# Schattenwirtschaft Botnetz — ein Milliongeschäft für Cybercriminelle

Yuri Namestnikov

Innerhalb der letzten zehn Jahre haben sich Botnetze stark gewandelt: von kleinen Netzwerken mit einigen Dutzenden Computern, die zentral gesteuert wurden, zu komplizierten, weit verzweigten Systemen, bestehend aus Millionen von Rechnern mit dezentralisierter Steuerung. Doch was ist der Grund für die Schaffung derart riesiger Zombie-Netze? Diese Frage lässt sich mit einem Wort beantworten: Geldgier.

Ein Botnetz, auch Zombie-Netz genannt, ist ein Zusammenschluss von Computern, die mit einem Schadprogramm infiziert sind. Es ermöglicht Cyberkriminellen die Fernsteuerung der befallenen Rechner, ohne dass Anwender etwas davon bemerken. Zombie-Netze können inzwischen auch ohne größeres Fachwissen aufgebaut und gesteuert werden. Sie sind daher lukrativ einsetzbar. Die Folge: die Anzahl von Botnetzen wächst.

Doch wie funktioniert so ein Botnetz? Was muss ein Cyberkrimineller tun, wenn er ein Zombie-Netz aufbauen will? Und wie können sich die User dagegen wehren?

Damit ein solches Netzwerk entsteht, müssen Anwendercomputer mit einem speziellen Programm – einem Bot – infiziert werden. Bots sind Schadprogramme, die die infizierten Computer zu einem Netzwerk zusammenschließen. Dabei muss man nicht einmal programmieren können. Möchte man ins Cybercrime-Geschäft einsteigen, wird man in einschlägigen Foren fündig, in denen Bots zum Verkauf angeboten werden. Dort können auch Extras wie Obfuskation (unter Obfuskation versteht man die Verschleierung von Programmcodes, die dazu dient, die Entdeckung durch Antiviren-Programme zu erschweren) und Verschlüsselungscodes für Bots geordert werden, damit sie nicht durch Antivirus-Programme entdeckt werden. Bereits existierende Botnetze können aber auch einfach gestohlen werden.

Um so viele Anwendercomputer wie möglich mit einem schädlichen Bot-Programm zu infizieren, werden massenhaft Spam-Mails verschickt, Mitteilungen in Foren oder in sozialen Netzwerken gepostet oder Drive-by-Downloads eingesetzt. Außerdem verfügt jedes Bot-Schadprogramm – wie alle Viren und Würmer – über eine Selbstreproduktionsfunktion.

Beim Versenden von Spam oder beim Posten in Foren und sozialen Netzwerken setzen Cyberkriminelle verschiedene Social-Engineering-Tricks ein, um das potentielle Opfer dazu zu bringen, das Bot-Programm zu installieren. Als Köder dienen zum Beispiel interessante Videos: Will ein Anwender das gepostete Video anschauen, muss er ein spezielles Programm auf seinem Rechner installieren. Nach Download und Start der entsprechenden Datei ist der Computer infiziert. Auch wenn der Anwender das Video immer noch nicht abspielen kann, wird er nach der Infektion keine weiteren Veränderungen auf seinem Computer bemerken. Auf diese Weise wird der Computer unbemerkt zum treuen Diener des Botnetz-Betreibers.

Eine weitere, häufig verwendete Methode ist ein so genannter Drive-by-Download. Dabei installiert sich beim Besuch einer infizierten Website über Sicherheitslücken – meist in den gängigen Internet-Browsern – ein Schadprogramm auf dem PC des Anwenders – natürlich ohne dass er es bemerkt.

Um Schwachstellen in Browsern auszunutzen, werden spezielle Programme verwendet: So genannte Exploits, mit denen nicht nur unbemerkt Schadprogramme auf einen Computer eingeschleust, sondern der PC auch heimlich gestartet werden kann. Der Anwender schöpft keinen Verdacht, dass sein Computer infiziert ist. Das gefährliche dabei: Wird eine populäre Anwendung gehackt, sind hunderttausende von Anwendern gefährdet.

