Piraten-Software - Wenn Schadprogramme den PC kapern

Mit Sicherheitslücken lässt sich viel Geld verdienen. Das wissen nicht nur die Hersteller von Schutzprogrammen, sondern auch die Programmierer von Viren, Würmern und Trojanern. Die haben mittlerweile eine regelrechte Industrie aufgebaut, die von Datenspionage, Spam-Versand und Auftragsmorden an Webservern lebt. Und Ihr PC dient womöglich schon als Werkzeug.

Die Zeiten haben sich geändert. Früher war es eine Frage der Ehre, dass sich ein Virus möglichst weit verbreitete, um dann laut auf sich aufmerksam zu machen. Damit stillten die Programmierer ihr Geltungsbedürfnis. Heute geht es nur noch ums Geld. Fälle wie der des deutschen Entwicklers von Agobot und Phatbot, der internationales Aufsehen erregte, motivieren nicht nur Jugendliche dazu, mit selbst geschriebener Bot-Netz-Software ihr Taschengeld aufzubessern. Auch professionelle Programmierer verdienen hier ihr Geld.

Die Qualität der Schadsoftware hat darunter keineswegs gelitten. Sie nutzt teils noch unbekannte Sicherheitslücken, um sich auf fremden Computern einzunisten. Bot-Net-Clients versenden unter Kontrolle von außen Spam, spionieren Daten aus, laden bezahlte Werbung oder legen durch verteilte Denial-of-Service-Attacken fremde Server lahm. Sie verstecken sich durch Rootkit-Techniken (siehe c't 2/07, S. 86) erfolgreich vor Anti-Viren-Programmen, sodass sie - auch dank Flatrate - meist lange unentdeckt bleiben. So gelingt es, Netze aus zigtausend Bots aufzubauen. Diese werden dann an Auftraggeber vermietet. In solchen Netzen hängen nicht nur Computer unvorsichtiger Privatanwender, sondern auch Firmenrechner; selbst die NASA war schon betroffen.

Besonders wertvoll für Bot-Netz-Betreiber sind gekaperte dedizierte Server bei Webhostern. Ist ein solcher Server eingerichtet, schaut der Besitzer meist nur noch selten vorbei. Die Angreifer können sich ungestört breit machen, nicht selten optimieren sie das System auf ihre Bedürfnisse und tauschen beispielsweise den Kernel aus. Die Netzanbindung der Server ist sowohl in Up- wie in Download-Richtung schnell. Sie eignen sich damit als Steuer- und Verteilzentrale in Bot-Netzen oder als Server für Phishing-Sites, die beispielsweise mit nachgemachten Bankseiten den Besuchern Zugangsdaten entlocken. Damit die wertvollen Server dabei nicht zu schnell auffliegen, leitet ein System aus ständig wechselnden Bots die Zugriffe weiter.

Um unentdeckt zu bleiben, versuchen die Eindringlinge, auf dem infizierten System möglichst wenig Schaden anzurichten. Es gibt sogar Beispiele, die das System nach anderen Schädlingen durchsuchen, und unliebsame Konkurrenz entfernen. Doch von Mutualismus kann keine Rede sein. Ein versteckter Bot-Netz-Client stiehlt dem Anwender Ressourcen. Wird der infizierte Computer für Straftaten missbraucht, hinterlässt er seine IP-Adresse als Spur, der die Ermittlungsbehörden folgen, um den Rechner womöglich zu beschlagnahmen. Mehr zur rechtlichen Situation von Besitzern infizierter Rechner lesen Sie im Kasten auf Seite 78 in c't 2/07.

Organisiertes Verbrechen

Die Szene ist gut organisiert, die Aufgaben werden verteilt. So gibt es die Programmierer, die oft schlau genug sind, sich aus strafrechtlich Relevantem herauszuhalten, und die Logistiker, die einerseits für die Verbreitung von Schadsoftware sorgen und andererseits den Kontakt zu zahlenden Kunden herstellen. Die Leute fürs Grobe bringen Erfahrung mit traditionelleren Formen des Ver-

brechens ein, indem sie etwa durch Phishing erbeutetes Geld waschen oder lästigen Mitbewerbern auf die Füße steigen. Und schließlich sind da noch die Marketender, die gegen Bezahlung Nützliches wie unverdächtige Domains, gestohlene Identitäten oder Kreditkartendaten herbeischaffen.

