Botnetze

Thomas Köhler

August 19, 2010

Abstract

Diese Ausarbeitung soll im Rahmen des Seminars "'Gefahren aus dem Internet"' der Universität Jena einen Überblick zu der Problematik Botnetze geben, sowie einen Einblick in deren Funktionsweisen und Verwendungsmöglichkeiten geben.

Contents

1 Einführung

Die sehr schnelle Verbreitung des Internets und fortschreitende Automatisierung in allen Bereichen hat auch zu einer neuen Art der Internetkriminalität geführt, welche automatisch über das Internet Straftaten begeht und so Geld für den Botnetzbetreiber bringt. Die Idee der sogenannte Botnetze ist zwar nicht neu, aber die Anzahl der illegalen Netze ist in den letzten 10 Jahren stark gestiegen.

2 Begriffsklärung

Was verbirgt sich hinter dem Begriff Botnetz? Als erstes ist es ein zusammengesetztes Wort aus 'Bot' und 'Netz'. Bot kommt dabei von Roboter. In dem diesem Fall ist Bot aber eine Software. Also eine Software, die selbstständig Aufgaben ausführt. Die Aufgaben werden von dem Ersteller bei der Erschaffung in Auftrag gegeben oder interaktiv während der Laufzeit. Mit Netz ist hier das Internet, beziehungsweise die Verbindungsstruktur der Bots über das Internet gemeint. Die einzelnen Einheiten teilen sich also Befehle oder Ergebnisse mit. Somit wird aus den einzelnen Bots ein großes Botnetz. Schon seit 1996 verteilt GIMPS (Great Internet Mersenne Prime Search) über ihren Client, z.B. Prime95, Mersennezahlen um sie auf Heimrechnern von Interessierten, auf die Primzahleigenschaft zu prüfen. Nach einem ähnlichen Prinzip verteilt SETI Teleskopdaten und die notwendige Berechnungssoftware um auf vielen privaten Rechnern nach Leben auf fremden Planeten zu suchen. Im weiteren werden illegale Botnetze betrachtet. Ein illegaler Bot hat die relevante Eigenschaft, dass die Botsoftware nicht vom Benutzer freiwillig installiert wurde, beziehungsweise in den meisten Fällen hat der PC-Besitzer keine Kenntnis von dem Bot.

3 Gefahr

Die Gefahr besteht in erster Linie darin, dass man als PC-Besitzer keine Kenntnis davon hat des der eigene PC Teil eines Botnetzes ist. Eine Frage die sich nun stellen könnte ist, wenn der Besitzer nichts davon merkt, warum es dann für ihn nachteilig ist. Die Frage ist leicht zu beantworten. Der Bot hat in aller Regel volle Kontrolle über den PC und damit auch über die persönlichen Daten des Besitzers. Solche Daten sind für den Internet-Kriminellen von hohem Wert. Er kann sie weiter verkaufen oder selbst verarbeiten. Für den Besitzer ist das in der Regel unangenehm. Außerdem verliert der Besitzer Rechenleistung und Bandbreite, welche der Internet-Kriminelle finanziell nutzen kann. Dabei muss er aufpassen das der Anteil entsprechend gering ist, sodass der Besitzer es nicht bemerkt. Auch sollte der ehrliche Mensch ein schlechtes Gefühl dabei haben, wenn der eigene

Rechner für Straftaten benutzt wird. Die Motivation sich über Botnetze zu informieren sollte also bei jedem gegeben sein.

4 Verbreitung

Die Möglichkeiten seinen Computer mit einem Bot zu infizieren, sind zahlreich. Einen Rechner nennen wir infiziert wenn er eine illegale Botsoftware installiert hat und das kann schneller passieren als man glaubt. So kann in jeder ausführbaren Datei ein Bot stecken. Er kann auch über eine Spammail mit Bildern auf das System gelangen. Möglich ist, dass aber auch über eine Internetseite die einen Browserbug ausnutzt. In den letzten beiden Fällen muss man nicht einmal aktiv eine Datei heruntergeladen haben. Schadsoftware kann sich also vollständig unbemerkt verbreiten. Einen unterschied zwischen der Verbreitung von Schadsoftware und Botsoftware gibt es im speziellen nicht, so ist jede Verbreitungsmöglichkeit für Schadsoftware auch für Botsoftware denkbar.

