Und ewig grüsst das Botnetz

Ein Artikel von mir in der taz über Botnetze. Da dort die Links fehlen und mir mein Original und auch meine Überschrift besser gefallen als das, was in der taz zu lesen ist, hier mein Text:

Das drittgrößte Botnetz der Welt wurde abgeschaltet. Das verkündete Atif Mushtaq, ein IT-Experte von FireEye – das britische Unternehmen verkauft Firmen Sicherheitssoftware gegen „Cyberkriminalität". Das so genannte Grum-Net soll für rund die Hälfte des weltweiten Aufkommens unerwünschter E-Mail-Werbung (Spam) verantwortlich gewesen sein.

Das Grum-Botnet wurde schon 2008 entdeckt und war spezialisiert auf E-Mails, die für pharmazeutische Produkte warben – fast immer für angebliche Potenzmittel. Botnetze sind von Malware infizierte Rechner, die von Spammern dazu benutzt werden, ungeheure Massen von E-Mails zu versenden oder die sogar in der Lage sind, Schadsoftware nachzuladen, damit der betroffenen Computer übernommen und missbraucht werden kann, ohne dass dessen Besitzer das merkt. Die zentralen Kommandoserver, die Befehle versenden, stehen oft in Ländern, die beim Kampf gegen Spam nicht unbedingt die Avantgarde bilden – beim Grum-Botnet etwa in Russland und Panama.

Botnetze können nur existieren, weil Server im Internet schlecht gewartet werden, weil private Nutzer sich nicht für Sicherheit interessieren oder sich auf den trügerischen Schutz von Anti-Viren-Software verlassen, und weil viel Software in Umlauf gelangt, deren Quellcode nicht offen („Open Source") ist – die eine nützliche Funktion verspricht, in die aber auch eine Spionage- oder Schadfunktion eingebaut worden ist. Da sich die meisten privaten Nutzer kaum für Technik interessieren, gehört es zu den Standard-Funktionen der Malware, den Virenscanner des betroffenen Rechners zu umgehen oder abzuschalten.

Wie viele Computer Teil eines Botnetzes sind, kann niemand genau sagen – die Verlautbarungen der Anti-Viren-Software-Lobby suggerieren, dass ein Fünftel aller Rechner im Internet angeblich schon befallen seien. Das Klappern gehört bekanntlich zum Handwerk. Nach Angaben von Vinton G. Cerf, einem der „Väter“ des Internet und „Google-Evangelist“, sollen es sogar ein Viertel aller Computer im Internet sein.

Die Sicherheitsfirma Symantec behauptete sogar, Cyberkriminalität wie Botnetze, Phishing-Attacken und der Versand trojanischer Pferde per E-Mail seien ein Exportschlager Deutschlands. Das kann an den im europäischen Durchschnitt schlechten oder gar nicht vorhandenen Internet-Kenntnissen der Nutzer liegen, an der hohen Verbreitung der für Malware-Attacken besondern empfänglichen mobilen Endgeräte wie Smartphones, und daran, dass so genannte „sozialen“ Netzwerke wie Facebook hierzulande beliebt sind. Diese sind indirekt besonders effektive Einfallstüre für schädliche Software, weil sie vom Nutzer verlagen und ihn dazu erziehen, die von Experten empfohlenen Sicherheits-Features – wie das Verbot „aktiver Inhalte“ – abzuschalten. Wer Datenspionage per default erlaubt, öffnet potentiell auch Einfallstore für bösartige Dateien, die den Rechner zum Teil eines Botnetzes machen können.

In den letzten Jahren häuften sich die Meldungen über „entscheidende Schläge“ gegen Botnetze – wie Srizbi, Rustock, Mega-D, Pushdo.A, Storm, and Waledac. Das Waladec-Botnetz sollte nach Angaben von Microsoft bis zu 1,5 Milliarden Spam-Mails täglich verschickt haben, das Rustock-Botnetz sogar bis zu rund 44,1 Milliarden. Obwohl diese Botnetze durch eine Kombination juristischer und technischer Aktionen lahmgelegt wurde, nahm die Zahl der unerwünschten Werbemails aber nicht signifikant ab.

Der Kampf gegen Spam ist ein Kampf gegen eine Hydra, die immer wieder nachwächst. Der Versand unerwünschter Werbung mit Hilfe eine Botnetzes ist ein erfolgreiches, effektives und

kostengünstiges Geschäftsmodell. „Sie haben dreißig Trilliarden Dollar gewonnen – klicken sie hier!“ – „Ihr Konto wurde gesperrt und wenn sie nicht 100 Euro sofort überweisen, schalten wir ihren Rechner ab.“ Es gibt Leute, die tun alles, was man ihnen sagt. Da die menschliche Dummheit bekanntlich unendlich groß ist, wird es daher auch Botnetze unendlich lange geben.