WebWizard Blitz-News – Thema: Sicherheit – vom 27.04.2008

Bot Netz durch Infiltration eliminieren

Französische Forscher haben sich exemplarisch nun den Storm Worm genauer angesehen. Das riesige Botnet, das im Internet für Spams, DDOS-Angriffe und Viren sorgt, soll endlich selbst angegriffen werden.

Bisherige Botnetze, also von Kriminellen zusammengeschaltete Rechner, die dann für Betrügereien und den Versand von Spam-eMails entwendet werden, wurden am besten am Kopf erwischt. Schaltet man die Zentrale aus, verliert das Botnetz die Steuerung und wird damit wertlos. Bei Storm Worm und anderen modernen Botnetzen ist das nicht mehr so - sie steuern sich gegenseitig über ein P2P-Netzwerk. Eine zentrale Steuereinheit kann man da nicht ausmachen und eliminieren, die Eurecom-Forscher mussten also andere Wege aufzeigen.

Der StormWorm nutzt Overnet zur Verteilung von Nachrichten und Programmen im Botnet. Overnet kann man sich wie ein großes Filesharing-Netzwerk vorstellen, das auch für legale Zwecke verwendet wird - es gilt also vorrangig, normale Nachrichten von denen des Storm Worm zu unterscheiden und die letzteren auszuscheiden.

Zum Jahreswechsel erkannten die Forscher bis zu 40.000 aktive Knoten im Overnet-Netzwerk, die auf Storm Worm-Zombies (also 'übernommene' und missbrauchte Computer) basieren.

Zur Zerstörung des Botnetzes müssten die Wissenschaftler die vom Virus befallenen Rechner selbst ändern, was rechtlich nicht ganz einfach sein dürfte. Einen Angriff auf das Netzwerk der Kriminellen könnte also daran scheitern, dass man selbst in rechtliche Fallen tritt. Technisch wäre sie laut den Informationen der Wissenschaftler aber machbar.

Die beim Usenix-Leet 08-Treffen gezeigten Möglichkeiten der Erkennung von Bot-Aktivität im P2P-Netzwerk könnten aber noch einen Nutzen haben: Langfristig kann man damit auch die Drahtzieher und den Ausgangspunkt der Plage lokalisieren. Die Forscher könnten also den Grundstein gelegt haben, um den Bot-Betreibern endlich das Handwerk zu legen.