5 Möglichkeiten eines Bots

Es gibt viele verschiedene Bots und alle haben andere Funktionen, eines haben aber alle gemeinsam, ihr Ziel ist es Geld für den Botnetzbetreiber einzubringen. Dazu gibt es verschiedene Möglichkeiten, die im Folgenden erläutert werden.

5.1 Spam

Eine typische Anwendung ist das Versenden von Spam, nach Expertenschätzungen kommen 80% aller Spammails aus Botnetzen [4]. Spammails sind unerwünschte e-Mails mit Werbung oder Schadsoftware. Der Bot hat Zugriff auf die privaten Daten des PC-Besitzers und durchsucht diese nach e-Mail Adressen, welche dann zu einer Spamliste hinzugefügt werden. Diese Liste ist außerdem mit Adressen aus anderen Quellen gefüllt. Nun wird jedem infiziertem PC eine Teilliste und eine oder mehrere zu versendene e-Mail mitgeteilt, welche dann an die Adressen verschickt wird. Die Vorteile des Botnetzes sind dabei, das die e-Mails gut verteilt sind. Jeder PC hat eine andere IP-Adresse und somit geht der Spamfluss weiter, auch wenn ein Versender auf einer IP-Blacklist ist. Auch stehen ausreichend Rechenleistung und Bandbreite zur Verfügung um auch große Mengen in kürzester Zeit zu bewältigen. Das Verschicken von Spam kann für den Botnetzbetreiber zweierlei Nutzen haben. Er kann direkt für das versenden von Auftragsspammails bezahlt werden, oder aber er versendet eigene e-Mails mit seinem Bot, um sein Netz zu vergrößern.

5.2 DDoS

Eine weitere typische Nutzung sind DDoS-Attacken. DDoS steht dabei für Distributed Denial of Service, heißt einen angebotenen Service durch Überlastung arbeitsunfähig machen. 'Distributed' zu deutsch verteilt, signalisiert das der Angriff von mehreren, meist mehreren tausenden, Rechnern ausgeht. Der Angreifer braucht daher viele Ressourcen, um eine DDoS Attacke auszuführen. Hier liegt der Vorteil wenn man die Kontrolle über ein Botnetz hat. Es gibt verschiedene Möglichkeiten einen Service zu überlasten, drei davon werden nachfolgend vorgestellt.[1] [3]

Zum einen kann man die Bandbreite sättigen. Jeder Server der Dienste stellt hat eine maximale Anbindung an das Netzwerk beziehungsweise das Internet. Die vorhandene Bandbreite kann gesättigt werden indem viele infizierte Rechner auf den Dienst zugreifen. Dabei ist es sinnvoll wenn die Zugriffe Traffic verursachen, sodass die gesamte Bandbreite von Bots beansprucht wird. Damit erhalten ernsthafte Anfragen keine Verbindung zum Server oder von ihm keine Antwort. Diese Anfragen enden somit meist mit einem Time-out beim Servicenutzer. Der Dienst erscheint abgeschaltet.

