Threat Update: Botnets

e-center, Technology Unit
Lukas Feiler
26. Mai 2006

Inhalt

1. Einleitung

Ein Botnet ist eine Ansammlung von gehackten Computersystemen, die zentral gesteuert werden können.[1] Der Begriff Botnet setzt sich aus den Begriffen „robot“ und „network“ zusammen. Als Bot wird jenes Programm bezeichnet, das auf den einzelnen Systemen des Botnets installiert ist und – ähnlich einem Roboter – weitgehend selbstständig seine Arbeit verrichten kann. Die gehackten Systeme selbst werden ob ihrer Fremdbestimmtheit treffend als Zombies bezeichnet. Daher hat sich für ein Botnet auch der Begriff „Zombie Army“ etabliert. Ein durchschnittliches Botnet besteht aus ca. 20.000 Computersystemen.[2] Schätzungen zufolge sind ca. 47 Millionen Computersysteme weltweit Teil eines Botnets.[3] Bei den Zombies handelt es sich meist um schlecht gewartete PCs von Heimanwendern. Viele zur Erstellung eines Botnets erforderliche Angriffswerkzeuge sind im Internet frei verfügbar, weshalb es auch Personen, die über keine besonderen technischen Kenntnisse verfügen, möglich ist als Angreifer zu fungieren. Jene Person, die die Kontrolle über das Botnet ausübt wird häufig als „Botmaster“ bezeichnet.

2. Die Funktionsweise eines Botnets

Drei Faktoren bestimmen maßgeblich die Eigenschaften eines Botnets: die Art der Rekrutierung von Systemen für das Botnet, die Organisationsform des Botnets und die Fähigkeit sich selbst zu aktualisieren.

2.1. Rekrutierung von Systemen für das Botnet

Grundsätzlich sind dem Botmaster keine Grenzen bei der Wahl der „Rekrutierungsmethode“ gesetzt. Es können hierzu beispielsweise E-Mail-Viren, die den Benutzer zum Öffnen eines

---

[1] vgl *Jones*, BotNets: Detection and Mitigation
[2] *Kawamoto*, Bots slim down to get tough; SANS NewsBites, Volume: 7, Issue: 55, Botnets Get Lean to Avoid Detection
[3] SANS NewsBites, Volume: 8, Issue: 33, Bot Crimes on the Rise

Attachments auffordern, präparierte Websites, die Sicherheitslücken in Browsern ausnützen, trojanische Pferde[4] oder Würmer[5] verwendet werden. Wie auch immer es zur Ausführung der Befehle des Botmasters auf einem System kommt, bewirken diese stets die Installation des Bots, wodurch der übernommenen Rechner als Zombie Teil des Botnets wird.
Die gewählte Rekrutierungsmethode ist ausschlaggebend für die Dynamik des Botnets. Während bei trojanischen Pferden oder Viren die Verbreitungsgeschwindigkeit durch die erforderliche menschliche Interaktion stark begrenzt ist, können durch den Einsatz von Würmern in wenigen Minuten zigtausende von Systemen in Zombies verwandelt werden.[6]

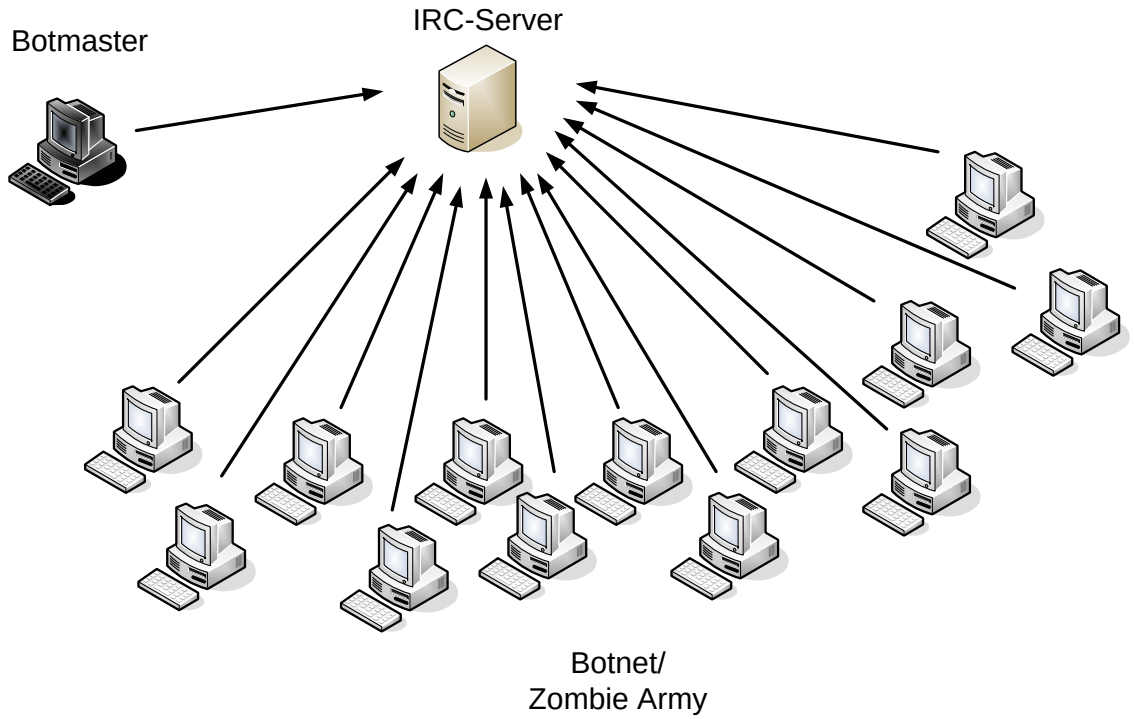
2.2. Organisation des Botnets

Grundsätzlich kann in zentrale und dezentrale Strukturen unterschieden werden. Die meisten Botnets sind derzeit noch zentral organisiert.