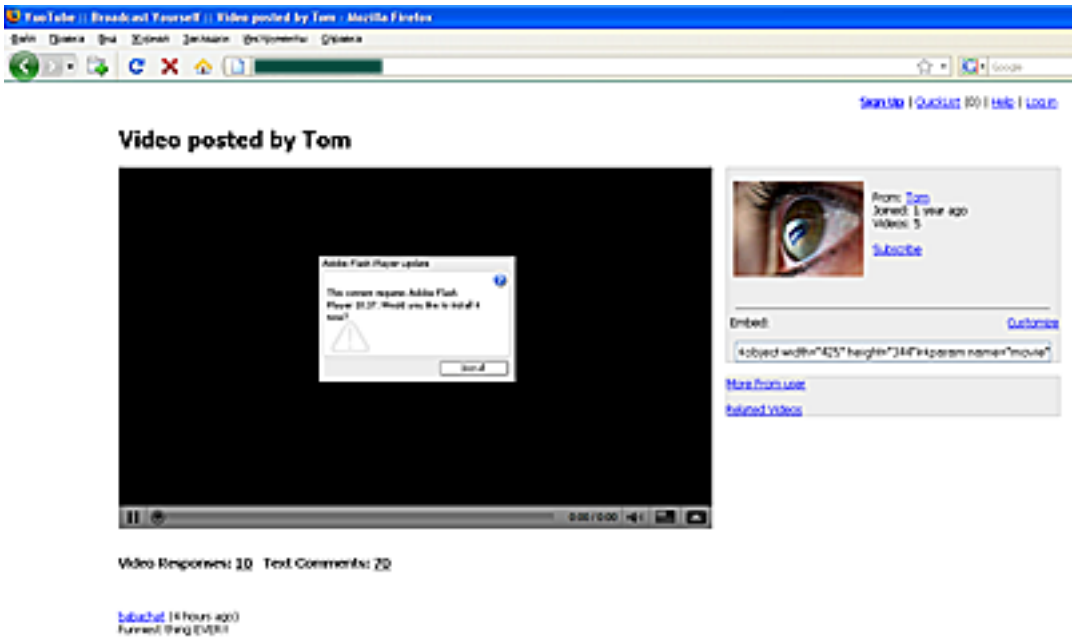


Abb.1 User-Köder: Eine gefälschte Youtube-Seite

Ein weiterer Verbreitungsweg ist die Selbstverbreitungsfunktion eines Bot-Programms. So kann sich ein Bot beispielsweise durch die Infizierung aller auf dem Rechner verfügbaren ausführbaren Dateien verbreiten. Oder er spürt alle verwundbaren Computer des Netzes auf und infiziert diese. Jüngste Beispiele für derartige Bots sind die Vertreter der Familien Virut und Kido. Virut ist ein polymorpher Datei-Virus, bei Kido handelt es sich um einen Netzwurm. Das von Kido alias Conficker aufgebaute Zombie-Netzwerk ist derzeit weltweit das größte seiner Art.

Das raffinierte an Zombie-Netzen ist, dass der Botnetz-Betreiber unbemerkt vom Anwender die infizierten Computer mit Hilfe eines Kontrollzentrums, dem so genannten Command-and-Control-Server (C&C), steuern kann. Dieses Kontrollzentrum ist beispielsweise über einen IRC-Kanal oder eine Internet-Verbindung mit den Bots verbunden. Schon mit ein paar Dutzend Zombie-Rechnern kann der Betreiber Geld verdienen. Der Gewinn ist abhängig von der Stabilität und dem Wachstumstempo des Botnetzes.

# Wie sich mit Botnetzen Geld verdienen lässt

Um mit infizierten Computern Geld zu verdienen, gibt es mehrere Möglichkeiten: DDoS-Attacken, Diebstahl vertraulicher Informationen, Spamversand, Phishing, Suchspam, betrügerische Generierung von Klicks sowie der Download von Adware und Schadprogrammen. Egal, für welche Einkommensart sich der Cyberkriminelle entscheidet, gewinnbringend sind sie alle. Eine Beschränkung ist nicht nötig, denn mit einem Botnetz können alle oben genannten Attacken durchgeführt werden – und zwar gleichzeitig!