Eine andere Art des Angriffes ist das Sättigen von Verbindungen. Die Server haben eine maximale Anzahl an möglichen Verbindungen, Ziel des Angreifers ist es alle Verbindungen zu besetzen. Dies wird zum Beispiel erreicht mit einem Drei-Wege-Handschlag, welchen viele Server anbieten. Geplant ist, dass der Client anfragt, der Server antwortet und auf eine Bestätigung vom Client wartet. Bei einer DDoS Attacke bleibt die Antwort des Clients aus, da er ein infizierter Rechner ist. Der Server wartet vergeblich und dabei bleibt die Verbindung für eine gewisse Zeit offen. Sind alle Verbindungen auf diese Weise besetzt erhalten alle weiteren Anfragesteller eine Ablehnung wegen Überlastung. Der Dienst ist kurzzeitig offline. Da die Verbindungszahl meist sehr hoch ist, sind auch hier viele infizierte Rechner nötig, da ein Rechner mit einer IP nur eine Verbindung besetzen kann.

Eine dritte Möglichkeit ist es einen Programmfehler in der Serversoftware auszunutzen. Dabei wird ein Service entsprechend belastet um den Fehler auszulösen, das Serverprogramm stürzt ab oder läuft in eine Endlosschleife. Das Ergebnis ist, dass der Service nicht mehr Nutzbar ist. Für einen solchen Angriff muss die Serversoftware fehlerhaft sein und der Angreifer muss auch von dem Fehler wissen. Die Vorteile sind dass mitunter nicht so viel Rechenlast notwendig ist und der Service meist einen Tag offline ist, da es dauert bis ein Admin den Fehler behoben hat.

Für den Internet-Kriminellen sind DDoS Attacken eine Art Auftragsgeschäft. Der Auftragsgeber teilt die Adresse des Ziels mit und auch die Dauer und Uhrzeit des Angriffs. Der Botnetzbetreiber rechnet nach Stunden ab, eine Stunde Angriff kann zwischen 10 und 40 Euro liegen. Die Abwicklung der Geschäfte passiert dabei über sogenannte Garanten, sie erhalten das Geld vom Auftraggeber, prüfen die Leistungen des Auftragsausführer

und gibt das Geld an ihn weiter, wenn die Leistung im Sinne des Auftragsgeber war. Garanten sind also die Vertrauensträger beim kriminellen Geschäft. Die Motive des Auftragsgeber können dabei verschieden sein, in Frage kommt dabei alle weswegen ein Mensch gerne einen Nachteil für einen anderen Menschen wünscht, in etwa um einen wirtschaftlichen Vorteil zu erlangen, denn während das Internetangebot eines Konkurrenten nicht erreichbar ist, das eigene aber schon bedeutet dass ein deutlicher Vorteil, da in der heutigen Zeit Zuverlässigkeit und unterbrechungsfreie Bereitstellung der Dienste die wichtigsten Punkte für potenzielle Kunden sind. DDoS Attacken werden auch zur Erpressung genutzt. Ein Botnetzbetreiber schickt eine Drohung an einen Gewerbe oder Betrieb. Die Geschäfte der Opfer sind dabei sehr stark von der Internetpräsenz abhängig. Wird der geforderte Betrag nicht gezahlt, ist genau diese relevante Präsenz für Stunden oder Tagen Ziel eines DDoS Angriffes. Viele Erpresste bezahlen lieber, anstatt zur Polizei zu gehen, da die Polizei nicht schnell genug handelt könnte und der Forderung nachkommen mit unter günstiger ist als das fehlen der Internetpräsenz. Auch wenn die Forderungen meist mehrere Tausend Euro hoch sind.

5.3 Proxydienste

Internet-Kriminelle sind gerne anonym im Netz, daher bieten die Bots meist eine Funktion zum weiterleiten von Anfragen und Antworten ohne das die Verbindungsdaten gespeichert werden. So kann er anonym in Foren Aufträge annehmen und mit Auftragsgebern oder Garanten kommunizieren, ohne Angst haben zu müssen ein Ermittler könnte seinen Aufenthaltsort oder reale Identität bestimmen. Dazu ist eigentlich nur ein infizierter Rechner notwendig, aber wenn man ohnehin mehrere hat, kann man die Anfragen auch in einer Reihe schicken lassen oder häufig den Proxy ändern.

