Pro-Seminar Spam

Seminararbeit

Erkennung von Botnetzen

Institut für Informatik
Universität Potsdam

eingereicht von:
Michael Winkelmann (738901)

Wintersemester 2009/2010

Inhaltsverzeichnis

1 Einführung

Spam sind auf elektronischem Wege vom Empfänger unverlangt zugestellte und nicht gewollte Nachrichten. Meist haben diese Nachrichten lediglich Werbung zum Inhalt, seltener befinden sich aber auch Viren im Anhang. Laut einer von Google in Auftrag gegebenen Studie sind mehr als 94% aller E-Mail-Nachrichten sind unerwünscht (Wat09). Botnetze sind dabei die häufigste Variante, Spam zu verschicken. (Kam08)

Botnetze sind grundlegend betrachtet nichts weiter als eine Gruppe von Bots, die auf vernetzten Rechnern laufen, miteinander kommunizieren und ferngesteuert werden können. Bots sind kleine, meist vollständig selbständig arbeitende Computerprogramme, die sich wiederholende Aufgaben abarbeiten. Man unterscheidet zwischen gutartigen und bösartigen Bots. Gutartige Bots sind beispielsweise Webcrawler von Internet-Suchmaschinen. Bösartige Bots sind sammeln E-Mail-Adressen für Spamzwecke oder spionieren nach Sicherheitslücken, um so Server zu cracken. Kommunizieren mehrere solcher bösartigen Bots untereinander über mehrere Rechner verteilt, so handelt es sich um ein Botnetz. Durch einen Angreifer werden zahlreiche einem Bot infiziert, der sich mit einem IRC-Server verbindet, einen festgelegten Channel betritt und Befehle vom Botnetz-Besitzer entgegennehmen kann. Die meisten Botnetze können von einem Server aus durch einen Botnetz-Operator gesteuert und überwacht werden. Man spricht hier von einem „Command-and-Concrol-Server“, kurz *„CC“*.

Um das Botnetz zu erweitern, müssen die Bots verbreitet und auf möglichst vielen Rechnern installiert werden. Die Verbreitung der Bots, auch als Spreading bezeichnet, kann über verschiedene Wege erfolgen. Zum Beispiel kann der Bot sich als Anhang in einer E-Mail befinden. Der Benutzer wird in einer E-Mail dazu aufgefordert, diesen zu öffnen. Immer häufiger befindet sich jedoch ein Link in der E-Mail, der auf eine infizierte Webseite verweist und durch Anklicken den Rechner infiziert. Ein anderer Verbreitungsweg findet über Downloads statt, die der Benutzer freiwillig herunterlädt und ausführt. Dabei sind die Bots meist Trojaner, die zum Beispiel als Cracks oder Warez getarnt sind. Die Verbreitung von Bots kann auch über Software-Fehler im Betriebssystem, im Browser oder in einer Anwendung auf dem Computer erfolgen. Bots, die sich auf diesem Wege verbreiten, verfügen meist über eine Funktion zur automatischen Weiterverbreitung.

Botnetze sind für die Internet-Kriminalität eine bedeutungsvolle Plattform, weshalb bei diesen Netzwerken derzeit eine starke Expansion zu beobachten ist. Derzeit ist jeder zehnte PC Teil eines Botnetzes (Kam08), wodurch sie eine der größten illegalen Einnahmequellen im Internet darstellen.

Botnetze können für verschiedene Zwecke eingesetzt werden. Dazu zählt zum Beispiel die Verwendung als Proxy. Dabei wird eine Verbindung zu einem dritten Computer über einen infizierten PC hergestellt und die Ursprungsadresse bleibt dabei verborgen. Der Zwischenhost kann so für weitere Angriff auch weitere Rechner missbraucht werden, denn aus sich des Zielcomputers kommt der Angriff vom Proxy. Anderes Beispiel für einen Verwendungszweck sind DDos-Attacken. Wenn solche eine Attacke mit allen sich im Netzwerk befindlichen Bots mit der entsprechenden zur Verfügung stehenden Bandbreite durchgeführt wird, so können mit großer Wahrscheinlichkeit die Netzwerk-Dienste auf dem Zielrechner außer Betrieb gesamte oder dessen gesamte Bandbreite an die infizierten Rechner verbraucht werden.