Zur Implementierung einer zentralisierten Struktur kommt meist IRC – das Internet Relay Chat Protocol[7] – zum Einsatz. Grundsätzlich ermöglicht IRC die schriftliche Kommunikation mehrerer Benutzer in Echtzeit (sog. „chatten“). Ein Benutzer verbindet sich hierzu mit einem IRC-Server und schließt sich dann einem bestimmten Chat-Room (sog. Channel) an. Channels können durch Passwörter (im IRC-Jargon als „Keys“ bezeichnet) geschützt werden. Weiters sind jedem Channel ein oder mehrere Benutzer mit administrativen Rechten (sog. „Channel Operators“ od auch „ChanOps“) zugeordnet.[8]
Im Falle des Einsatzes von IRC zur Organisation eines Botnets nehmen die einzelnen Bots die Position von IRC-Benutzern ein. Sie verbinden sich zu einem vom Angreifer zuvor bestimmten IRC-Server und schließen sich dort einem vom Botmaster eingerichteten Channel[9] an. Zur zentralen und einheitlichen Steuerung aller Bots verbindet sich der Botmaster mit diesem Channel und sendet über diesen eine oder mehrere Nachrichten an alle Bots. Die Nachrichten werden von den Bots als Befehle interpretiert, die je nach Ausgestaltung des Bots die unterschiedlichsten Aktionen auslösen können.

Die folgende Abbildung zeigt die Struktur eines zentral organisierten Botnets.

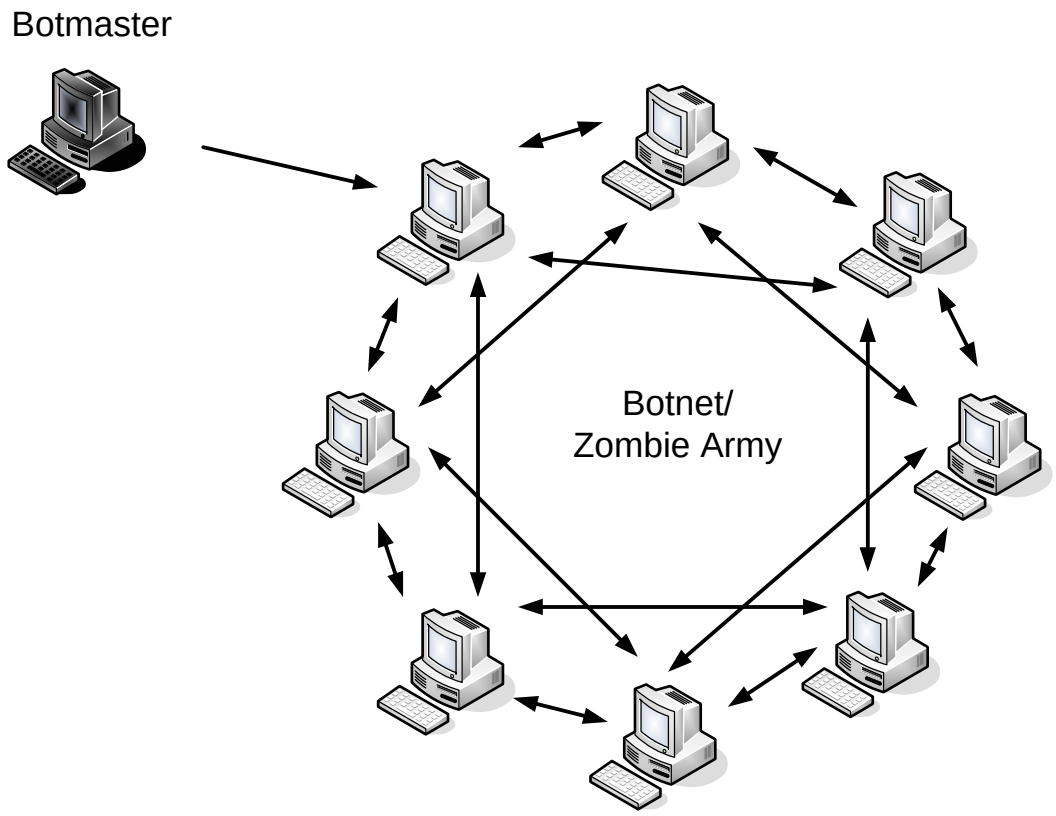
[4] Mythologisch unkorrekt auch als „Trojaner“ bezeichnet.
[5] Würmer erfordern im Unterschied zu Viren für ihre Verbreitung keinerlei menschliche Interaktion.
[6] vgl *Staniford/Paxson/Weaver*, How to 0wn the Internet in your spare time
[7] spezifiziert in RFC 1459; aktualisiert durch RFCs 2810, 2811, 2812, 2813
[8] Vor der Möglichkeit sich durch statische Listen dauerhaft die Position eines Channel Operators zu sichern, war es erforderlich dies von Programmen während seiner Abwesenheit besorgen zu lassen. Diese als „Bots“ bezeichneten Programme nahmen weiter am Channel teil und wahrten so die Rechte des abwesenden Channel Operators.
[9] Im Zusammenhang mit Botnets wird ein solcher Channel auch als „Command and Control Channel“ (kurz „C&C“) bezeichnet. Vgl http://www.spamhaus.org/faq/answers.lasso?section=ISP%20Spam%20Issues#143.



Der zentrale IRC-Server stellt grundsätzlich einen Single Point of Failure für das gesamte Botnet dar.[10] Zur Bekämpfung eines zentral organisierten Botnets ist es ausreichend den zentralen IRC-Server auszuschalten. Es ist hingegen nicht erforderlich, die einzelnen Zombies zu desinfizieren (dh den Bot zu deinstallieren). Die Widerstandsfähigkeit von zentral organisierten Botnets ist daher relativ gering.

Um eine höhere Widerstandsfähigkeit zu erreichen, werden Botmaster dazu übergehen dezentrale Strukturen einzusetzen. Denn um ein dezentral organisiertes Botnet zu bekämpfen, ist es nicht ausreichend einige wenige Systeme aus dem Botnet zu entfernen. Obgleich dezentrale Botnets in der Praxis derzeit nur vereinzelt auftreten[11], erscheint es aus heutiger Sicht wahrscheinlich, dass sie mittelfristig zentral organisierte Botnets ablösen werden. Dezentrale Botnets können die unterschiedlichsten Methoden zur Vernetzung der einzelnen Bots einsetzen. Besonders nahe liegt jedoch die Verwendung von als Open Source Software zugänglicher Peer-to-Peer (P2P) Technologie.[12] Die folgende Abbildung zeigt ein dezentrales Botnet.