5.4 Hosting

Das Anbieten von Diensten durch ein Botnetz ist problematisch, da es sich nicht um einen zentralen Server handelt der mit einer statischen Adresse angesprochen werden kann, sondern um viele einzelne Computer welche alle eine unterschiedliche Internetanbindung und damit auch eine andere IP-Adresse haben. Genau im letzten Punkt liegt aber der Vorteil für den Botnetzbetreiber. Es gibt zwei Arten von profitablen Dienste die der Betreiber stellen kann, zum einen sind das Dateien. Beim File-Hosting liegen auf den infizierten Rechnern illegale Dateien welche anderen, nach Bezahlung, bereitgestellt werden. Bei diesen Dateien handelt es sich meistens um solche welche von den Ermittlern stark gesucht werden, wie etwa kinderpornographische Inhalte. Wenn ein Ermittler nun aber einen Host gefunden hat, hat er nicht den Kriminellen gefunden, sondern nur einen infizierten Com-

puter. So ist der Botnetzbetreiber sicher und kann über andere Infizierte weiter seine illegalen Inhalte verbreiten.

Eine andere Art ist das Phishing-Hosting. Dabei werden sogenannte Phishingseiten gehostet um an Logindaten zu kommen. Eine solche Seite sieht für gewöhnlich so aus wie eine bekannte Seite, wie etwa die Anmeldeseite von eBay oder einem Mailserviceprovider. Wird der unbedarfte User auf eine solche geleitet denkt er, er wäre bei eBay und gibt seine Daten ein. Diese Daten gelangen aber in die Hände des Internet-Kriminellen und der User wird nicht eingelogt. Mit den Logindaten kann der Kriminelle nun die e-Mails des Opfers lesen, einen Account übernehmen oder sie verkaufen. Phishing ist nicht an ein Botnetz geknüpft und existiert auch mit normalen Hostservern. Der Nachteil bei solchen ist die möglicherweise fehlende Anonymität, es gibt aber viele Server die man im Ausland anonym mieten kann. Ein anderer Vorteil des Botnetzes ist die Immunität gegen eine Blacklist, große Browseranbieter führen Blacklisten von verdächtigen Servern und warnen vor dem Besuch mit einem Warnbild. Da ein Botnetz sehr viele Adressen hat, kann eine Blacklist immer nur einen kleinen Teil sperren und der Botnetzbetreiber kann weiter Daten sammeln.

Hosting und Proxydienste können auch kombiniert werden. Dabei werden die Dienste von einem normalen Server gestellt. Kunde oder Opfer werden aber auf Adressen verwiesen welche zu den infizierten Rechner führen. Die Bots leiten dann die Anfrage weiter, so spart man sich das Hochladen der Hostinginhalte auf die Botrechner.

5.5 Verkauf und Vermietung

Ein erfolgreiches Botnetz kann schon mal schneller wachsen als sein Betreiber Aufträge finden kann, auch ist das wirkliche Nutzen seines Botnetzes mitunter gefährlicher und schwieriger als der Aufbau. Dies sind Gründe warum ganze Netze vermietet oder verkauft werden. Dem Käufer wird dazu ein Tool mit einfacher grafischer Oberfläche zur Verfügung gestellt, mit dem auch unerfahrene Nutzer einfach die Funktionen des Botnetzes nutzen können. Mit zwei Klicks ist so eine DDoS Attacke gestartet. Verkauf und Vermietung ist für die Betreiber sehr lokrativ. So werden mitunter infizierte Rechner mit kryptografischen Funktionen ausstatten, sodass unterschiedliche Passwörter für unterschiedliche Teilnetze benötigt werden um sie zu kontrollieren. So kann man einem Teilnetz ein bestimmtes Passwort zuteilen, dieses Verkaufen und der Käufer hat nun Kontrolle über die Rechner des Teilnetzes. Der Rest des Netzes ist aber weiterhin unter alleiniger Kontrolle des ursprünglichen Betreibers.