Man gibt sich interessierten Talenten gegenüber freundlich und offen. Über bekannte Foren wie Ryan1918 findet die erste Kontaktaufnahme öffentlich statt. Dort bieten die Rookies stolz ihre Bot-Netze zur Miete an, mit oft offensichtlich gefälschten Screenshots, in denen die Zahl der angeschlossenen Clients um den Faktor 10 bis 100 übertrieben wird. Hier hat sich eine Community gebildet, zusammengeschweißt durch ein starkes Gruppengefühl und den Reiz des Verbotenen. Es werden auch schon mal erbeutete Kreditkartendaten feilgeboten, doch letztlich geht es darum, vom Talentsucher einer größeren Organisation entdeckt zu werden.

Aber nicht jeder spielt freiwillig mit. So berichtet McAfee in seinem Cybercrime-Report, dass die kriminellen Banden unter anderem talentierte Studenten als Programmierer anheuern. Sie gehen dabei mit traditionellen Mafia-Methoden vor und führen die Helfer zunächst über lukrative, einfache Aufgaben an die Grenze der Legalität und dann darüber hinaus. Will jemand doch noch abspringen, wird er durch plumpe Erpressung motiviert. Ein Sicherheitsexperte, den wir für diesen Artikel befragten, bat uns, seinen Namen keinesfalls zu nennen. Die Szene reagiere immer brutaler und auch in Deutschland würden Leute mittlerweile direkt bedroht.

Die Szene profitiert nicht nur von den aktiven Helfern. Viele Anwender unterlassen es aus Leichtsinn, bekannt gewordene Sicherheitslücken durch regelmäßige Updates zu schließen. Hinzu kommt, dass viele PC-Nutzer Schwarzkopien von Windows nutzen und aus Angst vor Entdeckung auf Online-Updates verzichten. Das erleichtert die Verbreitung von Schadsoftware ungemein.

Profis legen allerdings Wert auf Aktualität und die Preise für bis dato unbekannte Sicherheitslücken steigen. Ging der WMF-Exploit für Windows im Dezember 2005 noch für zirka 4000 US-Dollar über den Tisch, werden derzeit für Vista-Exploits bis zu 50 000 Dollar geboten. Der AV-Hersteller Trend Micro unterwanderte kürzlich eine Cracker-Börse, auf der so gut wie alles verschachert wurde, was im Bereich Internet-Kriminalität eine Rolle spielt: vom eBay-Account (7 Dollar) über Kreditkartennummern (inklusive dreistelligem Sicherheitscode und Ablaufdatum 25 Dollar) bis hin zu fertigen Bot-Netz-Clients für bis zu 20 000 Dollar und unbekannte Sicherheitslücken in Applikationen, die je nach deren Popularität bis zu 30 000 Dollar bringen. Der Sicherheitsreport 2006 von MessageLabs Intelligence beziffert die Wochenmiete für ein betriebsbereites Bot-Netz mit 25 bis 60 Dollar pro 1000 Clients.

Gut im Geschäft

Auf der dunklen Seite lassen sich derzeit im Wesentlichen drei Geschäftsmodelle für das Ausnutzen von Sicherheitslücken beobachten: Spam, Spionage und Sabotage. Spam gibt den deutlichsten Hinweis auf den Erfolg der Bot-Netze: Im letzten halben Jahr stieg die lästige E-Mail-Werbeflut sprunghaft an (siehe c't 2/07, S. 80).

Spionage und Datenklau finden hingegen im Verborgenen statt und werden oft gar nicht publik. 2005 gelangten Unbekannte in den Besitz der Daten zu rund 40 Millionen Kreditkarten auf Servern der Firma CardSystems, die im Auftrag von MasterCard und Visa Zahlungen abgewickelt hatte.

2006 wurden vor allem Daten von kleineren Web-Shops mit Lücken in der Server-Software professionell abgeräumt.