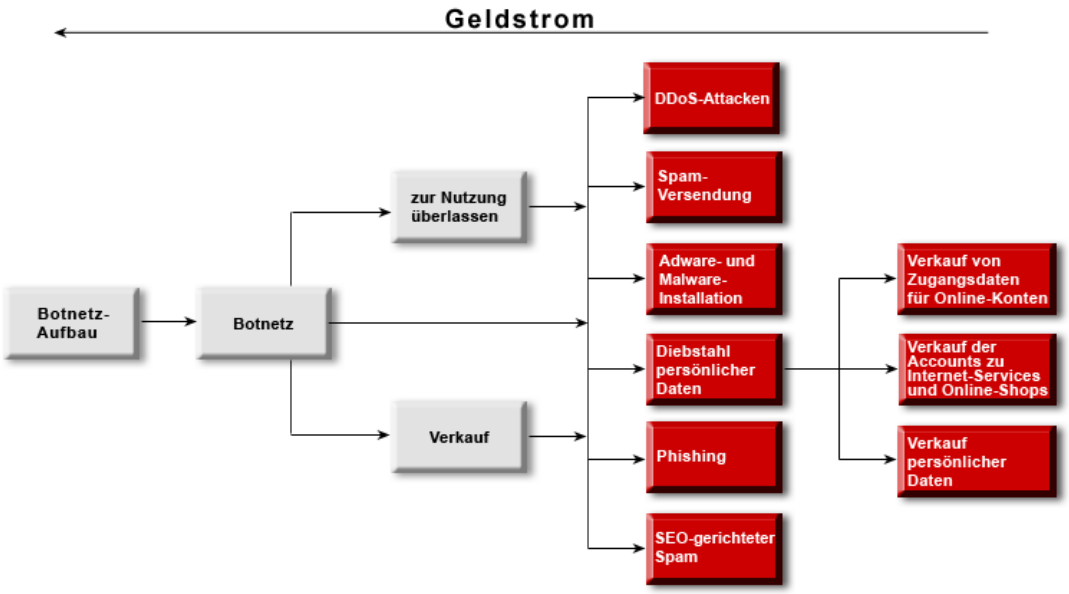


Abb. 2 Geschäfte mit Botnetzen

## DDoS-Attacken

Distributed Denial-of-Service-Attacken (DDoS-Attacken) sind Angriffe auf ein Computersystem mit dem Ziel, dieses derart zu überlasten, dass es nicht mehr in der Lage ist, Anfragen legitimer User zu bearbeiten – das System verweigert sozusagen den Dienst (Denial of Service). Um einen DDoS-Angriff durchzuführen, werden meist zahlreiche Anfragen an den Opfercomputer geschickt. Der Service wird verweigert, weil die Ressourcen des angegriffenen Computers für die Bearbeitung aller eingehenden Anfragen nicht ausreichen. Für Cyberkriminelle sind DDoS-Attacken eine effektive Waffe und ein Botnetz ist das ideale Werkzeug zur Durchführung derartiger Angriffe. DDoS-Attacken werden hauptsächlich im unlauteren Wettbewerb gegen unliebsame Konkurrenten, aber auch von Cyberterroristen eingesetzt.

Ein Botnetz-Betreiber könnte beispielsweise einem Unternehmen eine DDoS-Attacke auf die Webseite seines Konkurrenten anbieten. Die Webseite wird wegen Überbelastung lahmgelegt und der Cyberkriminelle erhält dafür eine Entlohnung. Doch auch die Botnetzbetreiber selbst nutzen DDoS-Attacken, um Lösegeld von den angegriffenen Firmen zu erpressen.

Da die Folgekosten einer gelungenen DDoS-Attacke meist teurer sind, als das geforderte Lösegeld, lassen sich viele Unternehmen von Cyberkriminellen erpressen. So führte im Januar 2009 ein Angriff auf godaddy.com dazu, dass mehrere tausend Seiten, die auf den Servern des Unternehmens gehostet wurden, fast 24 Stunden lang nicht erreichbar waren. Handelte es sich hierbei um eine illegale Maßnahme eines direkten Konkurrenten oder wurde godaddy.com von Online-Kriminellen erpresst? Beide Varianten sind gleichermaßen wahrscheinlich. Endgültig aufgeklärt wurde der Fall nie. Derselbe Provider wurde übrigens im November 2005 schon einmal Opfer einer DDoS-Attacke, doch in diesem Fall war der Dienst nur eine Stunde lang nicht erreichbar. Der zweite Angriff war da schon wesentlich gefährlicher, was in erster Linie mit dem Zuwachs von Botnetzen zu erklären ist.

Im Februar 2007 wurde eine Reihe von Angriffen auf Root-DNS-Server verübt. Von diesen „Domain Name Servern“ hängt das reibungslose Funktionieren des gesamten Internets ab. Es ist unwahrscheinlich, dass das Ziel dieser Attacken die Zerschlagung des Internets war, denn Zombie-Netze sind nur innerhalb des World Wide Web existenzfähig. Vielmehr ist der Angriff als Machtdemonstration der Botnetz-Betreiber zu verstehen.