5.6 Sonstiges

Hat der Bot die Kontrolle über den infizierten PC erlangt, kann er sich der Daten habhaft machen. Diese persönlichen Daten kann der Botnetzbetreiber nutzen oder verkaufen. Allerdings bietet sich ihm auch die Möglichkeit sie lokal zu verschlüsseln und dem Besitzer der PCs mitzuteilen das er bezahlen muss um wieder an seine Daten zu kommen. Er erpresst also ein Lösegeld für die Daten. Dies ist aufwendig, gefährlich und wenig lukrativ, deswegen wird diese Funktion selten genutzt. Da dem Betreiber viele Rechner und somit viel Rechenleistung zur verfügung steht, kann er auch versuchen an Passwörter mit Brute-Force Angriffen zu kommen. Dabei wird jedes mögliche Passwort geraten und überprüft. Vorteil ist, das er somit die Passwörter von gezielten Opfern ermitteln kann, der Nachteil ist, das starke Passwörter auch bei einer sehr hohen Anzahl von ratenden PCs nicht in einer akzeptablen Zeit gefunden werden können.

Mit vielen Rechnern gehen auch viele IPs einher, diese kann der Betreiber nutzen um den Wert gewisser Internetseiten zu erhöhen. Der Wert einer Seite hängt stark von der Zahl an Besuchern ab. Wenn jeder Bot jeden Tag diese Seiten besucht, wird eine solche Seite sehr schnell wertvoll und kann verkauft werden.

Auf allen infizierten Rechnern läuft ungewollte Software. Daher ist es einfach, etwas mehr zu installieren und noch eine Spyware mit einzuschmuggeln welche dem Besitzer ungewollt Werbung anzeigt, dies bringt zusätzlich Geld. Der Nachteil ist, das der User erkennt, dass auf dem PC ungewollte Software installiert ist und sich möglicherweise bemüht sie zu entfernen.

6 Verbindungsstrukturen

Der Unterschied zwischen einem normalen Computerschädling und einem Botnetz ist die Vernetzung zwischen den einzelnen Bots. Die verschiedenen Verbindungsstrukturen sind daher ein wichtiges Merkmal für die Eigenschaften eines Botnetzes. Grundsätzlich gibt es zwei Arten die zu Unterscheiden sind.

6.1 Command and Control

Dies ist zu vergleichen mit der klassischen Server Client Architektur. Dabei sind die Clients die einzelnen Bots, sie werden von einem Command and Control Server gesteuert. Der Botnetzbetreiber kontrolliert den CnC Server und gibt diesem Befehle. Der Server ist verbunden mit den einzelnen Bots, und reicht die Befehle weiter. So erhält jeder Bot die Befehle von dem Server fast zeitgleich. Dafür ist ein potenter Server notwendig, der es schafft eine hohe Zahl an Clients zu verwalten. Solch ein Server wird entweder anonym im Ausland gemietet oder ebenfalls infiziert. Das Problem ist, das ein pro-

fessionell genutzter Server meist andere Software, also Betriebssystem und Sicherungssoftware, hat welche zu überwinden gilt. Es ist also Notwendig den Server und die Clients jeweils auf zwei unterschiedliche Weisen zu infizieren. Ein weiterer Nachteil für den Betreiber ist, dass der CnC Server einen großen Schwachpunkt für das Botnetz darstellt. Wird er abgeschaltet bricht das Botnetz zusammen. Die Rechner sind zwar noch infiziert, können aber nicht mehr befehligt werden.

