente. Néanmoins la combinaison d'automatisation et de démocratisation des accès Internet à haut débit n'incite pas à la recherche. Cela en est à un point que l'attaque land, consistant à envoyer des paquets UDP dont l'adresse source et destination ainsi que les ports source et destination sont identiques, a été remise au goût du jour et publiée début mars. La seule modification est le lancement en parallèle des attaques, ce qui était autrefois presque impossible compte tenu des performances des 486...
Pire, le fait que ce type d'attaque ressurgisse indique clairement que les stacks IP n'ont pas été correctement corrigés. S'ils ne plantent pas dès le premier paquet, ils nécessitent toujours des opérations CPU nombreuses et coûteuses. Certes, il était impossible de s'en apercevoir il y a quelques années, mais c'était sans compter avec l'évolution des performances des ordinateurs personnels.
Comme quoi si la stratégie du « jusqu'ici ça va » ne peut être utilisée en politique, elle devient totalement inexploitable en informatique, où tout est gardé en mémoire et la sanction immédiate.

Exploitation des DoS

Un point n'a cependant toujours pas été abordé. Quelles sont les motivations qui mènent à perpétrer un déni de service ? Tout d'abord, il faut s'affranchir d'une excuse fallacieuse et faussement valorisante auprès des cryptos vrais hackers : un déni de service permet de générer une attaque à la Mitnick en descendant le système dont nous allons usurper la relation de confiance. Certes, il est toujours possible de trouver des systèmes qui font tourner les r* services, suffisamment obsolètes pour que l'ISN soit prédictible et qui sont sur des réseaux n'implémentant aucun mécanisme d'anti-spoofing... Bon, mais voila quoi, il faut rester raisonnable.

La guerre des DoS

La taille d'un paquet d'initiation d'une connexion TCP est relativement faible (une soixantaine d'octets en général). Ainsi, l'envoi de multiples paquets SYN n'engendre pas nécessairement une augmentation du débit à destination d'un site, mais peut handicaper le système d'exploitation ou le

serveur applicatif ciblé ou encore le routeur d'accès le desservant. D'un autre côté, les paquets ICMP ou UDP ne nécessitent pas de mise en place de connexion et peuvent transporter des charges utiles conséquentes.
Dans les graphiques suivants, illustrant un cas récent, on observe la décorrélation totale entre le nombre de flux et le débit d'un site. Vers 14h05 a lieu une augmentation anormale du débit en provenance du bloc d'adresses, probablement un UDPFlood ou ICMPFlood : un nombre moyen de paquets pour un volume de données important. Puis vers 16h45, on constate une augmentation anormale du nombre de flux à destination du bloc d'adresses, sans trop de répercussion sur le débit : un SYNFlood. Assisterait-on à un conflit dont l'arme principale est le DoS ?

