Premier Bilan de l'Attaque du 25/01/2003 contre le réseau - 1/2

Entre 150.000 et 200.000 serveurs auraient jusqu'à présent été touchés, selon Vincent Gullotto, vice-président chez Network Associates de la cellule anti-virus d'urgence et 5 des 13 root serveurs principaux d'internet...

Le ver qui a exploité une faille connue depuis juillet 2002 de la base de donnée maison de microsoft à savoir SQL SERVER a gravement touché internet dés Vendredi Soir.

L'attaque a ensuite duré toute la journée de Samedi. Le pire semblait passé samedi soir, même si ce programme peut encore avoir des effets dans les prochains jours, a expliqué Alfred Huger, directeur de l'ingénierie chez Symantec, société spécialisée dans la sécurité sur internet basée en Californie. Le virus "et très rapide et très efficace', a-t-il ajouté.

Le ver Saphir a commencé à se répandre samedi à 00h00 (05h00 GMT) en Asie et s'est rapidement propagé à des serveurs basés sur la côte Est des Etats-Unis et en Europe du Nord, selon Tom Ohlsson, vice-président du marketing chez Matrix NetSystems, une société de surveillance.

Au plus fort de l'attaque, dans la matinée, environ 20% du trafic de données en transit sur internet a été perdu, une proportion dix fois supérieure à la normale, selon Ohlsson.

Entre autres effets, le trafic audio via internet, souvent utilisé par les institutions financières pour relier entre elles des salles de marché éparpillées dans le monde, a été interrompu.

Le réseau subit encore des latences importantes sur certains fournisseurs d'accés.

Le Sapphire Worm ou le SQL Slammer - nom donné à ce ver car des ingénieurs de beaucoup d'entreprises de sécurité informatique US furent sortis des bars vendredi soir juste aprés minuit de tout urgence pour contenir l'attaque - exploite les résultats d'un buffer overflow sur une faille de sécurité sur le serveur Microsoft.

Une fois la faille trouvée, le ver infecte la machine sans causer aucun dommage : il n'y a pas de destruction de fichier en particulier. Sa seule activité va être de chercher une nouvelle victime en scannant massivement et aleatoirement un ensemble d'adresse IP.

C'est cette activité de scan qui va créer un embouteillage sur le réseau si le ver infecte un nombre n'élévé de machines scannant toutes à leur tour des range d'IP.

Un nombre trés importants d'attaques auraient ainsi été détéctées durant les douzes derniéres heures causant l'arret de 5 des 13 routeurs principaux d'internet (déja touché par une attaque il y a peu de temps). Sur les 8 routeurs'Safe', 2 aurait été prêt de sombrer à leur tour avec des temps de latence avoisinant les 10 secondes.

Le Slammer ne scanne pas des addresses locales donc ne pénétre pas les réseaux internes une fois qu'il touche une porte sur le web comme le fait le ver Nimda. Il se réplique simplement lui même sans causer aucun dommage colatéral au niveau soft.

Ce ver n'est donc pas aussi dangereux qu'un autre ver recemment découvert qui exploite une autre faille du SQL SERVER appellée'vulnérabilité SA/nopassword'. Ce nouveau ver serait beaucoup plus dévastateur car il exploiterait une faille logicielle plutôt qu'une erreur de configuration des serveurs ou un manque de mise à jour sécurité.

Premier Bilan de l'Attaque du 25/01/2003 contre le réseau - 2/2

L'attaque, d'aprés de nombreux articles et experts, aurait commencé en Corée du Sud ou à Honk-Kong ce qui expliquerait pourquoi la Corée du Sud a vu son réseau haut débit complétement saturé au tout début de l'attaque.

Les Experts recommendent aux administrateurs systéme de fermer immédiatement le port SQL de tout leurs serveurs - le ver n'utilisant que le port 1434 en UDP (LE port de monitoring de SQL). De plus ils rappellent que la faille de sécurité avait été signalé depuis plusieurs mois par Microsoft et que le patch est disponible sur le site de Microsoft à cette adresse :
Patch SQL

ou encore est disponible dans le SQL 2000 service pack à :
SQL 2000 service pack

Au final le réseau a encore montré pour la deuxiéme fois en quelques mois sa solidité et surtout sa capacité de réaction. Paralyser complétement internet est une chose difficile même si cette deuxiéme alerte est plus chaude que la derniére.

L'attaque a aussi montré la nécessité de bien suivre les alertes sécurité et de patcher correctement les serveurs... pour une fois Microsoft ne peut pas etre accusé de tout les maux.
En France l'impact semble avoir été minime : des sites comme grenouille.com en ont fait les frais, certains liaisons de FAI furent pertubés dans la matinée.
Le fait que cela arrive le Week End et principalement dans la nuit ou la matinée en France a réduit l'impact réel au niveau des internautes français. Aucun media national en a en tout cas fait écho.

Et derniére question : pourquoi et par qui ?
Il est pour l'instant impossible de répondre à cette question.

Certaines rumeurs avancent l'hypothése d'une protestation contre le nouveau systéme PALLADIUM (qui va changer de nom) de Microsoft.

Les sites d'information grand public français à coté de la plaque... réactivité nulle

Alors qu'Internet subit l'attaque la plus importante de son histoire, faites le tour des sites web d'information en France : Lemonde, 01net, Zdnet...
Samedi 25 janvier à 19 heures, apparament, rien ne se passait !
Ne parlons même pas des chaines d'information télévisées.
Réactivité nulle de nos media.
Seuls les sites communautaires ou "libres" sortent l'information et la commente : activité sans précédent des forums.

Les médias Français seraient-il allergiques aux nouvelles technologies ?