Ein Beispielprotokoll für ein CnC-Netz ist das IRC-Protokoll, welches vor allem bei den frühen Botnetzen eingesetzt wurde, da es bereits IRC-Bots gab und bei vielen Systemen schon ein Low-Level IRC-Client installiert war. Wurde ein Rechner infiziert verband er sich mit einem IRC-Raum um dort von einem ausgezeichnetem Usernamen Befehle zu empfangen. Die Räume waren meist auf öffentlichen Servern, dies führte zu Botnetzpiraten. Ein Botnetzpirat kapert ein fremdes Botnetz. Dies ist möglich in dem er den Raum sucht wo sich die Bots treffen. Das ist möglich, da es sich um den Raum handelt wo an die Tausend oder mehr User sind. Jetzt muss er noch herausfinden welcher User derjenige ist der die Befehle gibt und sich seinen Namen aneignen, was je nach IRC-Server unterschiedlich schwer sein kann. Hat er den Namen kann er, wenn er weiß wie, selber Befehle geben. Unabhängig davon ist es für Ermittler oder den Betreiber des IRC-Server einfach den CnC-Server, beziehungsweise CnC-Raum, des Botnetzes abzuschalten, was zur Ursache hat dass das Botnetz stirbt. Aus diesen und anderen Gründen wird gibt es kaum noch IRC-Botnetze.

6.2 Peer-to-Peer

Jeder Bot kann Befehle erhalten und weiter senden, es gibt keinen ausgezeichneten Server der die Befehle verteilt. Somit auch keinen zentralen Knoten an dem man das Botnetz zerschlagen könnte. Der Betreiber kann sich bei einem beliebigen Bot anmelden und ihm Befehle geben, und auch befehlen das die Befehle weiter gegeben werden. Es darf keine globale Liste geben auf der alle Bots stehen, sonst könnten Botnetzgegner mit dieser Liste wieder das gesamte Netz zerschlagen, auch wäre das erstellen und aktuell halten einer solchen Liste nicht einfach. In den Anfangszeiten gab es Server die solche Listen pflegten, allerdings konnte man dann das Botnetz mit diesem Server abschalten. Stattdessen hat in neueren Netzen jeder Bot eine Liste seiner Nachbarn, welche zum Beispiel ein ähnliches Datum der Infizierung haben oder auf die gleiche Art infiziert wurden. Diese Nachbarschaftslisten nutzen die Bots zum verteilen der Befehle. Entweder sendet jeder der einen neuen Befehl erhalten hat, diesen an seine Nachbarn oder jeder prüft ob einer seiner Nachbarn einen aktuelleren Befehl hat. Im Vergleich zu Command and Controll dauert das weitergeben der Befehle wesentlich länger, was bei zeitkritischen Anwendungen, wie zum Beispiel eine DDoS Attacke ein Problem sein könnte.

Es gibt auch Mischformen, wo manche Bots die Aufgaben eines Servers übernehmen. Geeignete infizierte Rechner werden als Server ausgezeichnet, diese erhalten eine Liste ihrer Clients und außerdem eine Liste einiger Nachbarservern, so erhalten alle Bots die Befehle. Möglich ist auch, dies die Clients ihren Server kennen, so ist eine Liste beim Server nicht nötig. Die teils sehr komplizierte Netzwerkprotokolle die so etwas ermöglichen zeigen das die Botnetzentwickler über hohe Fachkenntnisse verfügen, außerdem zeigt der hohe Aufwand der in einem modernen Botnetz steckt wie viel Geld sich damit verdienen, beziehungsweise ergaunern, lässt.

7 Schutzmöglichkeiten

Um viel Geld mit einem Botnetz zu verdienen muss es groß sein. Um eine möglichst große Zahl an infizierten Rechnern im Botnetz zu haben, versuchen die Botnetzbetreiber solche Rechner anzugreifen von denen es möglichst viele gibt. Wie zum Beispiel MS Windows PCs mit x86 Architektur, welche einen großen Marktanteil haben. Solche Rechner sind insbesondere gefährdet, aber auch wenn der eigene Rechner zu einer Minderheit gehört ist dies keine Sicherheitsgarantie. So sind gibt es auch Botnetze die gezielt Linuxsysteme angreifen [2].