[10] IRC ermöglicht es auch einen Channel auf redundante Weise über mehrere IRC-Server anzubieten. Dies erhöht die Widerstandsfähigkeit des Botnets jedoch nur unwesentlich.
[11] vgl *Fendley*, As the Bot Turns, SANS Internet Storm Center
[12] So wurden bereits Botnets gesichtet, die die P2P-Sofware WASTE (http://waste.sourceforge.net) einsetzen. Vgl *Fendley*, As the Bot Turns, SANS Internet Storm Center.



Wie in der Abbildung angedeutet, ist es dem Botmaster möglich, neue Befehle an jedem Punkt des Botnets einzuschleusen. Denn erhält ein Bot einen Befehl, verteilt er diesen über das dezentrale Netz an alle anderen Bots. Um dem Botmaster eine Authentifizierung zu ermöglichen, so dass nur er Befehle im Botnet ausführen kann, können alle Befehle mit einer elektronischen Signatur versehen werden. Jeder der Bots müsste diesfalls über den Public Key des Botmasters verfügen. Nur bei korrekter Signatur würde der Befehl ausgeführt bzw. an die anderen Bots weitergeleitet werden.

Die Widerstandsfähigkeit des Botnets äußert sich in den Auswirkungen der Desinfektion einzelner Bots. Zunächst ist entscheidend mit wie vielen anderen Bots ein Bot in direkter Verbindung steht (in obiger Abbildung mit vier). Denn umso geringer diese Anzahl ist, desto größer ist die Wahrscheinlichkeit, dass durch die Desinfektion eines oder mehrerer Bots andere Bots ihre Verbindung zum Botnet verlieren.[13] Es darf jedoch nicht vernachlässigt werden, dass nach dem Verlust der Verbindung zum Botnet die Möglichkeit besteht durch das Auffinden anderer Bots erneut eine Verbindung herzustellen. Im Ergebnis kann daher festgehalten werden, dass eine gänzliche Abschaltung eines dezentralen Botnets – im Unterschied zu zentral organisierten Botnets – kaum möglich ist, da sie die Desinfektion nahezu aller Zombies erfordert.

2.3. Botnet Updates

Fortgeschrittenere Botnets verfügen über die Möglichkeit sich selbst zu aktualisieren. Hierzu ist es nur erforderlich, dass der Botmaster einen Befehl auf allen Bots ausführen kann, der bewirkt, dass eine neuere Version des Bots aus dem Internet herunter geladen und installiert wird. Botnet Updates ermöglichen es beispielsweise mehrere Botnets zu einem zusammenzufassen oder ein zentrales in ein dezentrales Botnet zu transformieren.

---

[13] *Reiher/Li/Kuenning*, Midgard Worms: Sudden Nasty Surprises from a Large Resilient Zombie Army

2.4. Worst Case: ein aktualisierbarer, dezentraler Botnet-Wurm

Eine Kombination verschiedener oben genannter – und in der Praxis isoliert bereits eingesetzter – Techniken könnte zur bislang größten Bedrohung für das Internet erwachsen.

Wie unter 2.1. dargestellt, sind unterschiedliche Methoden zur Rekrutierung von neuen Zombies denkbar. Die weitaus effizienteste – und daher gefährlichste – besteht im Einsatz eines Wurms. Als Wurm wird jene Schadsoftware („Malware") bezeichnet, die sich selbstständig (dh ohne menschlicher Interaktion) durch die Ausnützung von Sicherheitslücken im Internet verbreitet. Da jedes infizierte System in Sekunden (oder gar Sekundenbruchteilen) wiederum andere Systeme infiziert, ergibt sich eine äußerst hohe Verbreitungsgeschwindigkeit. So können bereits in wenigen Minuten zigtausende Systeme als Zombies für ein Botnet rekrutiert werden.[14] In einem derart kurzen Zeitraum ist eine menschliche Reaktion – sei es durch das Personal eines ISP oder eines Großunternehmens – nahezu unmöglich.

Unter 2.2. wurde die äußerst hohe Widerstandsfähigkeit dezentraler Botnets dargestellt. Aus Sicht eines Botmasters sind dezentrale Botnets zentral organisierten Botnets daher jedenfalls vorzuziehen.

Verfügt das Botnet auch über die Funktionalität sich selbst zu aktualisieren, so entsteht eine noch größere Widerstandsfähigkeit und Dynamik des Botnets. Die Effektivität des Wurmes könnte dadurch wesentlich gesteigert werden, da dieser mit Exploits[15] für die neuesten Sicherheitslücken ausgestattet werden könnte. Auch die Erkennung des Bots durch Anti-Viren Software könnte durch Updates erheblich erschwert werden.[16]

Zusammenfassend verfügt ein derartiges Botnet daher über folgende Eigenschaften:

a) die Rekrutierung neuer Zombies erfolgt durch einen Wurm
b) das Botnet ist dezentral organisiert, wodurch das Entfernen einzelner Systeme die Operabilität des Botnets nicht wesentlich beeinträchtigt.
c) der Botmaster kann alle Bots (einschließlich des Verbreitungsmechanismus) jederzeit aktualisieren

Ein derartiges Botnet kann daher auch als aktualisierbarer, vom Angreifer steuerbarer Wurm betrachtet werden.[17]

3. Einsatzgebiete eines Botnets

Mit einem Botnet besitzt ein Botmaster eine äußerst gefährliche „Waffe", die auf unterschiedlichste Weise eingesetzt werden kann. Im Folgenden soll ein Überblick über die möglichen Verwendungen eines Botnets gegeben werden.

Eine der ersten Anwendungsbereiche für Botnets bestand in der Durchführung von Distributed Denial of Service (DDoS) Attacks.[18] Der Botmaster bringt hierbei alle Bots dazu, gleichzeitig ein bestimmtes anderes System mit Anfragen zu überfluten, wodurch dieses nicht mehr in der Lage ist, legitime Anfragen zu beantworten. Verfügt beispielsweise ein Botmaster über 10.000 Bots mit einer durchschnittlichen Bandbreite von 1 Megabit pro Sekunde, so ist er in der Lage einen Datenverkehr von ca. 10 Gigabit pro Sekunde zu erzeugen. Übersteigt

---

[14] vgl *Staniford/Paxson/Weaver*, How to 0wn the Internet in your spare time
[15] Ein Exploit ist ein Programm oder Programmteil, zur automatisierten Ausnützung einer Sicherheitslücke.
[16] Um die Erkennung weiters zu erschweren könnten zusätzlich Rootkit-Funktionalitäten implementiert werden.
[17] *Reiher/Li/Kuenning*, Midgard Worms: Sudden Nasty Surprises from a Large Resilient Zombie Army
[18] vgl *Puppe/Maier*, Von allen Seiten, Maßnahmen gegen Distributed-Denial-of-Service-Angriffe, iX 4/2005, S. 107

dies die dem angegriffenen System zur Verfügung stehende Bandbreite, so tritt ein Denial of Service ein.