Am häufigsten werden Botnetze jedoch für die Verbreitung von Spam-Mails eingesetzt. Laut einer Studie sind Botnetze sind für mehr als 80% der versendeten Spam-Mails verantwortlich (Kam08). Spammer erwerben dabei, sofern sie nicht selbst ein Botnetz besitzen, den Zugriff auf das Botnetz entweder beim Programmierer oder bei speziellen Händlern oder mieten ihn für eine bestimmte Zeit. Der Spammer bekommt dann auch Zugriff auf den Botnetz-Operator, mit dem er dem Botnet gezielt Instruktionen geben kann, um so Spam zu versenden. Der Preis für Spam schwankt je nach Zielgruppe und der Anzahl der Adressen, an die die Nachrichten gesendet werden. Die Preise liegen meist im Bereich von 70 Dollar für hunderttausende Adressen und 1000 Dollar für mehrere Dutzend Millionen

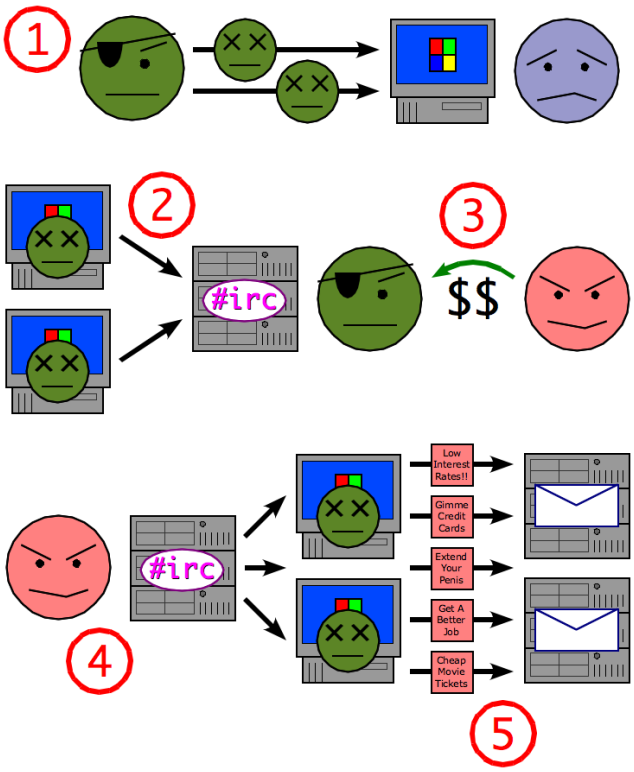

Abbildung 1: Funktionsweise von Botnetzen. (1) Angreifer versendet Bots, die zahlreiche PCs infizieren. (2) Infizierter PC loggt sich bei einem IRC-Server ein, um so ein Netzwerk mit anderen infizierten Systemen zu bilden. (3) Spammer erwirbt Zugriff auf das Botnet. (4) Spammer gibt dem Botnetz die Instruktion, dass infizierte PCs Spam versenden sollen. (5) Infizierter PC versendet Spamnachrichten zu den Mailservern der Internetbenutzer. *Bildquelle:* (Wik06)

Adressen. Im Jahr 2008 verdienten Spammer mit der Versendung von unerwünschten Mitteilungen eine Summe von ca. 780 Millionen Dollar (Kam08). Botnetze arbeiten stets im Verborgenen und sind nur schwer zu identifizieren und zu bekämpfen. Daher sind sie für Spam ideal geeignet, da die Nachrichten anonym und verteilt versendet werden können. Um Spam zu verhindern, ist es jedoch extrem hilfreich, diese Botnetze zu identifizieren und infizierte Computer von den Bots zu befreien.

Jedoch geben die Spammer durch das Verschicken von Nachrichten im Gegenzug auch viele ungewollte Informationen über sich preis, die für das Erkennen eines Botnetzes genutzt werden können. Die vorliegende Arbeit widmet sich diesem Thema. Als erstes werde ich versuchen, die Merkmale, die Botnetz-Spam typischerweise aufweist, zusammenzufassen und zu beschreiben. Danach werde ich das System AutoRE beschreiben, welches in der Lage ist, versendete Spam-Mails zu erkennen und Spam-Kampagnen zuzuordnen. Die Einteilung in Spam-Kampagnen und weitere daraus gewonnene Informationen können dann dafür benutzt werden, Botnetze zu identifizieren und ihr Verhalten zu beobachten. Abschließend werde ich die Ergebnisse und Beobachtungen dieser beiden Arbeiten zusammenfassen, diskutieren und zum Schluss noch einen kurzen Ausblick auf eventuelle Verbesserungsmöglichkeiten geben. Als Hauptquellen verwende ich die beiden Arbeiten „Characterizing Botnets from Email Spam Records“(ZDSW08) und „Spamming Botnets: Signatures and Characteristics“(XYA+08). Anzumerken ist, dass beide Arbeiten lediglich einen relativ kleinen Testdatensatz an Spam-Mails verwenden. Auch die Beobachtungszeiträume sind sehr begrenzt. In (ZDSW08) wurden die Botnetze innerhalb einer Zeitspanne von neun Tagen beobachtet, in (XYA+08) stammten die Testmails aus den Monaten November 2006, Juni 2007 und Juli 2007. Dadurch besitzen die Ergebnisse und Beobachtungen eine verringerte Genauigkeit.