In vielen Foren wird offen für die Umsetzung von DDoS-Attacken geworben. Ein Blick auf die einschlägige Liste verrät, dass die Preise für 24-Stunden-Angriffe zwischen 50 und einigen Tausend Dollar schwanken. Diese Preisspanne ist durchaus verständlich: Ein relativ kleines Botnetz (mit etwa 1.000 Computern) schafft es bereits, einen vergleichsweise kleinen, ungesicherten Online-Shop eines unliebsamen Konkurrenten für einen Tag außer Betrieb zu setzen. Der Preis ist dementsprechend gering. Eine ganz andere Summe wird allerdings gefordert, wenn es sich bei dem Ziel um einen internationalen Großkonzern mit gesicherter Webseite handelt. In diesem Fall werden weitaus mehr Zombie-Rechner benötigt, um eine erfolgreiche DDoS-Attacke zu verüben. Die Folge: Der Auftraggeber muss tiefer in die Tasche greifen.

Nach Angaben von shadowserver.org gab es im Jahr 2008 zirka 190.000 DDoS-Attacken, mit denen Cyberkriminelle rund 20 Millionen Dollar verdient haben. Zum Gesamtschaden erpresster Lösegelder gibt es keine Zahlen, weil diese nicht erfasst werden können.

## Diebstahl vertraulicher Informationen

Vertrauliche Informationen, die auf Anwendercomputern gespeichert sind, verüben auf Kriminelle eine geradezu unwiderstehliche Anziehungskraft. Dabei stehen Kreditkartennummern, Bankinformationen und Passwörter zu verschiedenen Diensten (etwa E-Mail, FTP, Instant-Messenger) hoch im Kurs. Moderne Schadprogramme ermöglichen es den Kriminellen, genau die Daten auszuwählen, die sie benötigen. Zu diesem Zweck müssen sie lediglich das entsprechende Modul auf den Computer laden, der ausgespäht werden soll.

Die gestohlenen Informationen werden dann weiter verkauft oder von den Online-Betrügern selbst missbraucht.

In den entsprechenden Untergrund-Foren werden beispielsweise täglich in hunderten Anzeigen Bankverbindungsdaten zum Verkauf angeboten. Der Preis für die Bankdaten hängt von der Liquidität des Anwenders ab und schwankt zwischen 1 und 1.500 Dollar pro Konto. Die untere Grenze zeigt, dass die Gesetze der Marktwirtschaft auch für Cyberkriminelle gelten. Um wirklich viel Geld verdienen zu können, müssen immer neue Daten strömen, die zum größten Teil aus einem stabil wachsenden Zombie-Netzwerk stammen.

Gerade für Kriminelle, die Bankkarten fälschen, sind solche Finanz-Informationen sehr interessant. Dies zeigt das Beispiel einer brasilianischen Cybergang, deren Mitglieder vor zwei Jahren verhaftet wurden. Mit Hilfe gestohlener Informationen war es ihnen gelungen, 4,74 Millionen Dollar von fremden Bankkonten abzuheben.

Einige Cyberkriminelle sind auch „nur“ an persönlichen Daten interessiert, die in keiner direkten Verbindung zum Geld des Anwenders stehen. Interessant sind hier vor allem der vollständige Vor- und Familienname, das Geburtsdatum, die Adresse sowie die Sozialversicherungs-Nummer. Diese Daten reihen meist, um Dokumente zu fälschen, Kredite zu bekommen und Bankkonten zu eröffnen.

Der Wert gestohlener, persönlicher Daten steht in direktem Zusammenhang mit dem jeweiligen Land, in dem ihr rechtmäßiger Besitzer lebt. So kosten die vollständigen, persönlichen Angaben eines Bürgers der Vereinigten Staaten von Amerika beispielsweise fünf bis acht Dollar. Auf dem Schwarzmarkt stehen die Daten von EU-Bürgern besonders hoch im Kurs – sie kosten das Zwei- bis Dreifache. Der Grund: Online-Betrüger können diese Daten in allen EU-Ländern verwenden. Der weltweite Durchschnittspreis für ein vollständiges Datenpaket einer Person beträgt etwa sieben Dollar.

