

COMPUTER

Nahkampf im Netz

Kriminelle wenden im Internet immer ruchlosere Tricks an, um an Geld und Daten zu kommen. Spam-Jäger wie der US-Computerexperte Patrick Peterson bieten der Online-Mafia Paroli.

Patrick Peterson hat mächtige Gegner. Sie heißen „Kraken“, „Storm“ oder „Srizbi“. Sie sitzen im Internet wie teuflische Spinnen, hinter sich eine virtuelle Armee willenloser Helferlein, bereit, jederzeit zuzuschlagen.

Kommt das Signal zur Attacke, fluten diese sogenannten Botnets das Internet im Millisekundentakt mit E-Mail-Müll. Die Infoschnipsel sausen durch die Breitbandleitungen der Welt und vereinen sich zu einer gewaltigen Flut. Dann branden sie an die Spundwände der Netzgesellschaft, 160 Milliarden an jedem Tag. Und Peterson soll dafür sorgen, dass der Damm nicht bricht.

Peterson ist Spam-Jäger, ein Kämpfer gegen die Geißel des Computerzeitalters. Zusammen mit einem eingeschworenen Club von Spezialisten bewirkt der 40-jährige Sicherheitsexperte von Cisco Ironport in San Bruno, Kalifornien, dass die rund 1,7 Milliarden Internetnutzer nicht im Datenmüll ersticken und dass Terabytes privater Daten privat bleiben.

Seine Gegenspieler sitzen in Russland, in China, in Indien, in Australien oder vielleicht gleich nebenan in einem unscheinbaren Bürohaus in San Francisco. Sie sind gut ausgebildet, findig und intelligent, und sie kennen keine Skrupel. Glaubt man Peterson, sind sie zu einer professionell organisierten Online-Mafia herangereift, die sich mit jedem Großkonzern messen kann.

„Diese Kriminellen sind viel reicher und viel gefährlicher, als wir es uns noch vor kurzem vorstellen konnten“, sagt der IT-Experte. „Es scheint, als habe der Lehrstoff der Harvard Business School seinen Weg in den Online-Untergrund gefunden.“

Dann springt Peterson auf und eilt an eine Tafel, um mit rotem Filzstift wieder eines der „Geschäftsmodelle“ der „bad guys“ zu skizzieren. Und jede seiner Geschichten klingt wie eine Räuberpistole.

Ein Krieg tobt im Netz, und er nimmt an Härte zu. Spam-Mails machen fast 90 Prozent des gesamten E-Mail-Verkehrs aus. Sie sind nicht nur ein Ärgernis. Sie verstopfen das Internet und kosten deshalb Milliarden. Die allermeisten dieser Nachrichten werden von Computern verschickt, deren Besitzer keine Ahnung vom zombiehaften Wirken ihrer Maschinen haben. Online-Gangster kapern die Rechner und programmieren sie um in willfährige Diener.

Über elf Millionen Computer weltweit sollen betroffen sein. Sie dienen als

Drückerkolonne einer Schattenindustrie, die alles verkauft – von gefälschten Rolex-Uhren und Viagra-Pillen über windige Kredite bis hin zu getrocknetem Tigerpenis.

Und noch weit schlimmer: Mit ruchlosen Tricks versuchen die Kriminellen, arglosen Internetsurfern das Geld aus der Tasche zu ziehen.

In den USA beispielsweise ist jeder fünfte Internetnutzer im Laufe der vergangenen beiden Jahre Opfer von Online-Betrug geworden, schätzt die US-Verbraucherorganisation Consumers Union. Der Schaden: acht Milliarden US-Dollar.

Doch weil die Sicherheitsexperten nicht schlafen, ist ein Wettrüsten im Netz in Gang gekommen, bei dem Spezialisten ihre Computerprogramme aufeinander loslassen wie wild gewordene Pitbulls. BadCow, Dark-Mailer oder AlekseyB nennen sich die „bad guys“. Auf der Seite der Guten stehen Menschen wie Patrick Peterson.

„Man muss den Feind kennen, nur so kann man sich vor ihm schützen.“ Im Konferenzraum in San Bruno kommt Peterson in Fahrt. Gerade erläutert er die „Kundenakquise“ der Gangster. Medienereignisse zum Beispiel würden von ihnen inzwischen systematisch verwertet.

