- 4ck -

(tAd – 3/11/04)

J'sais pas où il a pu récupérer mes coordonnées ce fils de pute, mais le fait est qu'il va manger, et grave. Trois heures qu'il essaye de flinguer ma passerelle ce con, elle tient c'est le principal. Je commence par rechercher les sources de l'attaque de masse en farfouillant mes logs, j'en récupère quatorze adresses IP malveillantes. Etant donné que je me doute que c'est pas quatorze pékins qui attaquent en simultané, j'en déduis que c'est une attaque DDOS, et vu que le trafic reçu bouffe quatre vingt dix pour cent de ma bande passante, j'me doute que c'est pas des connexions RTC, m'enfin ça n'empêche pas que ça ne soit pas des connexions personnelles.

Je commence par rechercher un port d'entrée sur ces machines, histoire de savoir comment mon attaquant s'est approprié le droit de les utiliser, et surtout d'être bien sûr de savoir qui c'est ce fils de pute. Je sollicite les ports les plus communs sur une première machine, la gamme NetBios y passe, des fois que ça aurait pu être facile... rien de concluant. Je continue sur la gamme de serveurs classiques du Web, FTP, HTTP, HTTPS, MySQL, MSSQL... pas plus! Je tente l'accès distant Telnet, SSH, et les ports de toutes les suites de prise en main à distance, j'm'y casse les dents.

«Putasserie d'chiotte de bâtard, nique sa mère!!!» Spliff time! Faut cogiter là. Et se calmer. Putain c'que j'aimerai être un maître Zen parfois. Ou, pas un maître, mais un type qui s'énerve jamais. Ou rarement. Avec juste de quoi être ferme quand il faut. Mais bon, c'est pas l'cas, et faut qu'j'mette un terme à ces conneries. Putain il est passé par où?

J'me décide à scanner une large plage de ports d'un autre serveur, ça mord! Je récolte quelques ports ouverts. J'ouvre une connexion sur le premier, l'en-tête indique une vieille version d'un service Web réputé... merdique. Un tour sur le site, histoire d'identifier un peu de qui il s'agit. Une boite lithuanienne de tuyaux apparemment. Un whois sur son adresse IP pour être sûr de l'information. Ah, non, c'est un gros hébergeur polonais. Bon. Ça à vaguement l'air d'un serveur mutualisé.

Je trouvai la même version de service sur chacune des quatorze machines. Une rapide recherche me permis de trouver un maximum de requêtes à tester pour récupérer des droits d'exécution sur les serveurs. Je les testai une à une sur trois bécanes. Elles répondirent toutes à la même. Je m'immisçai.

L'accès me permet de visiter les disques durs des machines – un vrai moulin - et d'en extirper les logs de connexion, qu'il me fallait analyser.

De ces logs je tirai le script d'attaque, son heure d'exécution. Le script en faute indique bien ma propre adresse pour cible de ses foudres. Je tirai aussi une adresse IP, commune à chacun des logs, utilisant une faille semblable à celle qui m'avait permis d'accéder à ces fichiers - mon coeur palpite, Kickback tape en fond – les données correspondent jusque là.

Un dernier whois, histoire d'identifier le lascar une fois pour toute. IP qui m'indique bien le répartiteur proche de chez lui. J'en étais sûr... Apparemment une IP fixe, bougera pas d'ici demain. Je décide de pioncer, finalement calmé par l'heure et la ganja.

«D'où ça je me suis introduit illégalement sur une machine? Mais où tu vas là mec? Je réponds à mon attaquant...» J'avais eu beau m'expliquer avec mes mots, personne dans l'hémicycle ne compris quoi que ce soit. «Chercher à se faire justice soi-même... c'est mal» et bla et bla. J'ai pris trente six mois fermes, pour l'exemple qu'on disait.