Auch E-Mail-Adressen werden häufig mit Hilfe von Botnetzen zusammengetragen. Im Gegensatz zu Kreditkartennummern und Kontodaten lassen sich diese meistens von nur einem einzigen infizierten Computer stehlen. Die Adressen werden anschließend zum Verkauf angeboten, wobei sich der Preis oft nach dem „Gewicht“ richtet – kein Kilo-, sondern ein Megabyte-Preis. Die besten Kunden sind in diesem Fall natürlich Spammer. Eine Liste mit einer Millionen E-Mail-Adressen kostet zwischen 20 und 100 Dollar, der von Spammern in Auftrag gegebene Spam-Versand an eben diese Adressen zwischen 150 und 200 Dollar.

Für Online-Verbrecher sind auch Accounts für verschiedene Bezahldienste und Online-Shops interessant. Daten dieser Kategorie sind zweifellos billiger als Bankverbindungsdaten, allerdings ist auch das Risiko, wegen des Diebstahls dieser Daten strafrechtlich verfolgt zu werden, wesentlich geringer. Accounts für den beliebten Online-Game-Shop Steam werden für etwa 7 bis 15 Dollar pro Account verkauft.

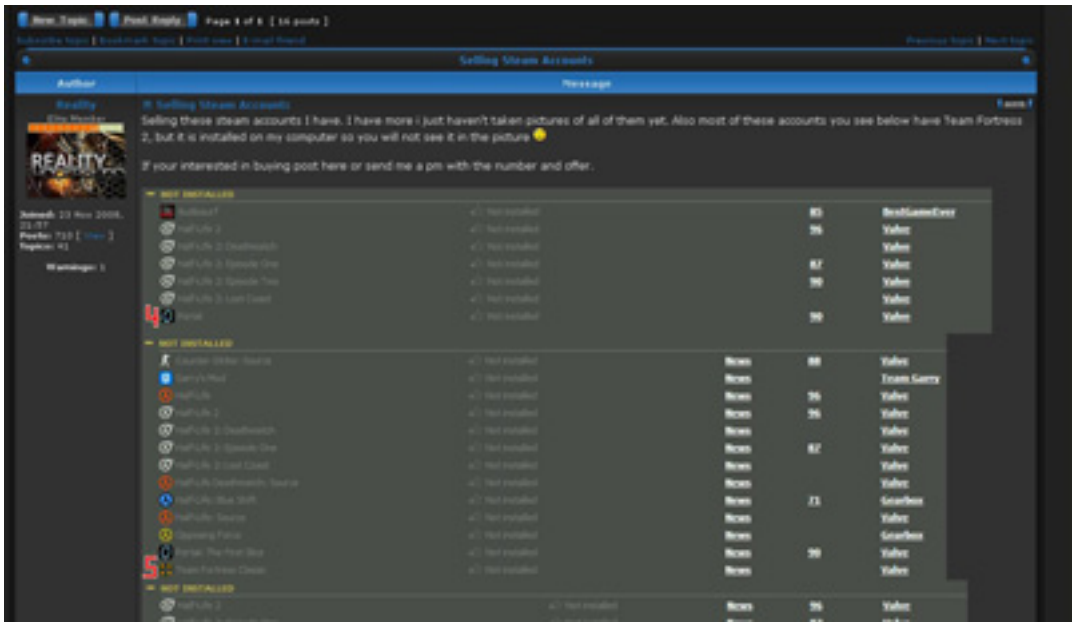

Abb. 3 Verkaufsangebote für Steam-Accounts in einem Forum

## Phishing

Cyberkriminelle produzieren Phishing-Webseiten wie am Fließband. Phishing-Webseiten sind gefälschte Webseiten bekannter Internetfirmen und Banken. Unvorsichtigen Anwendern sollen hier persönliche Angaben gestohlen werden. Diese Seiten wollen Cyberkriminelle begreiflicherweise davor schützen, offline genommen zu werden. An genau dieser Stelle kommt das Zombie-Netz zu Hilfe: Über Zombie-Netze wird die Fast-Flux-Technologie zum Einsatz gebracht, die es ermöglicht, die IP-Adresse bei gleich bleibender Domain-Adresse im Minuten-Takt zu ändern. Die Lebensdauer einer Phishing-Site wird so verlängert, weil dadurch ihre Entdeckung und Abschaltung erschwert wird. Dazu werden zum Zombie-Netz gehörende Heimcomputern als Web-Server mit Phishing-Content verwendet. Fast-Flux ermöglicht ein erfolgreicheres Verbergen gefälschter Webseiten im Netz als über die klassische Methode des Proxy-Servers. Die bekannte Phishing-Gruppe Rock Phish arbeitet mit den Betreibern des Botnetzes Asprox zusammen. Rock Phisher ist für die Hälfte aller Phishing-Attacken im Internet verantwortlich. Mitte des vergangenen Jahres modernisierte die Cybergang im Laufe von fünf Monaten unter Verwendung von Fast-Flux ihre Infrastruktur. Der Umbau lief äußerst professionell ab, die Phisher bauten kein eigenes Fast-Flux-Netz auf, sondern kauften eine bereits bestehende Lösung von den Asprox-Betreibern. Für das Fast-Flux-Hosting zahlen Kriminelle – meistens Spammer – zwischen 1.000 und 2.000 Dollar im Monat. Der durchschnittliche mit Phishing erzielte Gewinn ist mit den Einnahmen aus dem Diebstahl vertraulicher Daten vergleichbar und beträgt mehrere Millionen Dollar jährlich.