7.1 private Schutzmöglichkeiten

Botnetze sind deswegen so erfolgreich weil es viele ungeschützte oder unzulänglich geschützte Rechner gibt. Dabei sind nur wenige einfache Punkte zu beachten um sich zu schützen. Stets ein aktuelles Betriebssystem verwenden, dazu zusätzlich aktuelle Sicherheitssoftware, wie ein Antivirenprogramm und eine Hard- oder Softwarefirewall. Die Schutzmaßnahmen die im Betriebssystem integriert sind, sind häufig unzulänglich. Auch ist es wichtig immer die aktuellste Version des Browsers zu haben um vor Browserexploits geschützt zu sein. Browserexploits nennt man das Ausnutzen von Fehlern in einem Browser, bei guten Browseranbietern werden solche Fehler aber mit der öffentlichen Entdeckung gefixt. Die Nutzer der alten Version sind aber weiterhin angreifbar. Auch bieten viele Browser Schutzmaßnamen vor Phishingseiten, welche aktualisiert werden müssen. Das wichtigste überhaupt ist aber ein vorsichtiger Umgang mit Dateien aus dem Internet, das aktuellste System nutzt nichts wenn man unvorsichtig ist. Nur Dateien von vertrauenswürdigen Seiten laden. Dateien welche den Kopierschutz von kommerzieller Software umgehen oder das versprechen, sind häufig schadhaft. Auch das e-Mail Programm sollte stets aktuell sein. e-Mails mit Bildern können schon beim laden der Bilder Schaden anrichten. Die meisten e-Mailclients bieten daher eine Option Bilder erst zu laden wenn der Benutzer zustimmt das die e-Mail vertrauenswürdig ist, diese Option sollte aktiviert sein.

7.2 Botnetzzugehörigkeit testen

Wie jede Schadsoftware versucht sich ein Bot so gut wie möglich zu verstecken, in der Prozessliste des Windows Taskmanager ist der Bot meistens nicht zu finden. Verraten tut er sich nur wenn er seinen Aufgaben nachgeht und entsprechend Rechenleistung oder Bandbreite beansprucht. Enttarnen kann man den Bot auch wenn er einen Dienst stellt, von dem der Besitzer nichts weiß. Wird der Rechner nicht benutzt, die Router LED blinkt aber oder die Festplatte dreht sich hörbar, könnten das Zeichen für Schadsoftware sein, die Daten über mittelt oder nach persönlichen Daten sucht. Es kann aber auch einfach ein automatisches Update oder die Festplatten Indexierung sein. Ein modernes Betriebssystem übernimmt, ähnlich wie ein Bot, eigenständig Aufgaben. Möchte man mit Sicherheit sagen ob man zu einem Botnetz gehört, muss man seine Netzwerkpakete mit einem Sniffer überprüfen. Ein solches Programm zeigt einem die versendeten und empfangenen Pakete an und versucht möglichst viele Informationen darüber anzuzeigen. Um zwischen erwünschten und unerwünschten Paketen zu unterscheiden sind aber viel Erfahrung und Fachkenntnisse notwendig. Wenn im Testzeitraum nicht auffälliges zu sehen war, kann der Bot aber auch inaktiv gewesen sein. Manche Bots verhalten sich auch ruhig, wenn sie erkennen das ein Netzwerksniffer gestartet wurde. Letzteres kann man aber umgehen indem man den Sniffer auf dem Router startet, sofern er dies ermöglicht.