Da der Botmaster durch den auf jedem Zombie installierten Bot grundsätzlich über vollen Systemzugriff verfügt[19], kann er auch beliebige Programme installieren. Häufig bringen Botmaster Spyware zum Einsatz um finanziell verwertbare Daten zu erlangen. Beispielsweise könnten als Sniffer bezeichnete Programme dazu verwendet werden den Netzwerkverkehr der einzelnen Benutzer aufzuzeichnen und zu analysieren. Ebenso ist der Einsatz von Keyloggern denkbar, die jeden Tastendruck protokollieren.[20]

Wird Peer-to-Peer Technologie zur Organisation des Botnets eingesetzt, liegt es besonders nahe, das Botnet zum Hosting von rechtswidrig vervielfältigter Software, Musik und Filmen („Warez“) zu verwenden.[21]

Weiters eignen sich Botnets hervorragend zum Versenden von Spam. Schätzungen zufolge werden bereits 60 bis 70% aller weltweiten Spams von Botnets versendet.[22] Dies ist eine äußerst lukrative Verwendungsmöglichkeit eines Botnets, da bestimmte Werbeunternehmen für die Möglichkeit Spams zu versenden Entgelt anbieten.[23]

Ebenso wie für das Versenden von Spam kommen Botnets zunehmend für das Versenden von Phishing-Mails zum Einsatz. Der Vorteil der Verwendung eines Botnets liegt in der schweren Rückverfolgbarkeit.

Eine weitere Verwendungsmöglichkeit eines Botnets besteht im sog. Pharming. Hiermit wird eine Angriffsform bezeichnet, mit der die Auflösung eines Domainnamens in eine IP-Adresse manipuliert werden kann. Da das im Bereich des Internets stets verwendete Protokoll IP[24] eine Adressierung einzelner Computersysteme nur durch IP-Adressen vornehmen kann, muss jeder Domainname in eine IP-Adresse aufgelöst werden. Hierzu werden idR DNS-Server verwendet. Vor Durchführung einer DNS-Abfrage wird von den meisten Betriebssystemen jedoch eine lokale Datenbank nach dem Domainnamen durchsucht.[25] Wird die lokale Datenbank vom Botmaster manipuliert, und beispielsweise der Eintrag „192.168.1.100 www.amazon.com“ hinzugefügt, so würde bei Eingabe des Domainnamens www.amazon.com eine Verbindung zu 192.168.1.100 anstelle des tatsächlichen Amazon.com-Servers hergestellt werden. Damit ist es möglich Benutzer auf eine Site umzuleiten, die der tatsächlichen Site zum verwechseln ähnlich sieht. Ähnlich wie bei Phishing-Angriffen, sollen die Benutzer dazu gebracht werden Zugangsdaten oder Kreditkartendaten preiszugeben.

Auch die Verbreitung von Adware wird durch Botnets erheblich erleichtert. Als Adware wird Software bezeichnet, die automatisch und unaufgefordert Werbung anzeigt. Auf jedem Zombie Adware zu installieren ist für Botmaster eine der schnellsten Möglichkeiten Kapital

---

[19] Statistisch gesehen gilt dies insbesondere für schlecht konfigurierte Windows-PCs.
[20] Um die Effizienz bei der Suche nach relevanten Zugangsdaten zu erhöhen wäre es auch möglich nur die ersten 100 Zeichen zu protokollieren, die beispielsweise nach der Eingabe der Zeichenkette „ebay.com” eingegeben wurden.
[21] vgl *Vamosi*, Pirated movies now playing on a server near you
[22] Evers, Most spam still coming from the U.S., CNET News.com, http://news.com.com/Most+spam+still+coming+from+the+U.S./2100-1029_3-6030758.html
[23] vgl. U.S. FTC Operation Spam Zombies, http://www.ftc.gov/bcp/conline/edcams/spam/zombie/
[24] Internet Protocol, spezifiziert in RFC 791
[25] Unter UNIX/Linux handelt es sich um die Datei /etc/hosts, unter Windows um C:\WINDOWS\system32\drivers\etc\hosts.

aus einem Botnet zu schlagen. Meist schließt der Botmaster einen Vertrag mit Werbeunternehmen, die ihm einen bestimmten Betrag für jede angezeigte Werbung bzw. für jeden Klick auf einen Werbe-Banner bezahlen.[26]

Eine der neu entdeckten Möglichkeit der gewinnbringenden Verwendung eines Botnets besteht in der Überlistung von „Pay per click"-Werbediensten wie Google AdSense[27]. Das Geschäftsmodell derartiger Werbedienste stellt sich wie folgt dar: Ein Kunde des Werbedienstes bezahlt für jeden Click (dh für jeden vom Werbedienst ausgehenden Besuch der Kundenwebsite) einen bestimmten Geldbetrag. Die Werbeeinschaltungen erfolgen zu einem großen Teil auf Websites Dritter. Diese erhalten für jeden von ihrer Site ausgehenden Click einen erheblichen Anteil, desjenigen Betrages, den der Kunde an den Betreiber des Werbedienstes für diesen Click bezahlt. Dieses Geschäftsmodell kann dadurch überlistet werden, dass der Dritte auf dessen Website die Werbeeinschaltung erfolgt, ein Botnet dazu benützt Clicks zu generieren. Dadurch bezahlt der Kunde für künstlich generierte Clicks, wobei der Großteil des Entgelts dem Dritten (dh dem Botmaster) zufließt.[28]

4. Strafrechtliche Beurteilung

Im Folgenden sollen Handlungen im Zusammenhang mit Botnets auf ihre Strafbarkeit hin untersucht werden.

