Virus: Doomjuice fait des petits

Comme son grand frère, Doomjuice.B (ou Mydoom.D) se propage de la même manière que son prédécesseur découvert le 9 février en recherchant sur Internet tous les ordinateurs infectés par Mydoom.A ou Mydoom.B, selon l'éditeur Kaspersky Labs.

La sale bête est plus vicieuse, puisque Doomjuice.B place dans son entête une adresse http aléatoire qui le rend encore plus difficile à repérer et à filtrer. Dès qu'il a établi la connexion avec l'ordinateur infecté via le port 3127 ouvert par Mydoom, Doomjuice.B envoie sa copie qui sera exécutée par la partie cheval de Troie de Mydoom. Traduction: Doomjuice.B ne se propage pas par e-mail ou par les plateformes de P2P. Il utilise la « back door » ouverte par Mydoom sur les ordinateurs pour attaquer. L'objectif principal de Doomjuice.B est de lancer une attaque par déni de service sur le site de Microsoft. Le ver se copie dans le répertoire système de Windows sous le nom « REGEDIT.EXE » et s'inscrit dans la clé de la base de registre qui gère les lancements automatiques. Ensuite, il vérifie la date du système. Si la date est comprise entre le 8 et le 12 du mois, l'attaque par déni de service n'est pas lancée. Il en va de même si le mois correspond au mois de janvier. Autrement dit, l'attaque par déni de service orchestrée par Doomjuice.B touchera le site www.microsoft.com chaque mois, à l'exception du mois de janvier, du 1er au 8ème jour et du 12ème jusqu'à la fin du mois. Cette attaque se traduira par l'envoi d'une multitude de requêtes http vers le port 80 du site de Microsoft. Néanmoins, l'éditeur a depuis longtemps préparer ses arrières. La précédente version de Doomjuice qui devait aussi attaquer le site de la firme n'a pas fait de grands dégâts. **Le rythme d'apparition des versions s'accélère, le danger grandit**

Plus que le volume de propagation de MyDoom en janvier, s'est le rythme auquel apparaissent les nouvelles versions qui est inquiétant. S'il ne s'agissait que de recopie de code avec des modifications mineures, ce rythme se serait pas inquiétant en soi, mais il s'agit au contraire de modifications que nous pourrions qualifier de concertées.

Ainsi MyDoom-A s'attaque à SCO, puis MyDoom-B s'en prend à Microsoft, puis Doomjuice-A profite des failles ouvertes par MyDoom, qu'il continue de diffuser, et aujourd'hui Doomjuice-A se propage en changeant d'identité, et sans le code MyDoom. Quelle sera la prochaine évolution ? Déjà, les pirates modifient le code afin se protéger et de se protéger du risque de remonter à la source. De plus, la virulence d'une attaque est généralement immédiate, alors que précédemment les temps de propagation étaient beaucoup plus longs. Quant à la dérive mafieuse, elle semble pour le moment ne concerner principalement que les auteurs de spam, mais cette tendance peut aussi s'inverser rapidement. Mise à jour, anti-virus et pare-feu seront d'actualité pour longtemps encore !