Für den Betroffenen ist es der schlimmste anzunehmende Einbruch, wenn durch gezielte Industriespionage wertvolle Geschäftsinformationen in die Hände der Konkurrenz gelangen. Im Hintergrund solcher Aktivitäten werden häufig Geheimdienste aus dem Fernen Osten angenommen. Besonders von sich reden machte in diesem Zusammenhang „Titan Rain“, eine dem chinesischen Geheimdienst zugeordnete Abteilung mit dem Spezialgebiet Internet-Spionage. Es gibt jedoch keinen Grund anzunehmen, dass sich die Nachrichtendienste anderer Nationen in vornehmer Zurückhaltung übten. Die NSA beispielsweise beschäftigt mehr IT-Sicherheitsexperten als jedes Unternehmen und ist bekannt dafür, dass sie amerikanische Firmen schon mal mit hilfreichen Informationen über die Aktivitäten ausländischer Konkurrenz versorgt.

Aber auch infizierte Rechner von Privatpersonen sind lohnende Ziele für Datenspione. So genannte Keylogger laufen unbemerkt im Hintergrund, erkennen Fenster mit Passwortabfragen und protokollieren dann die Eingaben des Benutzers. Die Daten übermitteln sie in regelmäßigen Abständen an einen externen Server, wo die Gauner sie abholen. Auf einem infizierten Rechner fallen den Spionen in der Regel fünf bis zwanzig Identitäten in die Hände, angefangen beim E-Mail-Zugang, über Amazon-, eBay- und PayPal-Accounts bis hin zum Homebanking. Etliche solcher Identitäten lassen sich gewinnbringend nutzen, besonders wenn man Bestätigungs-Mails aus dem Postfach fischen kann, ehe der Nutzer sie bemerkt.

Große Bot-Netze eröffnen das Geschäftsfeld der Sabotage und Erpressung: Wenn zigtausend PCs gleichzeitig Müll an einen Server schicken, geht dem garantiert die Luft aus. Und selbst sechs Jahre nach den ersten verteilten Denial-of-Service-Attacken, die Server vom Kaliber Yahoo, Amazon und eBay aus dem Netz katapultierten, ist gegen die rohe Gewalt tausender Zombies noch kein Kraut gewachsen. Das ermöglicht Schutzgelderpressungen im Stil: „Entweder du zahlst x-tausend Euro, oder wir schießen deinen Server aus dem Netz.“ Und wer dann nicht zahlt, wird tatsächlich Schwierigkeiten haben, sein Web-Angebot aufrechtzuerhalten. Eine solche Organisation hat das FBI schon 2004 im Zuge der Operation Cyberslam ausgehoben. Oder der Betreiber eines Bot-Netzes lässt sich von jemandem dafür bezahlen, dass er dessen Mitbewerber schädigt. Das geht allerdings unauffälliger, wenn die Bots gezielt Werbebanner abrufen, für die der Geschädigte einen Pay-per-Click-Vertrag abgeschlossen hat.

Die Ermittlungsbehörden gehen verstärkt gegen diese Form der Computerkriminalität vor. Die Chancen bei Ermittlungen aufgrund von Anzeigen seien sehr hoch, sagte ein Sprecher des LKA Baden-Württemberg gegenüber c't. Immer mehr Landeskriminalämter bauen Abteilungen auf, die auch anlassunabhängig ermitteln und beispielsweise auf offensichtliche Angebote in Foren reagieren können.

Gegenwehr

Die internationale Zusammenarbeit zwischen Behörden hat sich verbessert, was ungemein hilft, da die Verbrecherorganisationen oft aus dem Ausland operieren oder sich über mehrere Länder verteilen. Außerdem unterstützt Microsoft weltweit Beamte mit Know-how; im September 2006 über-

reichte das FBI neun Mitarbeitern des Software-Herstellers eine Auszeichnung für ihre Mithilfe bei der Ermittlung der drei Verantwortlichen für die Mytob/Zotob-Würmer.

Doch die Dunkelziffer ist sicherlich hoch. Selbst wer Anti-Viren- und Anti-Rootkit-Tools nutzt (siehe c't 2/07, S. 90), kann nicht völlig sicher sein, dass sein Computer mit DSL-Anschluss nicht ausspioniert wird oder gar Teil eines Bot-Netzes ist. Regelmäßige Updates und Tests mit verschiedenen Tools können das Risiko zumindest reduzieren. Am wichtigsten ist jedoch das eigene Verhalten: Gesundes Misstrauen gegenüber Dateien, die per E-Mail ankommen, ist ein guter Schutz.