In den ersten Tagen nach dem Tod Michael Jacksons etwa verschickten Spammer bis zu 4,3 Milliarden E-Mails täglich, die den Empfängern unter anderem ein Video von Jacksons Leiche in Aussicht stellten. Wer dem in der Mail empfohlenen Link folgte, löste indes unbemerkt den Download von Schadsoftware aus. „Ist ein Rechner mit so einer Software infiziert, können die Kriminellen unbemerkt zugreifen“, sagt Peterson.

Offen wie ein Scheunentor ist dann das Allerheiligste des Heim-PC. Die Verbrecher legen gleichsam eine Standleitung nach außen. Tastaturbefehle lassen sich unbemerkt abgreifen. Kreditkartennummern, Kontodaten oder Passwörter sind nicht mehr sicher.

Selbst Einmal-Codes wie Tan-Nummern für Überweisungen fingen die Gangster ab, berichtet Peterson: „Die Verbrecher verhindern deren Übermittlung an die Bank und benutzen sie kurz darauf selbst.“

Oder die sogenannte Scareware, von Peterson zum „Cybercrime-Produkt des Jahres“ gekürt: Ein solches Programm gaukelt dem Nutzer vor, der eigene PC sei



Server-Farm in den USA: Der Gegner sitzt in Russland, Indien oder im Büro nebenan

bald reif für den Elektroschrott. Kurz darauf preisen eingehende Spam-Mails eine vielversprechende Anti-Virus-Software an.

Das Programm ist optisch professionell gestaltet, tut indes nichts anderes, als das von den Gangstern selbst initiierte Problem zu lösen. Von der Pein befreit, schöpft der Käufer noch nicht einmal Verdacht. Ihm ist ja geholfen worden.

Peterson weiß von Banden, die auf diese Weise 50 Millionen Dollar jährlich umsetzen. Wie deckt der Spam-Detektiv derlei Treiben auf? Er schickt die Software der Ganoven in den „digitalen Zoo“.

Rund um die Welt hat der IT-Experte zusammen mit Kollegen ein Netzwerk aus präparierten Computern eingerichtet. Auf diesen Testgeräten läuft keinerlei Anti-Viren-Software. Schadprogramme haben deshalb leichtes Spiel. Sind sie erst installiert, beginnt der große Lauschangriff. „Wir lassen die Programme atmen, essen und pupsen, und wir lassen sie mit ihrem kriminellen Mastermind reden“, erläutert Peterson. „Andererseits halten wir sie in ihrem Käfig immer so weit unter Kontrolle, dass kein Schaden entsteht.“

Was der Forscher dann beobachtet, lässt ihn oftmals staunen. Der Computervorm Conficker etwa hält die Szene schon fast ein Jahr lang in Atem. „Die Jungs, die Conficker programmiert haben, sind verdammt gut“, sagt Peterson, „sie verwenden zum Beispiel Verschlüsselungsverfahren,



CLAY McCLACHLAN / AURORA SELECT

IT-Experte Peterson: Digitaler Zoo für die Schadsoftware

ren, die so neu sind, dass sie selbst von uns noch kaum benutzt werden.“ Nach „monatelangem Nahkampf“ sei das Programm, das rund zehn Millionen Windows-Computer weltweit befallen hat, immer noch nicht besiegt. „Conficker verändert sich ständig; inzwischen haben die Urheber 80 Prozent des Programmcodes erneuert“ – ein Alptraum für jede Sicherheitsfirma.