Time	URLs	Source ASes	URLs
2006-11-02	66	38	http://www.lympos.com/n/?167&carthagebolets http://www.lympos.com/n/?167&brokenacclaim http://www.lympos.com/n/?167&acceptoraudience
2006-11-15	72	39	http://shgeep.info/tota/indexx.html?jhjb.cvqxjby,hvx http://shgeep.info/tota/indexx.html?ikjija.cvqxjby,hvx http://shgeep.info/tota/indexx.html?ivvx_ceh.cvqxjby,hvx

Abbildung 2: Zwei Beispiele für polymorphe URLs. *Bildquelle:* (XYA+08)

2 Merkmale von Spam-Mails aus Botnetzen

Spam aus Botnetzen unterscheidet sich in mehreren Punkten von anderen Spam-Mails. Die Betrachtung dieser speziellen Merkmale erlaubt eine einfachere Klassifizierung der Mails, die später für das Erkennen von Botnetzen benötigt wird. Für die Betrachtung der Merkmale wurden bisher umfangreiche Studien durchgeführt.

(ZDSW08) zeigten, dass die Ähnlichkeit der E-Mailtexte helfen kann, eine Botnet-basierte Spamkampagne zu identifizieren. Eine andere Studie (XYA+08) untersuchte verschiedene Inhaltsmerkmale der Spam-E-Mailtexte, darunter URL-Links. Dabei wurde herausgefunden, dass Spam-E-Mails, deren URL identisch sind, zu einem Cluster gruppiert werden können und oft auf einen Schlag versendet werden. Für spätere Betrachtungen ist dies von entscheidender Wichtigkeit. Spammer benutzen zufällige, von seriösen Webseiten stammende URLs, um die Spam-Mail für den Leser glaubwürdiger zu machen und die Wahrscheinlichkeit, dass sie durch einen Spam-Filter positiv markiert wird, zu verringern. Außerdem enthalten die Spam-Mails von Standard-Software generierte URLs.

Dadurch, dass die Spam-Mails sowohl Links auf seriöse als auch unseriöse Webseiten enthalten, kann man den Spam-Traffic nicht einfach in die Kategorien „seriös“und „verdächtig“vorklassifizieren. In der Lösung von (XYA+08) wird sowohl der Inhalt als auch der Adressraum betrachtet. Allerdings werden hier vordefinierte Listen benutzt, um die Zahl der False-Positives zu reduzieren. Diese Listen enthalten beispielsweise allgemeine Protocol-Header oder Peer-to-Peer-Adressen. Jedoch können Spammer diese Listen einfach umgehen und legale Webseiten missbrauchen. Statt die Spam-Mails zu vorklassifizieren, wird in AutoRE ein iterativer Ansatz angewendet.

Die URLs in einer Spam-Mail werden zusätzlich durch verschiedene Techniken verschleiert, um eine positive Erkennung durch den Spamfilter zu verhindern. Außerdem können entsprechend vom Spammer angepasste URLs Rückschlüsse auf den Benutzer geben, der sie angeklickt hat. Solche URLs werden als polymorphe URLs bezeichnet. Die Anzahl der polymorphen URLs hat sich der letzten Zeit signifikant erhöht. Ein Beispiel für solche URLs befindet sich in Abbildung 2.

Ein Problem ergibt sich jedoch für den Spammer bei der Auswahl von seriösen URLs. Eine bekannte URL würde von aktuellen Spam-Filtern als eine „Hintergrundrauschen“wahrgenommen und somit ignoriert werden. Bei einer Verwendung einer nahezu unbekannten URL hingegen würde dies Rückschlüsse auf das Botnetz zu lassen.

Weitere Betrachtungsmerkmale sind der IP-Adressraum und der Zeitpunkt des Versendens. Botnetz-Spam einer Spamkampagne wird dabei zum einen synchronisiert, d.h. in einem sehr engen Zeitfenster versendet. Dabei lässt sich feststellen, dass diese Mails in meist in einem bestimmten Rhythmus versendet verwendet und dass sich ihr Inhalt im Laufe der Zeit verändert. Mit Hilfe des Senderhythmus kann man die versendeten Mails Spamkampagnen zuordnen und so bereits eine erste Gruppierung vornehmen. In Abbildung 3 kann man erkennen, dass 50% aller Spam-Kampagnen bereits nach 12 Stunden beendet sind, wogegen 20% länger als acht Tage andauern. Das Erkennen von Spam-Kampagnen wird in Abschnitt 3 näher beschrieben.