4.1. Das Hacking von Systemen zwecks Erstellung eines Botnets

Zunächst stellt sich die Frage wie die Rekrutierung von Systemen für das Botnet zu beurteilen ist. Da sich der Botmaster Zugang zu einem Computersystem verschafft, über das er nicht verfügen darf, kommt § 118a StGB in Betracht. Neben dem nicht immer unproblematischen Erfordernis der Verletzung einer Sicherheitsvorkehrung als Element des objektiven Tatbestandes, ist insbesondere der erweiterte Vorsatz in den meisten Fällen wohl mehr als fraglich. § 118a erfordert einen in kumulativer Weise dreifach erweiterten Vorsatz in Form der Absichtlichkeit: der Täter muss (zum Zeitpunkt der Zugangsverschaffung!) mit Spionageabsicht (Absicht sich oder einem anderen von im Computersystem gespeicherten Daten Kenntnis zu verschaffen), Verwendungsabsicht (Absicht die Daten selbst zu benützen, einem anderen zugänglich zu machen oder zu veröffentlichen) und Gewinn- bzw. Schädigungsabsicht (Absicht sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen) handeln.
Aus der Tatsache, dass ein System für ein Botnet rekrutiert wird, kann keinesfalls eine Spionageabsicht abgeleitet werden. Denn in den meisten Fällen besteht für den Botmaster gar kein – oder nur ein sekundäres – Interesse an den im Zombie gespeicherten Daten. Auf Grund des engen subjektiven Tatbestandes ist es daher nicht nach § 118a StGB strafbar sich zu zigtausenden von Systemen Zugang zu verschaffen um zu einem späteren Zeitpunkt Distributed Denial of Service Attacks auszuführen, „Warez" im Botnet zu hosten, Spam oder Phishing-Mails über das Botnet zu versenden, Pharming zu betreiben[29], Adware auf allen Zombies zu installieren oder einen „Pay per click"-Werbedienst zu überlisten. Dies mag merkwürdig erscheinen, entspricht jedoch der (zu hinterfragenden) Wertung des

---

[26] SANS NewsBites, Volume: 8, Issue: 13, Botnet Suspect Indicted

[27] Im ersten Quartal 2006 generierte AdSense einen Umsatz von $928 Millionen; vgl http://investor.google.com/releases/2006Q1.html

[28] Vgl SANS NewsBites, Volume: 8, Issue: 40, Google Fraud: Botnets Used to Steal Money From Google Advertisers. Von Googles Kunden wurde eine Class Action gegen Google selbst angestrengt; vgl SANS NewsBites, Volume: 8, Issue: 20, Google Settles Fraudulent Clicks Suit. Zum aktuellen Stand des Verfahrens vgl http://www.clickfraud-legal-center.com,
http://www.betanews.com/article/Google_Click_Fraud_Settlement_Hits_Snag/1147446514

[29] Auch bei Pharming besteht grundsätzlich kein Interesse an im System gespeicherten Daten. Ziel des Pharmings ist es Zugang zu Informationen zu erhalten, die gleichsam im Kopf des Opfers gespeichert sind.

Gesetzgebers, dass Hacking nur dann strafbar sein soll, wenn ein Interesse an den im gehackten System gespeicherten Daten besteht.

Es kommt jedoch auch eine Strafbarkeit nach § 126c Abs 1 StGB in Betracht. Nach diesem Vorbereitungsdelikt ist strafbar, wer ein Hackertool (Z 1) oder ein Passwort (Z 2) mit dem Vorsatz herstellt, einführt, vertreibt, veräußert, sonst zugänglich macht, sich verschafft oder besitzt, dass es zur Begehung der §§ 118a, 119, 119a, 126a, 126b od 148a StGB gebraucht wird. Die zur Rekrutierung neuer Zombies erforderliche Software kann problemlos unter das Tatmittel der Z 1 subsumiert werden. Besitzt beispielsweise jemand eine derartige Software mit dem Vorsatz diese zur Erstellung eines Botnets zu verwenden, mit dem ein Distributed Denial of Service Attack (eine schwere Störung der Funktionsfähigkeit eines Computersystems iSd § 126b StGB) ausgeführt werden soll, so bestünde eine Strafbarkeit nach § 126c StGB. Handelt der Täter hingegen nur mit dem Vorsatz das Botnet zum Versenden von Spam oder Phishing-Mails[30] und zur Installation von Adware zu verwenden, so bestünde mangels erweitertem Vorsatz keine Strafbarkeit nach § 126c StGB.

In der Praxis wäre es äußerst schwer einen entsprechenden Vorsatz in Bezug auf § 118a oder § 126c StGB nachzuweisen. Denn die Behauptung sich ausschließlich damit abgefunden zu haben Spams zu versenden und Adware zu installieren wird in den meisten Fällen angesichts der Lukrativität dieser Aktivitäten als glaubhaft zu beurteilen sein.

Das Hacking von Systemen zwecks Erstellung eines Botnets wird daher nur in Ausnahmefällen eine Strafbarkeit begründen.

4.2. Der Handel mit Botnets

In der Praxis hat sich ein reger Handel mit Botnets etabliert. Gegenstand des – jedenfalls sittenwidrigen – Vertrages ist bei zentral organisierten Botnets der Zugang zum IRC-Server und bei dezentralen Botnets uU ein Private Key.

Zunächst ist eine Strafbarkeit des Veräußerers zu untersuchen. Tritt der Erwerber als unmittelbarer Täter ins Versuchsstadium und handelt der Veräußerer mit entsprechendem Vorsatz, so kommt nach allgemeinen Regeln eine Strafbarkeit als Beitragstäter durch sonstigen Beitrag in Betracht.
Darüber hinaus ist eine Strafbarkeit nach § 126c Abs 1 StGB denkbar, da sowohl die Zugangsdaten zum IRC-Server als auch ein für die Authentifizierung dienender Private Key unter das Tatmittel des § 126c Abs 1 Z 2 zu subsumieren sind.[31] Es ergeben sich jedoch wiederum die bereits erörterten Probleme im Bereich des erweiterten Vorsatzes. Wird das Botnet beispielsweise nur mit dem Vorsatz besessen bzw. veräußert, dass es zum Versenden von Spam oder Phishing-Mails und zur Installation von Adware verwendet wird, tritt keine Strafbarkeit nach § 126c Abs 1 ein.