## Spam

Täglich werden weltweit Spam-Mails verschickt. Der Versand von unerwünschten Mitteilungen ist derzeit eine der wichtigsten Funktionen moderner Botnetze. Nach Erkenntnissen von Kaspersky Lab werden gut 80 Prozent aller Spam-Nachrichten über Zombie-Netzwerke verschickt. Von den Computern ahnungsloser und gesetzestreuer Anwender werden Milliarden Werbemails für Viagra, Online-Casinos oder gefälschte Luxusartikel verschickt, die die Datenübertragungskanäle und elektronischen Briefkästen verstopfen. Hacker bringen so die Rechner von Anwendern in Gefahr, die sich nichts zu Schulden haben kommen lassen: Denn die Adressen, über die Spam versendet wird, werden von Antivirus-Unternehmen auf so genannte Schwarze Listen gesetzt.

In den vergangenen Jahren hat sich das Betätigungsfeld der Spammer erweitert, denn zum althergebrachten E-Mail-Spam gesellten sich ICQ-Spam und Spam in sozialen Netzwerken, Foren und Blogs. Auch dies ist ein Verdienst der Botnetz-Betreiber, denn einem Bot ein weiteres Modul hinzuzufügen ist technisch nicht sehr anspruchsvoll. Die Folge: Das Portfolio der Botnetz-Betreiber wurde um ein neues Geschäftsfeld reicher – beworben mit Slogans wie „Spam bei Facebook – extra günstig“.

Der Preis für Spam variiert nach Zielgruppe und Anzahl der Adressen, an die die Mitteilungen geschickt werden. Er schwankt zwischen 70 Dollar für Hunderttausende Adressen und 1.000 Dollar für mehrere Dutzend Millionen Adressen. Im vergangenen Jahr verdienten Spammer mit der Versendung von unerwünschten Mitteilungen rund 780 Millionen Dollar. Eine beeindruckende Summe für unerwünschte Werbung!

## Suchspam

Eine weitere Möglichkeit, Botnetze zu nutzen ist Suchoptimierung. Bei der Suchoptimierung geht es darum, die eigene Webseite bei den Ergebnissen der Suchdienste so hoch wie möglich zu positionieren. Denn je höher die Seite gelistet ist, desto mehr Anwender besuchen sie über den bei den Suchdiensten angegebenen Link.

Suchdienste berücksichtigen verschiedene Faktoren bei der Bewertung der Relevanz einer Webseite. Einer der wichtigsten Parameter ist die Anzahl der Links auf andere Seiten und Domains. Je mehr solcher Links vorhanden sind, desto höher erscheint die Seite im Ranking. Auch die Wörter, aus denen ein Link besteht, haben direkten Einfluss auf das Ranking. So hat der Link „kaufen Sie unsere Computer“ mehr Gewicht als ein Link, in dem lediglich die Wörter „Computer“ und „kaufen“ vorkommen.

Die Geschäfte mit SEO (Search Engine Optimization) sind an sich sehr beliebt. Viele Unternehmen zahlen ihren Webmastern viel Geld, damit sie ihre Internetseiten auf die obersten Ränge bringen. Die Betreiber von Botnetzen untersuchten verschiedene Verfahren und automatisierten dann den Prozess der Suchoptimierung.

Wenn Sie also in den Kommentaren zu einem Blogeintrag oder einem gelungenen Foto mehrere Links entdecken, die von einer unbekannten Person – oder manchmal auch einem Freund – stammen, wundern Sie sich nicht: Jemand hat bei Botnetz-Betreibern das Hochjubeln seiner Ressource in Auftrag gegeben. Ein eigens entwickeltes Programm wird auf den Zombie-Computer geladen und hinterlässt im Namen seines Besitzers Kommentare auf populären Ressourcen mit Links auf die zu optimierende Webseite. Der durchschnittliche Preis für den illegalen Suchspam-Service beträgt 300 Dollar monatlich.