Glück im Unglück: Conficker hat bisher kaum Schaden angerichtet. „Wir warten, ob dem Biest vielleicht ein dritter Arm wächst oder so etwas“, sagt Peterson, „aber bisher ist einfach nichts passiert.“

Peterson faszinieren solche Programme. Von seinem Schreibtisch im dritten Stock der Ironport-Zentrale aus folgt er der digitalen Spur der Schadsoftware, reist dabei mit den Datenströmen um die ganze Welt und versucht, die verschlüsselten Quellen des Übels zu enttarnen. „Für mich ist das wie ein Spionagethriller“, sagt der Forscher. „Ich versuche, das Geflecht des Betrugs zu entwirren; und dann kommt jener Moment, an dem das Ganze plötzlich einen logischen Sinn ergibt.“

Für diese Momente arbeitet Peterson. Sie geben ihm Kraft. Und besonders froh ist er, wenn am Ende der Recherche nicht nur ein Server steht, sondern sogar ein Mensch. So einer wie der 64-jährige Alan Ralsky etwa, den ein US-Gericht erst im Juni des Online-Betrugs für

schuldig befand: Der auch „Spam-König“ genannte US-Amerikaner verklebte das Netz über Jahre mit Milliarden von Müll-Mails. Zwischenzeitlich gelang es ihm gar, den chinesischen Aktienmarkt durch eine Flut von E-Mails zu seinen Gunsten zu beeinflussen.

Oder die Gebrüder Shah aus Missouri: Sie sammeln über acht Millionen E-Mail-Adressen von US-Studenten und bombardierten diese mit Werbung etwa für iPods oder Zahnweiß. Der Schaden: über vier Millionen Dollar.

Am Ende griff das FBI zu. Zur Überraschung der

Fahnder fanden sich auf den Rechnern der Ganoven unverschlüsselte Chat-Protokolle, über die sich Peterson bis heute amüsiert: „Wow, das funktioniert super“, hieß es da, oder: „Wir können nicht eine Million Dollar in unsere Steuererklärung schreiben“ – „Nein, lass uns Immobilien kaufen“ – „Okay, wo denn?“ Häuser in Columbia und St. Louis, ein Luxusapartment und mehrere Autos stellten die FBI-Beamten schließlich sicher.

Wird es gelingen, auch den großen, gut organisierten Online-Gangs das Handwerk zu legen? Peterson ist skeptisch. Vor allem Online-Betrug werde künftig vermutlich noch zunehmen. Jüngst erst erfuhr er von einem besonders dreisten Fall im US-Bundesstaat Kentucky, bei dem Diebe im Computersystem einer Bezirksregierung virtuelle Angestellte erzeugten und diesen fortan Geld überwiesen. Als der Schwindel aufflog, waren die Dollar längst in der Ukraine.

Oder soziale Netzwerke wie Facebook: Hier haben es Betrüger sehr leicht, weil sie das Vertrauensverhältnis der Nutzer missbrauchen können. „Wer wird schon misstrauisch, wenn ein Freund um Geld bittet?“ Die Intimität sei jedoch trügerisch. „Wer mein Passwort hat, ist noch lange nicht ich“, warnt Peterson.

„Die ‚bad guys‘ werden uns vermutlich immer einen Schritt voraus sein“, bilanziert der IT-Experte und fordert „gesunden Offline-Menschenverstand“ von den Internetnutzern: „Irgendjemandem auf der Straße würden Sie ja auch nicht einfach Ihre Kreditkarte rüberreichen.“

Wie mühsam der Kampf gegen die Betrüger ist, musste er sich selbst indes erst kürzlich wieder eingestehen, als die Kreditkarte seiner Frau ohne ihr Zutun mit 800 Dollar belastet wurde.

Wie die Gauner an die Daten kamen? „Ich könnte den Rest meines Lebens versuchen, das herauszufinden“, sagt der Sicherheitsexperte, „es würde mir nicht gelingen.“

PHILIP BETHGE

Hochprozentiges Spam...

Spam-Mails in Prozent aller E-Mails



... und mögliche Folgen

Die Funktionsweise von „Scareware“

1 Online-Kriminelle locken mit **Spam-Mails** Internetnutzer auf eine präparierte Web-Seite, z. B. mit einem Video.



2 Statt des Videos laden sie ohne ihr Wissen ein **Schadprogramm** auf ihren Rechner. Dieses verursacht **Betriebsstörungen**, z. B. wird der Rechner langsamer oder gibt merkwürdige Fehlermeldungen aus.



3 Die Gangster verkaufen den Betroffenen ein **gefälschtes Anti-Viren-Programm**. Dieses schafft tatsächlich Abhilfe. Der Nutzer schöpft deshalb noch nicht einmal den Verdacht, betrogen worden zu sein.