In Bezug auf den Erwerber eines Botnets stellt sich die Frage einer Strafbarkeit nach § 118a StGB. Durch den Erwerb der Zugangsdaten besteht zunächst nur die bloße Möglichkeit sich Zugang zu den Zombies zu verschaffen. Eine Zugangsverschaffung iSd § 118a erfolgt jedoch erst zu jenem Zeitpunkt, in dem der Erwerber die erlangten Zugangsdaten auch tatsächlich verwendet. Wie in vielen Fällen gestaltet sich auch hier die Behandlung des Tatbestandselements der Verletzung einer Sicherheitsvorkehrung im betroffenen Computersystem als problematisch. Die Verwendung des auf sozial-inadäquate Weise erlangten Private Key ist mE als Verletzung einer Sicherheitsvorehrung iSd § 118a zu

[30] Da bei Phishing ein Mensch und keine Maschine „getäuscht" wird, kommt § 148a StGB nicht in Betracht.
[31] vgl *Feiler*, Zur strafrechtlichen Beurteilung von IT-Sicherheitslücken, 7 f

beurteilen.[32] Bei der Verwendung der Zugangsdaten zum IRC-Server stellt sich die Situation insofern anders dar, als dass sich hier die zu verletzende Sicherheitsvorkehrung in Form eines Authentifizierungsmechanismus nicht in den Zombies sondern im IRC-Server befinden, über den der Botmaster idR verfügungsbefugt ist. Sieht man daher jeden einzelnen Zombie als ein Computersystem iSd § 118a, so kommt es zu keiner Verletzung einer in diesen Systemen befindlichen Sicherheitsvorkehrung.[33] Eine Strafbarkeit könnte sich nur durch folgende zwei mE zulässige Sichtweisen ergeben. Zum einen ist es denkbar das gesamte Botnet als ein Computersystem iSd § 74 Abs 1 Z 8 zu sehen. Da auch der IRC-Server als Steuerungselement Teil dieses Computersystems ist, befindet sich nun auch der Authentifizierungsmechanismus „im Computersystem". Da der Botmaster über dieses nicht alleine verfügen darf, würde die Verletzung der im Computersystem befindlichen Sicherheitsvorkehrung den objektiven Tatbestand des § 118a erfüllen. Die zweite Sichtweise besteht darin, das Internet als Computersystem iSd § 74 Abs 1 Z 8 aufzufassen. Diesfalls würde sich der Botmaster zu einem Teil des Computersystems (dem Botnet als Teil des Internets), über das er nicht verfügen darf dadurch Zugang verschaffen, dass er eine im Computersystem (dh im Internet) befindliche Sicherheitsvorkehrung verletzt. Bei dieser Betrachtungsweise ist der objektive Tatbestand des § 118a ebenso erfüllt.
Da bereits das Besitzen (sozial-inadäquat erworbener)[34] Zugangsdaten den objektiven Tatbestand des § 126c Abs 1 erfüllt, kommt auch für den Erwerber grundsätzlich eine Strafbarkeit nach genannter Bestimmung in Betracht.
Im Bereich des subjektiven Tatbestandes der §§ 118a und 126c stellen sich für eine Strafbarkeit des Erwerbers jedoch wiederum die bereits erörterten Probleme.

4.3. Der Einsatz von Botnets

Die hier zu behandelnden Sachverhalte können auch ohne die Zuhilfenahme von Botnets erfolgreich umgesetzt werden und stellen insofern Probleme des allgemeinen Computerstrafrechts dar. Aus diesem Grund werden sie nur in verkürzter Form dargestellt.

Wird ein Botnet für Distributed Denial of Service Attacks eingesetzt so ist in den meisten Fällen wegen der schweren Störung der Funktionsfähigkeit eines Computersystems eine Strafbarkeit nach § 126b StGB gegeben.
Beim Einsatz von Spyware (zB Keylogger und Sniffer) ist an eine Strafbarkeit nach § 119 bzw. § 119a StGB zu denken.
Beim Hosting von „Warez" kommt allenfalls eine Strafbarkeit nach dem UrhG in Betracht.
Das Versenden von Spam verwirklicht regelmäßig den Verwaltungsstraftatbestand des § 107 TKG. Demgegenüber ist das Versenden von Phishing-Mails idR als versuchter Betrug strafbar. Da es beim Pharming idR zu Modifikationen von Systemdateien kommt ist an eine Datenbeschädigung nach § 126a StGB zu denken. Wird jedoch lediglich der hosts-Datei[35] eine neue Zeile angefügt, so ist mangels nennenswertem Wiederherstellungsaufwand das vorliegen einer Schädigung zu verneinen, weshalb eine Strafbarkeit nach § 126a StGB in den meisten derartigen Fällen wohl nicht gegeben ist.
Die Einordung der Installation von Adware gestaltet sich als problematisch. Da idR keine bestehenden Daten beschädigt werden und es auch zu keiner schweren Störung der Funktionsfähigkeit des Computersystems kommt, scheidet eine Strafbarkeit sowohl nach

---

[32] Zur grundsätzlichen Frage der Verletzung einer Sicherheitsvorkehrung durch Verwendung von Authentifizierungsdaten und zum Erfordernis eines sozial-inadäquaten Verhaltens vgl *Feiler*, Zur strafrechtlichen Beurteilung von IT-Sicherheitslücken, 7 ff, 16
[33] Zu einem ganz ähnlich gelagerten Problem iZm Cross Site Scripting (XSS) *Feiler*, Zur strafrechtlichen Beurteilung von IT-Sicherheitslücken, 32 f.
[34] vgl wiederum *Feiler*, Zur strafrechtlichen Beurteilung von IT-Sicherheitslücken, 7 ff, 16
[35] unter UNIX/Linux /etc/hosts; unter Windows C:\WINDOWS\system32\drivers\etc\hosts

§ 126a als auch nach § 126b StGB aus. Da mE Adware als Programme, die automatisch und unaufgefordert Werbefenster öffnen nicht vom äußerst möglichen Wortsinn des Begriffes der „elektronischen Post“ erfasst sind, bleibt auch § 107 TKG unanwendbar.
Bei der Überlistung von „Pay per click”-Werbediensten kommt – abhängig davon ob schlussendlich eine Maschine oder ein Mensch eine Prüfung vornimmt und daher „getäuscht“ werden kann – eine Strafbarkeit nach § 148a bzw § 146 ff in Betracht.