## Installation von Adware und Schadprogrammen

Stellen Sie sich vor, Sie lesen online Ihr Lieblings-Automagazin und plötzlich öffnet sich ein Popup-Fenster, in dem Ihnen Autozubehör zum Kauf angeboten wird. Dies muss unter Umständen nichts Schlimmes bedeuten und vielleicht sind sie an dem einen oder anderen Teil sogar interessiert, allerdings haben sie kein für die Suche notwendiges Programm installiert. Die Antwort liegt nahe – Botnetz-Betreiber haben das benötigte Programm bereits bei Ihnen eingerichtet. Die meisten Firmen, die ihre Dienste per Online-Werbung anpreisen, zahlen für jede Installation ihrer Software zwischen 30 Cent und 1,50 Dollar. Verfügt ein Cyberkrimineller jedoch über ein Botnetz, ist er in der Lage mit nur wenigen Klicks jedes beliebige Programm auf tausenden Computern gleichzeitig zu installieren und auf diese Weise viel Geld zu verdienen. Der bekannte Online-Kriminelle D.K. Schaifer, der 2007 verurteilt wurde, nutzte ein Botnetz, das aus über 250.000 Rechnern bestand. Er konnte so innerhalb nur eines Monats über 14.000 Dollar mit der Installation von Adware auf 10.000 Computern verdienen.

Cyberkriminelle, die Schadprogramme verbreiten, arbeiten häufig nach demselben Schema und zahlen Geld für jede Installation ihrer Software. Dabei wird die Installation von Programmen auf Anwendercomputer in unterschiedlichen Ländern von den Firmen auch unterschiedlich vergütet. Für die Installation von Schadprogrammen auf 1.000 Computer in China werden durchschnittlich drei Dollar, für die USA durchschnittlich 120 Dollar gezahlt. Die Erklärung liegt nahe: Auf den Computern in Industrienationen finden sich wertvollere, das heißt eher auf Finanzen bezogene Informationen.

## Betrügerische Generierung von Klicks

Werbeunternehmen, die online nach dem Prinzip PPC (Pay-per-Click) arbeiten, bezahlen nach Anzahl der Klicks auf ihre Anzeigen. Für Botnetz-Betreiber ist der Betrug dieser Firmen ebenfalls lukrativ. Nehmen wir als Beispiel Google AdSense: Die Werbekunden bezahlen hier nach Anzahl der Klicks auf den von ihnen platzierten Anzeigen, in der Hoffnung, der klickende Anwender wird auch etwas kaufen. Google wiederum platziert Werbung kontextbezogen auf verschiedenen Internetseiten, die am Programm AdSense teilnehmen, und beteiligt den Inhaber der Seite prozentual an jedem Klick.

Allerdings sind nicht alle Webseiten-Besitzer ehrlich. So können Hacker, die über ein Botnetz verfügen, tausende einzelne Klicks pro Tag generieren, und zwar nur jeweils von einem Rechner, um bei Google keinen Verdacht zu erregen. So wandert das Geld des Werbeunternehmens direkt in die Taschen der Hacker. Leider konnten bisher die Täter in so einem Fall noch nie zur Verantwortung gezogen werden.

Nach Angaben von Click Forensics waren im Jahr 2008 etwa 16 bis 17 Prozent aller Klicks auf Werbe-Links gefälscht, wiederum ein Drittel davon wurde von Botnetzen generiert. Botnetz-Besitzer haben folglich im vergangenen Jahr auf diese Weise 33 Millionen Dollar verdient. Nicht schlecht für simple Mausklicks!

## Vermietung und Verkauf von Botnetzen

Die Marx'sche Formel „Ware – Geld – Ware" ist auf der ganzen Welt bekannt. Für die Betreiber von Botnetzen lautet diese Formel „Botnetz – Geld – Botnetz". Um ein Zombie-Netzwerk am Laufen zu halten und den Zufluss neuer Rechner zu gewährleisten sowie die Bots und das C&C vor Entdeckung durch Antivirus-Programme zu schützen, müssen Hacker Geld und Zeit investieren. Es fehlt den Botnetz-Installateuren daher die Zeit, selbst Spam zu versenden, irgendetwas zu installieren, zu stehlen oder Informationen zu verkaufen. Einfacher ist es, das Botnetz zu vermieten oder zu verkaufen – Interessierte gibt es mehr als genug.

