Date: Lundi 04 octobre 2004 à 20:46:58
Sujet: 3 Sécurité et Hacking

Attaque du reseau internet le 25/01/03

Vous l'avez sûrement constaté, le 25/01/03 a 10 heures, Internet ramait. De nombreux sites étaient inaccessibles ou considérablement ralentis (pour PPC et HFR, ça n'a rien à voir).

Vous l'avez sûrement constaté, le 25/01/03 a 10 heures, Internet ramait. De nombreux sites étaient inaccessibles ou considérablement ralentis (pour PPC et HFR, ça n'a rien à voir). Comme pouviez vous l'indiquer le log de votre Firewall, on observait un traffic UDP massif sur le port 1434, ce qui serait la cause directe de ces ralentissements. Le port 1434 UDP étant celui utilisé par Microsoft SQL pour écouter les demandes de requêtes, une hypothèse raisonnable est donc un ver extrêmement virulent. Internet Traffic Report est inatteignable à l'heure actuelle, mais on peut voir l'étendue des dégats sur cette page (Matrix Netsystems). [MAJ]Cette page permet de se rendre compte que UUnet (qui possède la plus grande infrastructure Internet mondiale, filiale de Worldcom) est en première ligne. Claranet semble également touché Depuis ce matin, 10 heures, une attaque de masse d'un ou de plusieurs groupes pirates est en train de mettre à mal le réseau des réseaux. Déjà plusieurs gros serveurs tel que Unet, Level 3, Ld Com ou encore H.P. sont hors service. L'attaque, subdivisées, vise l'Asie, l'Europe et le Pacifique au moment ou nous écrivons ces quelques lignes. Depuis plusieurs mois des "essais" d'attaques, comme le Déni de Service Distribué à l'encontre des root-serveurs ou encore contre UltraDNs. L'attaque semble provenir d'un DDOS basées sur un ver SQL. Depuis quelques semaines déjà, sur le réseau Darknet, les pirates parlaient d'une attaque de masse. On tente de savoir pourquoi ce samedi (Le week-end, pas grand monde travaille, ndlr) Le ver se nomme SQLsnake. Les premiéres alertes à son encontre date du mois de mai 2002. Il passe par le port 1433. Microsoft avait publié une alerte au sujet d'un probléme de sécurité qui visait sa version SQL 7 et son serveur de SQL 2000. Les potes à Bill avait expliqué, qu'un code malveillant appelé à l'époque Voyager Alpha Force, se promenait sur le réseau et volait les mots de passe des comptes d'administrateur. Ce virus avait touché à l'époque, dés son apparition, plus de 2 000 serveurs. Cette faille sql est utilisée par les forums warez pour faire des espaces de stockage. Les serveurs sous Os Linux, Microsoft, ... sont touchés. Les pays, pour le moment, les plus touchés sont : Les Etats-Unis, le Canada, la France, le Taiwan et la Chine, ... Les ports d'origines sont le 1433, 1434. Il semble aussi que le snake tape du côté du 4662. Chose rigolote les groupes warez utilisent cette même faille depuis plusieurs mois, voir le ZATAZ Papier 3, afin de placer leurs contrefaçons sur les serveurs piratés.
bon, apparament,le net as plusiur probleme en cette fin de semaine, PPC qui tombe du a des probleme de maintenance et qui devrait reouvrir d'ici lundi (ils on bcp de site heberger sur les serveur ce qui

n'aide pas)
et comme si cela ne suffisait pas, les serveur son apparamant attaqué. une vague de vers s'en prenderait au routeur de ces dernier, ce qui est considerer comme la plus grosse attaque vue a ce jour envers des les hebergeur/serveur. la plus part des fournisseur safferent a reparrer les degats et a remetre en route leurs systemes au plus vite et de proteger adequatement leurs machine face a ce genre d'attaque. le fait d'avoir plussieur probleme en meme temps peut faire croire que le probleme est commun a chaquun, mias il en est rien. PPC as des probleme de maintenace, et les autre des problemes de vers, reste a savoir une fois le serveur en place sils nauront pas ce 2éme probleme a regler loll. donc pas de pannique, pas la peine denvoyé 4000 mails a votre fournisseur internet, il ny peu rien.