5. Technische Gegenmaßnahmen

Grundsätzlich kann in proaktive und reaktive Maßnahmen unterschieden werden. Um bereits die Entstehung von Botnets zu erschweren, ist es erforderlich das weltweite Sicherheitsniveau von mit dem Internet verbundenen Systemen zu erhöhen. Das Betreiben einer Firewall, das unverzügliche Einspielen von Sicherheitsupdates und das Verwenden von Anti-Viren Software auf jedem der betroffenen Systeme sind hierbei die ersten (!) essentiellen Schritte.
Im Bereich der reaktiven Maßnahmen ist es zunächst nahe liegend zu versuchen, das Botnet außer Gefecht zu setzen. Dies ist bei zentral organisierten Botnets oft durch die gezielte Abschaltung des IRC-Servers möglich. Insbesondere US-Amerikanische und Israelische Behörden bzw. ISPs haben zu diesem Zweck eigene Task Forces eingerichtet.[36] Bei dezentralen Botnets werden sich die Bemühungen dieses abzuschalten auf Grund der höheren Widerstandsfähigkeit weitaus schwieriger gestalten. Um aktuellen Entwicklungen in der kriminellen Szene folgen zu können, ist der Einsatz von Honeypots bzw. Honeynets[37] jedenfalls unverzichtbar geworden.[38]

Für die aus den verschiedenen Einsatzgebieten von Botnets resultierenden Gefahren bestehen unterschiedliche Gegenmaßnahmen. Da Distributed Denial of Service Attacks häufig IP-Spoofing[39] verwenden, um die Rückverfolgbarkeit des Angriffs zu erschweren, besteht ein erster Schritt darin, IP-Spoofing durch Vorkehrungen seitens der ISPs weitgehend zu verhindern.[40]

Im Kampf gegen von Botnets ausgehenden Spam hat die U.S. Federal Trade Commission in Zusammenarbeit mit Regierungsbehörden anderer Staaten folgende fünf Maßnahmen vorgeschlagen:[41]
1) Port 25 sollte mit Ausnahme von authentifiziertem SMTP-Verkehr blockiert werden.[42]
2) Die Mail-Server der ISPs sollten von einem Anschluss aus nur eine beschränkte Anzahl von E-Mails pro Zeiteinheit gestatten.
3) Es sollten Möglichkeiten zur Identifizierung von Spam versendenden Zombies geschaffen werden. Wird ein System als Zombie identifiziert, sollte es unter Quarantäne gestellt werden.
4) Den Kunden sollten leicht verständliche Anweisungen gegeben werden, die es ermöglichen Angriffe durch Würmer, trojanische Pferde oder andere „Malware“ abzuwehren. ISPs sollten entsprechende Werkzeuge und Unterstützung zur Bewältigung des Problems anbieten.

---

[36] SANS NewsBites, Volume: 8, Issue: 19, Group Takes Aim at Botnet Command and Control Servers; *Vaughn/Evron*, Drone Armies C&C Report - 01 Apr 2006
[37] Es handelt sich hierbei um einzelne Rechner bzw. ganze Netzwerke, die bei strenger Überwachung nur dazu betrieben werden, Angreifer bei ihren Handlungen zu beobachten und so ganz nach dem Prinzip „Know your enemy“ von ihnen zu lernen.
[38] vgl *The Honeynet Project & Research Alliance*, Know your Enemy: Tracking Botnets
[39] Das Fälschen der IP-Absenderadresse (vgl RFC 791, 10 ff).
[40] Heise News, Europäische IP-Registry gründet Taskforce gegen Spoofing; RIPE 52 Proposal for a RIPE "IP Spoofing" Task Force; vgl BCP 38/RFC 2827, BCP 46/RFC 3013
[41] U.S. FTC Operation Spam Zombies, http://www.ftc.gov/bcp/conline/edcams/spam/zombie/
[42] Gem RFC 821 verwenden SMTP-Dienste den Port 25; ftp://ftp.rfc-editor.org/in-notes/rfc821.txt.

5) Kunden sollte die Möglichkeit gegeben werden, durch die Verwendung leicht verständlicher Werkzeuge ihr System zu desinfizieren. Soweit erforderlich, sollten ISPs hierbei wiederum Unterstützung anbieten.

Insbesondere die erste der genannten Maßnahmen erscheint zwar drastisch, angesichts der nicht enden wollenden Spam-Flut jedoch erforderlich.

6. Zusammenfassung

Botnets sind insbesondere in ihrer zukünftigen Form als dezentrale, aktualisierbare Botnet-Würmer eine der gefährlichsten Waffen im Bereich der Informationstechnologie. Auf Grund der dezentralen Natur des Internets zeigen technische Gegenmaßnahmen nur langsam Wirkung. Botnets verdeutlichen, dass Hacking – entgegen der Wertung des österreichischen Gesetzgebers – kein Kavaliersdelikt ist. Der erweiterte Vorsatz des § 118a StGB schränkt die Strafbarkeit des Hackings derart ein, dass Botmaster/Hacker, deren Vorsatz sich auf das Versenden von Spam oder die Installation von Adware beschänkt, keine strafbaren Handlungen setzen.

Die ersten Akte des Cyber-Terrorismus könnten darin bestehen sich Botnets zu nutze zu machen, um die Funktionsfähigkeit des gesamten Internets erheblich zu stören. So wäre ein Botnet bestehend aus 100.000 Zombies wohl dazu geeignet einen Distributed Denial of Service Attack gegen die dreizehn Root Name Server[43] durchzuführen, was innerhalb weniger Stunden zu einem gänzlichen Ausfall des Internets führen würde.

