Dossier – Piraten

Fortsetzung von Seite 25

Die wahre Wirkungsweise dieses Trojaners: Er öffnet auf den infizierten Rechnern nunmehr eine Hintertür, durch die sich die Software „Geobot“ einschleichen kann. Der *Zeit*-Autor Lars Reppesgaard recherchierte, dass mit auf diese Weise gekaperten Computern inzwischen ganze Schatten-Netzwerke entstanden sind. Dazu Dennis Jenkin von der Antivirus-Firma Kaspersky Labs: „Diese verborgenen Netzwerke bestehen aus bis zu 50.000 gekaperten Computern und werden dazu benutzt, um Spam-Mails zu verschicken. Der Versand einer Million dieser Mails bringt immerhin bis zu 10.000 Euro.“

Hijacker und Zombies

Bereits der gängige Fachjargon führt die Gefährlichkeit dieser und ähnlicher Aktivitäten plastisch vor Augen: Der Vorgang selber wird gerne als „Computer Hijacking“ beschrieben, und die dadurch entstandenen Cluster von per Fernsteuerung missbräuchlich verwendbaren Computern werden zumeist als „Zombie Networks“ bezeichnet. Aber auch der Variantenreichtum der über Netzwerke von gekidnappten Computern erfolgenden Aktionen müsste in Wahrheit jeden Internet-User nachhaltig beunruhigen: Neben der Verbreitung von Virenprogrammen und Spam-Mails und neben der Auskundschaftung persönlicher Daten können Zombie Networks auch für massierte Attacken auf Websites und Firmennetze eingesetzt werden. Und dies mit einer „digitalen“ Gewalt, dass in der jüngsten Vergangenheit selbst die mächtigen Server der Internet Professionals wie Amazon, Microsoft, Symantec oder Yahoo dem nicht gewachsen waren und für Stunden offline gehen mussten.

Meist nicht mit geballter geklauter Computer-Power, sondern mit umso mehr verbrecherischer Intelligenz arbeitet eine andere, jüngst zur rechten Plage gewordene Kategorie von Netzpiraten: die so genannten „Phisher“. Der Begriff „Phishing“ leitet sich vom Fischen (englisch: fishing) nach persönlichen Daten ab. Die anonymen Täter wenden dabei gleich mehrere Tricks an: In massenhaft versendeten und oft sehr glaubwürdig wirkenden Phishing-Mails fordern sie die Empfänger im Namen etwa einer Bank oder eines Versandhauses auf, ihre Zugangsdaten durch erneutes Eintippen zu bestätigen – und zu diesem Zweck einen Link zur entsprechenden Website anzuklicken. Macht dies der vertrauensselige Benutzer, landet er jedoch nicht auf der Homepage der Bank, sondern auf einem oft hervorragend nachempfundenen Internet-Konstrukt der Daten-Diebe, dem meist kaum anzusehen ist, dass es sich dabei um eine geschickte Fälschung handelt.

Traue keiner Internet-Site

Wenn der Benutzer dann noch brav der Aufforderung folgt, seine Pin- und Tan-Codes oder seine Kreditkartennummer einzugeben, sitzt er schon in der Falle der „phishenden Freibeuter“. Die hochwertvollen Daten sind futsch, der User kann nur hoffen, dass er nach dem Entdecken dieser Täuschung sein Konto nicht geleert vorfindet. Die getürkte Internetsite hingegen ist kurz darauf (durchschnittlich nach fünf Tagen) wieder spurlos aus dem Netz verschwunden. Und wer glaubt, die Urheber dieser hinterlistigen Phishing-Aktion seien in dubiosen, weil den internationalen Rechtsnormen nicht genügenden Staaten zu suchen, täuscht sich: Ein Drittel der Phishing-Aktionen hat seinen Ursprung in den USA.

Wie schmerzhaft dem auch sei: Ihre Arbeit wird den Netzpiraten durch das sorglose Verhalten der Internet-User enorm erleichtert, zeigt eine Studie aus den USA, welche AOL und die National Cyber Security Alliance (NCSA) im Dezember 2005 durchführten. Nur 42 Prozent der PC-Benutzer konnten mit dem Begriff „Phishing“ überhaupt etwas anfangen, und relativ gut informiert waren noch beträchtlich weniger: nämlich bloß ein Viertel der Befragten.

Und während die Mehrheit der Benutzer (83 Prozent) überzeugt war, ihren Internet-PC ausreichend gegen gefährliche Übergriffe geschützt zu haben, ergab die Analyse der konkreten Sicherheitsmaßnahmen ein völlig anderes Bild. Satte 81 Prozent der PC zeigten gravierende Mängel bei den Schutzmaßnahmen gegen Datenraub. 56 Prozent hatten entweder gar keinen Virenscanner installiert oder nicht up to date. 44 Prozent der Befragten hatten keine probat funktionierende Absicherung, etwa durch eine Firewall.

Last but not least: Die Brisanz dieser Fakten wird durch zwei weitere Erkenntnisse der AOL/NCSA-Studie noch verschärft. Konkret: 74 Prozent der Befragten benutzen ihren Computer für sensitive Transaktionen wie Online-Banking. Und immer noch 68 Prozent haben auf ihrem Heim-PC kritische Daten wie etwa berufliche Korrespondenz oder Informationen zur gesundheitlichen oder finanziellen Situation gespeichert. Ergänzt wird dieses bedenkliche Bild durch Einschätzungen der Analysten von Jupiter Research, welche den wachsenden Markt für Onlineshopping für das Jahr 2005 mit 26 Mrd. US-Dollar beziffern.