Die Pacht für ein E-Mail-Botnetz, das etwa 1.000 Mails pro Minute versendet (bei 100 Zombie-Rechnern online) beträgt etwa 2.000 Dollar im Monat. Der Preis für ein fertiges Botnetz – ebenso wie die Ausleihgebühr – ist abhängig von der Anzahl der infizierten Computer. In englischsprachigen Foren erfreuen sich betriebsbereite Botnetze der größten Beliebtheit. Kleine Zombie-Netze mit nur einigen hundert Bots kosten zwischen 200 und 700 Dollar, der durchschnittliche Preis für einen Bot beträgt 50 Cent. Größere Botnetze gehen für weitaus höhere Summen über den Tisch. Das Shadow-Botnet etwa, das von einem 19-jährigen Hacker aus den Niederlanden aufgebaut wurde und aus mehr als 100.000 Computern aus der ganzen Welt bestand, wurde für 37.290 Dollar verkauft. Eine Summe für die manch einer sich ein kleines Häuschen in Spanien kauft – der Kriminelle aus Brasilien zog aber das Zombie-Netzwerk vor.

# Fazit

Täglich fließen astronomische Summen in die Taschen derjenigen, die auf irgendeine Weise Geschäfte mit Botnetzen machen - und das steuerfrei. Geschäfte dieser Art werden mit allen möglichen Mitteln bekämpft, allerdings ist dieser Kampf auf Gesetzesebene äußert uneffektiv. Die Gesetze über Spam, über die Entwicklung und Verbreitung von Schadprogrammen und das Hacken von Computernetzen werden nicht in allen Ländern der Welt angewendet, sofern solche Gesetze überhaupt existieren. Die Inhaber oder Entwickler von Botnetzen, die sich bisher tatsächlich vor Gericht verantworten mussten, kann man an beiden Händen abzählen. Dies spiegelt nicht das tatsächliche Verhältnis wider – mittlerweile gibt es mehr als 3.600 Zombie-Netzwerke. Die Anzahl der funktionierenden Botnetze zu zählen, ist nicht ganz leicht; denn es gibt zwar einige Dutzend, die so groß sind, dass ihre Aktivität kaum zu übersehen ist, doch die Mehrheit der Zombie-Netzwerke ist kleiner und daher wesentlich schwieriger zu entdecken.

Zum gegenwärtigen Zeitpunkt werden Botnetze am effektivsten bekämpft, wenn Antiviren-Experten, Provider und die Strafverfolgungsbehörden eng zusammenarbeiten. Ein Ergebnis einer solchen Zusammenarbeit war beispielsweise die Schließung der folgenden drei Unternehmen: EstDomains, Atrivo und McColo. Als das Unternehmen McColo geschlossen wurde, sank das weltweite Spam-Aufkommen um die Hälfte, weil sich auf McColo-Servern die Kontrollzentren einiger der größten Botnetze befanden.

Obwohl Fachleute die Tätigkeit von tausenden Botnetzen verfolgen und Antivirus-Produkte Bots weltweit desinfizieren, können nur die Strafverfolgungsbehörden die Kontrollzentren der Zombie-Netze dauerhaft aus dem Verkehr ziehen und die Verbrecher verklagen. Die erwähnte Schließung von McColo hatte allerdings nur einen kurzfristigen Effekt, denn schon nach wenigen Wochen hatte das Spam-Aufkommen im Internet wieder seinen alten Level erreicht. Die Betreiber der Botnetze verlegten ihre Kontrollzentren einfach auf die Plattformen anderer Hosting-Provider und betrieben ihre Geschäfte wie gehabt, als wäre nichts gewesen. Mit vereinzelten Überprüfungen ist es hier leider nicht getan, ständige Kontrolle ist essentiell.

Zur effektiven Bekämpfung von Botnetzen ist die Mithilfe der Anwender ebenfalls sehr wichtig. Denn gerade Heimanwender stellen den größten Anteil der Zombie-Armeen. Die Vernachlässigung der einfachsten Sicherheitsregeln, wie die Nutzung von Antiviren-Software, die Verwendung sicherer Passwörter für Bankkonten und das Abschalten des Autostarts von Dateien mobiler Datenträger kann dazu führen, dass Ihr Computer zu einem weiteren Botnetz-Mitglied wird. Ihre Daten und Ressourcen gelangen dann in kriminelle Hände.