[43] vgl. http://www.root-servers.org

7. Quellen
Alle URLs beziehen sich auf den 26. Mai 2006.

BCP 38/RFC 2827: Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing
ftp://ftp.rfc-editor.org/in-notes/rfc2827.txt

BCP 46/RFC 3013: Recommended Internet Service Provider Security Services and Procedures
ftp://ftp.rfc-editor.org/in-notes/rfc3013.txt

Feiler, Zur strafrechtlichen Beurteilung von IT-Sicherheitslücken, 2006,
http://www.lukasfeiler.com/Zur_strafrechtlichen_Beurteilung_von_IT-Sicherheitsluecken.pdf

Fendley, As the Bot Turns, SANS Internet Storm Center, 30. April 2006
http://isc.sans.org/diary.php?storyid=1300

Geer, Malicious Bots Threaten Network Security, IEEE Computer, Vol. 38, no. 1, S. 18, Jänner 2005, http://csdl2.computer.org/comp/mags/co/2005/01/r1018.pdf

Heise News, Europäische IP-Registry gründet Taskforce gegen Spoofing, 27. April 2006
http://www.heise.de/newsticker/result.xhtml?url=/newsticker/meldung/72435&words=RIPE

Houle/Weaver, Trends in Denial of Service Attack Technology, CERT Coordination Center, Oktober 2001, http://www.cert.org/archive/pdf/DoS_trends.pdf

Jones, BotNets: Detection and Mitigation, FedCIRC, Februar 2003
http://web.archive.org/web/20040801041759/http://www.fedcirc.gov/library/documents/botNetsv32.doc

Kalt, RFC 2810, Internet Relay Chat: Architecture, RFC 2810, April 2000,
http://www.faqs.org/rfcs/rfc2810.html

Kawamoto, Bots slim down to get tough, CNET News.com, 16. November 2005,
http://news.com.com/Bots+slim+down+to+get+tough/2100-7355_3-5956143.html

Li/Ehrenkranz/Kuenning/Reiher, Simulation and Analysis on the Resiliency and Efficiency of Malnets, 2005, http://www.cs.hmc.edu/~geoff/ieee_smmsm_2005.pdf

Lipson, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues, CERT Coordination Center, November 2002, http://www.cert.org/archive/pdf/02sr009.pdf

Microsoft PressPass, Stopping Zombies Before They Attack: Microsoft Teams with Federal Trade Commission and Consumer Action to Promote PC Protection, 27. Oktober 2005
http://www.microsoft.com/presspass/features/2005/oct05/10-27Zombie.mspx

Naraine, Hunt Intensifies for Botnet Command & Controls, 2. März 2006,
http://www.eweek.com/article2/0,1895,1933210,00.asp

Puppe/Maier, Von allen Seiten, Maßnahmen gegen Distributed-Denial-of-Service-Angriffe, iX 4/2005, S. 107

Puri, Bots & Botnet: An Overview, SANS GSEC Practical v.1.4b, 2003
http://www.sans.org/rr/whitepapers/malicious/1299.php

Reiher/Li/Kuenning, Midgard Worms: Sudden Nasty Surprises from a Large Resilient Zombie Army, http://www.cs.uoregon.edu/~lijun/pubs/CSD-TR040019.pdf

RIPE, RIPE 52 Proposal for a RIPE "IP Spoofing" Task Force
http://www.ripe.net/ripe/meetings/ripe-52/agendas/ip-spoofing-bof.html

SANS NewsBites, Volume: 8, Issue: 33, Bot Crimes on the Rise, 23. April 2006,
http://www.sans.org/newsletters/newsbites/newsbites.php?vol=8&issue=33&rss=Y#200

SANS NewsBites, Volume: 7, Issue: 55, Botnets Get Lean to Avoid Detection, 16. November 2005, http://www.sans.org/newsletters/newsbites/newsbites.php?vol=7&issue=55#312

SANS NewsBites, Volume: 8, Issue: 40, Google Fraud: Botnets Used to Steal Money From Google Advertisers, 15. Mai 2006,
http://www.sans.org/newsletters/newsbites/newsbites.php?vol=8&issue=40#200

SANS NewsBites, Volume: 8, Issue: 37, Botmaster Sentenced To Nearly 5 Years In Prison, 8. Mai 2006
http://www.sans.org/newsletters/newsbites/newsbites.php?vol=8&issue=37#310

SANS NewsBites, Volume: 8, Issue: 13, Botnet Suspect Indicted, 13. Februar 2006,
http://www.sans.org/newsletters/newsbites/newsbites.php?vol=8&issue=13#301

SANS NewsBites, Volume: 8, Issue: 20, Google Settles Fraudulent Clicks Suit, 9. März 2006,
http://www.sans.org/newsletters/newsbites/newsbites.php?vol=8&issue=20#311

SANS NewsBites, Volume: 8, Issue: 19, Group Takes Aim at Botnet Command and Control Servers, 2. März 2006
http://www.sans.org/newsletters/newsbites/newsbites.php?vol=8&issue=19#312

Smith, Microsoft attacks Zombie Masters, SANS Internet Storm Center, 30. Oktober 2005,
http://isc.sans.org/diary.php?storyid=800

Spamhaus.org, What is a "honeypot" or "proxypot"? What is a "proxy hijack source" or "C&C"?
http://www.spamhaus.org/faq/answers.lasso?section=ISP%20Spam%20Issues#143

Staniford/Paxson/Weaver, How to 0wn the Internet in your spare time, in Proceedings of the 11th USENIX Security Symposium (Security '02), 2002,
http://www.usenix.org/events/sec02/full_papers/staniford/staniford.pdf

The Honeynet Project & Research Alliance, Know your Enemy: Tracking Botnets, 13. März 2005, http://www.honeynet.org/papers/bots/

The Honeynet Project, Know your Enemy: Tracking Botnets – Spreading,
http://www.honeynet.org/papers/bots/botnet-spreading.html

US-CERT, Cyber Security Tip ST06-001, Understanding Hidden Threats: Rootkits and Botnets, http://www.us-cert.gov/cas/tips/ST06-001.html

U.S. DOJ, Background On Operation Web Snare – Examples Of Prosecutions, United States v. Jay R. Echouafni et al. (Operation Cyberslam)
http://www.usdoj.gov/criminal/fraud/websnare.pdf

U.S. FBI, The Case of the "Zombie King" - Hacker Sentenced for Hijacking Computers for Profit, http://www.fbi.gov/page2/may06/botnet050806.htm

U.S. FTC, Operation Spam Zombies,
http://www.ftc.gov/bcp/conline/edcams/spam/zombie/

Vamosi, Pirated movies now playing on a server near you, CNET Software, 5. August 2002,
http://reviews.cnet.com/4520-3513_7-5021079-1.html

Vaughn/Evron, Drone Armies C&C Report - 01 Apr 2006
http://www.merit.edu/mail.archives/nanog/2006-04/msg00009.html