



Botnets

Botnets

Wie gut schlafen Sie eigentlich, wenn Sie an Ihr Computernetz denken? Alles im Griff mit Firewall und sonstigen Schutzeinrichtungen? Dann wird es höchste Zeit, schleunigst aufzuwachen und der Realität ins Auge zu schauen. Denn während Sie noch brav den Traum einer heilen Netzwelt träumen, sind ganze Armeen von gekaperten Rechnern, so genannte Botnets, vielleicht schon dabei, auch Ihr Netz zu knacken. Ohne dass Sie etwas wegfiltern oder verhindern können. Als erschreckendes Beispiel eines traurigen Computeralltags gelten zurzeit die mehr als 166.000 so genannten 'Zombie-Rechner' aus 74 Ländern, die im Juli 2009 per (DdoS)-Angriff die Server von Behörden und Unternehmen in den USA und Südkorea mit gleichzeitigen Anfragen überlasteten, während eingeschleuste MyDoom-Trojaner versuchten, deren Festplatten zu löschen. Schlimm zu wissen ist dabei, dass diese 'Armeen' Server von mehr als einem Terabyte Traffic pro Sekunde lahm legen können - und damit ein einträgliches Geschäft für Cyberkriminelle darstellen, die hier die größten illegalen Einnahmequellen des Internets vorfinden.

'Botnets' bestehen aus einzelnen Computern oder Servern, die ohne Wissen ihres Besitzers von Hackern ferngesteuert werden. Beim Aufbau ihrer 'Armeen' greifen sie neben privaten PC's auch Netzwerke kleiner Unternehmen oder Universitäten an. Einmal 'rekrutiert', steht der Rechner voll unter der Kontrolle der Netzwerkbetreiber, von denen er via Web regelmäßig seine Befehle erhält. So fanden Sicherheitsexperten auf einem Server in der Ukraine unter den Daten von 160.000 infizierten Computern auch Kundendaten und Angestellten-E-Mails einer US-Bank. Diese massenhaft erbeuteten Daten bringen viel Geld durch die Vermietung der Kapazitäten an Dritte und bilden die Grundlage zu Erpressungen. Legt eine DoDS-Attacke die Server lahm, kommen die Geschäfte der Geschädigten zum Erliegen, die dann die Forderungen der Cybererpresser oft erfüllen.

Dank Internet und gehackten Servern müssen sich die Täter nicht einmal dort befinden, wo die zentralen Masterserver stehen. Als im April 2009 das bisher größte Botnet aufflog, zeigte sich, dass gerade mal sechs Cyberkriminelle von einem ukrainischen Server aus knapp zwei Millionen Rechner weltweit kontrollierten – darunter viele aus dem Bereich der US-Regierung. Zur Einschleusung ihres Programms nutzten sie unter anderem Sicherheitslücken in Programmen wie Internet Explorer, Firefox oder PDF. Wen das noch kalt lässt, der hat entweder kein Computernetz oder nichts zu verlieren.