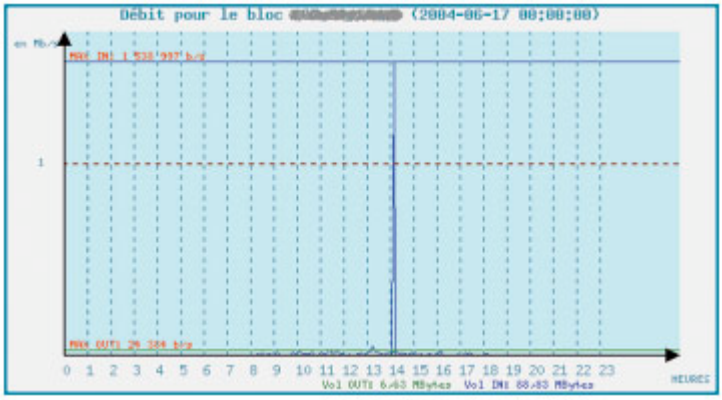

Figure 3a : 14h05 - Augmentation du débit

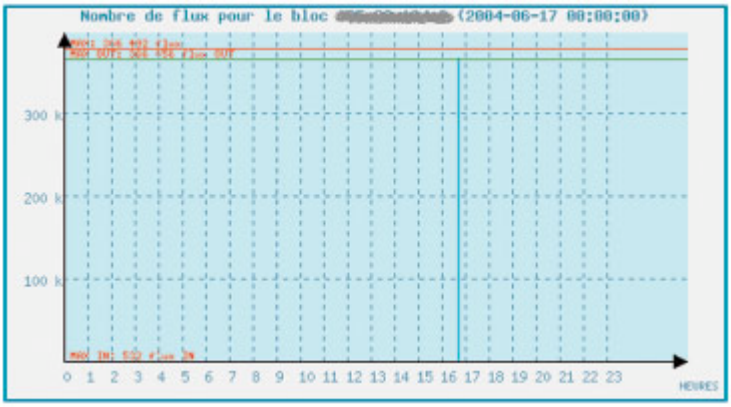

Figure 3b : 16h45 - Augmentation du nombre de connexions

Plus concrètement le premier motif des dénis de service est l'hacktivisme ou cyber-terrorisme en fonction du côté de la barrière (et à terme des barreaux) où l'on se trouve. Ce comportement est une réalité et se base sur une pseudo-information géopolitique comme seule justification.
L'humeur de l'auteur et un QI équivalent à celui d'une huître élevée sur le granit mazouté et radioactif de Saint-Jacut-de-la-Mer sont également des éléments déterminants.
Mais passons aux choses sérieuses et intéressons-nous directement au nerf de la guerre. Prenons une société qui gagne beaucoup d'argent grâce au Net, que ce soit de manière directe (vente en ligne, transactions financières, paris, etc.) ou non (opérateur, ISP, hébergeur, etc.). La disponibilité de vos liens et/ou de vos systèmes est la première préoccupation. Prenons maintenant un méchant. Quelques jours avant un événement important générant beaucoup, beaucoup d'argent chez la cible (tel qu'un match de coupe d'Europe pour les paris en ligne ou une réunion de la Fed pour les sites financiers), un déni de service temporaire de quelques dizaines de minutes est lancé. A l'issue de

cette opération une société de conseil basée aux îles Caïman contacte la victime et lui propose une protection contre cette attaque, pour un coût de l'ordre de quelques pourcents du coût qu'aurait cette attaque si elle était lancée le lendemain. C'est du racket. Ni plus, ni moins. C'est très à la mode et c'est la réalité des dénis de service aujourd'hui.

Conclusion

Les dénis de service ne sont pas seulement un délit (en France en tout cas). Ce sont aussi les actes les plus imbéciles du monde du switch et du baud que nous décrit le Mentor (quoique le spam apparaisse également comme un concurrent sérieux). Rendus plus efficaces par l'évolution rapide des technologies « grand public », ils représentent une vraie menace pour Internet.
L'objectif de ce dossier est de montrer concrètement la réalité de cette menace. Car si des solutions existent, l'incrédulité de nombreux « professionnels » des systèmes d'information en général et de la sécurité en particulier représente un risque plus grand encore.
Pourquoi, pourquoi j'ai pas pris la pilule bleue ?

Références

- [1] MISC 8, « Sapphire », par Éric Filiol

~~Retrouvez cet article dans : **Misc 19**~~

Posté par (La rédaction) | Signature : Renaud Bidou | Article paru dans 

Laissez une réponse

Vous devez avoir ouvert une session pour écrire un commentaire.

« Précédent Aller au contenu »

Identifiez-vous
Inscription
S'abonner à UNIX Garden

Articles de 1ère page

- réception d’images satellites : utilisation d’un système embarqué
- réception d’images satellites : principes de base
- Les chantiers OpenBSD
- Pour quelques bits d'information
- Linux embarqué : BusyBox « in a nutshell »
- La boîte à outils libres pour l’embarqué

- Sécurité avancée du serveur web Apache : mod_security et mod_dosevasive
- Quelques éléments de sécurité des réseaux privés virtuels MPLS/VPN
- Quelles solutions pour Linux embarqué ?
- Les systèmes embarqués : une introduction

Actuellement en kiosque :

Il y a actuellement

- 811 articles/billets en ligne.

Recherche

Catégories

- Administration réseau
- Administration système
- Agenda-Interview
- Audio-vidéo
- Bureautique
- Comprendre
- Distribution
- Embarqué
- Environnement de bureau
- Graphisme
- Jeux
- Matériel
- News
- Programmation

- Réfléchir
- Sécurité
- Utilitaires
- Web

Archives

- octobre 2008
- septembre 2008
- août 2008
- juillet 2008
- juin 2008
- mai 2008
- avril 2008
- mars 2008
- février 2008
- janvier 2008
- décembre 2007
- novembre 2007
- février 2007

GNU/Linux Magazine

- EuroBSDCon 2008 à Strasbourg 18 et 19 octobre
- GNU/Linux Magazine N°109 - Octobre 2008 - Chez votre marchand de journaux
- Édito : GNU/Linux Magazine 109
- GLMF, partenaire de l'évènement "Paris, capitale du Libre"
- GNU/Linux Magazine 108 - Septembre 2008 - Chez votre marchand de journaux

GNU/Linux Pratique

- EuroBSDCon 2008 à Strasbourg 18 et 19 octobre
- Linux Pratique Essentiel N°4 - Octobre/Novembre 2008 - Chez votre marchand de journaux
- Édito : Linux Pratique Essentiel N° 4
- Linux Pratique Essentiel N°4 : Références des articles
- Linux Pratique Essentiel 4 - Communiqué de presse

MISC Magazine

- Misc 39 : Fuzzing - Injectez des données et trouvez les failles cachées - Septembre/Octobre 2008 - Chez votre marchand de journaux
- Edito : Misc 39
- MISC 39 - Communiqué de presse
- Salon Infosecurity & Storage expo - 19 et 20 novembre 2008.
- Misc 38 : Codes Malicieux, quoi de neuf ? - Juillet/Août 2008 - Chez votre marchand de journaux