Ein wenig Paranoia hilft

Fazit aus alledem: Ein „offenes Meer an Gelegenheiten“ bietet sich den bösen Netzpiraten. Oder anders gesagt: eine üppige Landschaft von zwar vernetzten, jedoch relativ schlecht geschützten Internet-PC mit ihrer diversen Reichhaltigkeit an wertvollen persönlichen Daten. Und damit abschließend kein Missverständnis aufkommt: Selbst sträflich leichtsinnigen Opfern darf daraus keine Zuweisung einer Mitschuld erwachsen. Doch angesichts des kriminellen Raffinements der professionellen Netzpiraten könnte uns unbedarften Internetbenutzern ein Quäntchen jener Paranoia, welche die Medienkonzerne den vergleichsweise harmlosen jugendlichen Downloadern entgegenzubringen pflegen, gewiss nicht schaden.

Jakob Steuerer

http://de.wikipedia.org
www.staysafeonline.info

Naive Hacker und wuchernde Würmer

Seinerzeit agierten die „Code Warriors“ meist noch aus lauteren Motiven. Und heute? Ein kurzer historischer Streifzug.

Erfahrene User wissen längst: Gegen Internet-Würmer helfen weder Fliegenklatsche noch Gasmaske. Foto: Sandia National Laboratories, Randy Montoya

Wer weiß das schon: So mancher der heutigen Superstars der Computerszene begann seine Laufbahn als – Hacker! Darunter der junge Bill Gates, aber auch der spätere Apple-Gründer Steve Jobs, der die hackerische Manipulation der Telefon-Systeme blendend beherrschte. Dennochhatte keiner der beiden etwas Abgrund-Böses im Sinn: Für Gates stand eher die sportliche Ambition als Programmiergenie im Vordergrund, und der damals noch „arme“ Steve Jobs senkte solcherart seine Telefonkosten. Zudem beendete der kurz danach einsetzende Mega-Erfolg der ganz legalen Art ihrer beider Hacker-Karriere.

Ein unfreiwilliger Zerstörer

Zweifelhaften Ruhm hingegen erwarben sich alsbald ganz andere – und fallweise sogar unfreiwillig. So löste im Herbst 1988 ein hackender US-Student namens Robert Morris jr. vom Keyboard seiner universitären Unix-Workstation aus (mit einigen simplen Befehlszeilen) die erste ausgedehnte Virenkatastrophe aus. Das kleine Programm, seither als Prototyp eines „Internet-Worm“ berühmtberüchtigt, legte binnen weniger Stunden Ausbreitungszeit empfindliche Teile des US-Internet kurzerhand lahm. 3.000 Systeme waren davon direkt betroffen, 250.000 Rechner gefährdet. Die prominentesten Opfer: Nasa, Pentagon, die Elite-Universitäten Stanford, Cornell und Berkeley. Der Schaden belief sich auf zig Mio. Dollar.

Morris' Wurm (eigentlich ein „gutartiger“ Computervirus) wies nämlich einen winzigen, aber folgenschweren Programmierfehler auf, durch den er sich in den Systemen, in die er eindrang, wie wild vermehrte. Folge: Die „angesteckten“ Computer „hängten“ sich aus Überlastung „auf“, Großrechner-Netzwerke lagen tagelang brach. Dabei empfand sich Morris als „edler Hacker“, er wollte bloß zeigen, dass die Unix-Server des Internet schwere Sicherheitslücken aufwiesen. Dennoch: Er wurde zu Gefängnis und einer satten Geldstrafe verurteilt.

Heute wirkt jedwede idealistische Naivität, die noch Gates, Jobs oder sogar Morris bewegte, längst deplatziert: In den „Netzwerken des freien Meinungsaustausches“ tummeln sich gefährlich wirkungsvolle Gesellen, welche aus egomanen oder finanziellen, aus destruktiven oder omnipotenten Motiven agieren. Der Sicherheitsexperte Rob Clyde, Mitbegründer von Axent Technologies, analysiert, dass sich in der Zwischenzeit rund 30.000 Sites der hackerischen Sache verschrieben haben, das Gros davon mit dubiosen bis hin zu kriminellen Ambitionen.

Und potenzielles Angriffsziel ist jedermann: So kam selbst der Branchengigant Microsoft durch eine Hacker-Attacke gehörig ins Schleudern, berichtet die US-Branchen-Insiderin Amy Hart: Am 14. Oktober 2000 erhielt ein Angestellter von Microsoft eine E-Mail mit einem harmlos wirkenden Attachment. Dieses enthielt jedoch ein kleines Programm, welches sich automatisch im System installierte und einen Outsider-Zugang zum PC des Mitarbeiters und dessen Passwörtern öffnete. Eine ärgere Panik, etwa durch ein Übergreifen dieser Mechanismen auf das interne Netzwerk von Microsoft, konnte gerade noch verhindert werden.

Nur Bill Gates reagierte gelassen, denn ihm war zuvor schon klar gewesen: Das Internet hat seine jugendliche Unschuld längst verloren.

Jakob Steuerer