7.3 gewerbliche und staatliche Gegenmaßnahmen

Das Ziel von Staat und Gewerbe ist nicht das Schützen des eigenen Rechners, sondern der Schutz seiner Steuerzahler, seines Netzes oder seiner Server. Das Ziel ist also jeweils das gesamte Botnetz. Die größte Gefahr für Netz und Server gehen von den DDoS Attacken aus. Serverbetreiber versuchen diese zu unterbinden mit sogenannten Honeypots, zu deutsch Honigtopf. Ein solcher Honeypot bietet einen Dienst an, welcher für einen normalen Nutzer nicht zugänglich wäre, ein Bot erkennt das aber nicht und versucht auch diesen Service zu besetzen. Des Ergebnis ist, dass der Serverbetreiber die Adresse des Angreifers hat und diesen blocken kann. Da alle Bots den Honey-Service angreifen kennt er also alle Adressen der Angreifer und kann alle blocken. So bleiben die Dienste für ernsthafte Benutzer Online, es sei den dieser Nutzer ist Teil des Botnetzes, dann wäre er auch noch geblockt.

Eine andere Art von Honigtopf ist ein extra präpariertes System. Dieses ist leicht infizierbar. Ist das System infiziert ist der Bot gefangen, er wird nun von Fachkräften untersucht. Zum Beispiel kann er disassemblet werden. Heißt er wird in einer Programmiersprache dargestellt, die zwar Maschinennah ist, aber dennoch von entsprechenden Fachkräften gelesen werden kann. Sie finden so heraus mit welchen Servern er kommuniziert und sich auch sonst verhält. Die gesamte Kommunikation kann man auch einfacher über

einen Paketsniffer aufdecken und so, sofern vorhanden, den globalen Server finden und abschalten, wenn es die Rechtslage erlaubt oder der Server zum eignen Netz gehört. Rückschlüsse auf die realen Identitäten der Internet-Kriminellen lassen sich so allerdings für gewöhnlich nicht machen. Diese lässt sich herausfinden indem man sich als Auftragsgeber ausgibt und hofft das der Botnetzbetreiber so private Daten preis gibt, wie etwa Name oder Kontodaten. Dies ist aber den staatlichen Ermittlern vorbehalten.

8 Juristische Standpunkte

Opfer eines Botnetzes kann jeder werden. Ist ein System für das man Verantwortung trägt, so wie zum Beispiel der heimische PC, infiziert und Teil eines kriminellen Aktes, so ist man selbst erst einmal ein Ziel der Ermittler. Nun wird untersucht ob der PC ausreichend geschützt war, wenn dem so ist, hat man gute Chancen nicht haften zu müssen. Ist der eigene PC allerdings völlig ungeschützt, so handelt man fahrlässig und kann bestraft werden. Die staatlichen Maßstäbe für ein gesichertes System, sind nicht sehr hoch. Jeder kann sie leicht erfüllen und ist so auf der sicheren Seite. Es empfiehlt sich aber auch sein System darüber hinaus zu schützen. Auch wenn ein Richter meint, man hätte sich geschützt, entfernt das nicht die eigenen persönlichen Daten bei einem Internet-Kriminellen. Gegen den Botnetzbetreiber gibt es auch Gesetze, das ungewollte installieren von Schadsoftware ist eine Straftat. Die höchst Strafe kann bis zu 10 Jahren Haft sein, wenn man in einer Gruppe organisiert ist. Botnetzbetreiber agieren häufig in Gruppen, wegen den hohen Erfordernis an Fachkenntnissen.[11]

References

[1] http://de.wikipedia.org/wiki/Denial_of_Service

[2] http://www.pcwelt.de/start/sicherheit/sonstiges/news/2102940/linux_botnet_entdeckt/

[3] http://en.wikipedia.org/wiki/Denial-of-service_attack

[4] http://www.kaspersky.com/de/downloads/pdf/vkamluk_botnetsbusiness_0508_de_pdf.pdf

[5] http://de.wikipedia.org/wiki/Botnet

[6] http://en.wikipedia.org/wiki/Botnet

[7] www.fh-trier.de/index.php?id=4365 “Botnetze“

[8] http://blog.botnetzprovider.de/

[9] http://www.computerwoche.de/security/557828/index9.html
"Wie sich Bot-Netze enttarnen lassen"

[10] http://www.gulli.com/privacy/rechtliches

[11] http://dejure.org/gesetze/StGB/303b.html