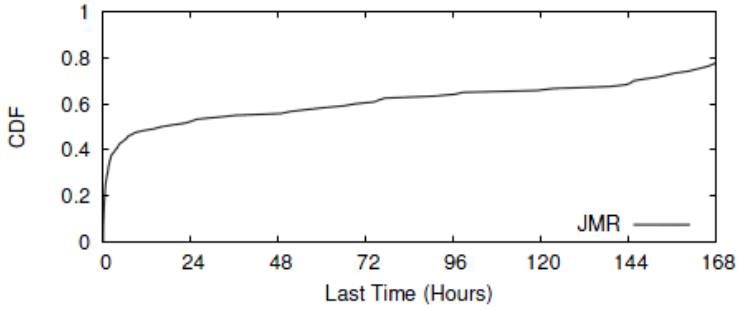

Abbildung 3: Anhand der kumulativen Verteilungsfunktion kann man erkennen, dass die 50% aller Spam-Kampagnen bereits nach 12 Stunden beendet sind, wogegen 20% länger als acht Tage andauern. *Bildquelle:* (ZDSW08)

Month	Nov 2006			June 2007		
	CU	RE	Total	CU	RE	Total
# of spam emails	2	3	5	6,751	43,778	50529
# of non-spam emails	10	0	10	154	561	715

Abbildung 4: Mit den Daten vom November 2006 konnte nur eine verschwindend geringe Zahl an Spam-Mails von Juli 2007 klassifiziert werden, erst mit den Daten vom Vormonat wurden zufriedenstellende Ergebnisse erzielt. Dies zeigt, dass sich der Inhalt der Spam-Nachrichten im Laufe der Zeit ändert. *Bildquelle:* (XYA+08)

Der IP-Adressraum ist fast immer über mehrere Ländergrenzen hinweg verteilt. Die Anzahl der IP-Adressen lässt dabei auch Rückschlüsse auf die Größe des Botnetzes zu. Ein Problem bei der Analyse des IP-Adressraums sind dynamische IP-Adressen. Dabei wird in einem bestimmten Zeitinterval immer eine neue IP-Adresse generiert. Dadurch kann der tatsächliche Urheber von Spam-Mails verschleiert werden. Jedoch lassen sich auch dynamische IP-Adressen identifizieren und so Rückschlüsse auf den Urheber der Spam-Mails zu. Wie dies genau geschieht, wird in (XYA+07) erläutert.

Außerdem verändert sich der Inhalt der Nachrichten mit der Zeit. Daher müssen die Trainingsdaten des Spam-Filters ständig aktuell gehalten werden. In Abbildung 4 zeigt die Ergebnisse eines Versuchs, Spam-Mails im Juli 2007 anhand der Daten vom November 2006 bzw. Juni 2007 zu klassifizieren. Im November 2006 wurden deutlich weniger Mails erkannt, weil der Zeitraum weiter zurücklag. Dies zeigt, dass sich der Inhalt der Spam-Nachrichten im Laufe der Zeit ändert.

Die beschriebenen Merkmale können nun bei der Erkennung von Botnetzen in Betracht gezogen werden.

3 Erkennung von Botnetzen anhand von Spamkampagnen

Botnetze können auf zwei verschiedene Arten erkannt werden. Die erste Variante sammelt Daten aus dem Botnetz durch IRC-Channel-Infiltration oder Traffic-Umleitung von „innen“. Bei der zweiten werden die Botnetze anhand von außen verfolgt, in dem man die von ihnen hinterlassenen Spuren beobachtet. Das Erkennen anhand von E-Mail-Spam fällt in die zweite Kategorie. Der Vorteil bei der Erkennung anhand von Spamkampagnen besteht darin, dass die Quelldaten, sprich die Spam-Mails, sehr leicht zu bekommen und verhältnismäßig leicht zu untersuchen sind.

Als Beispiel für ein System, welches Botnetze zuverlässig erkennt, soll das AutoRE-Framework beschrieben werden.

3.1 Signatur-basierte Botnet-Identifikation

AutoRE generiert Signaturen aus den in Abschnitt 2 beschrieben Merkmalen von Botnet-Spam. Dabei verwendet es als Eingabedaten lediglich eine Menge von E-Mails, die nicht als Spam/Nicht-Spam markiert sind. AutoRE arbeitet also komplett automatisch. Aus diesen Eingabedaten werden zwei Arten von Ausgaben produziert: Eine Menge von URL-Signaturen und eine damit verbundene Liste von IP-Adressen der Botnetz-Hosts. Dabei erkennt AutoRE auch die Zeitintervalle als auch die IP-Adressräume in denen Spam versendet wird.

Die Signaturen können entweder als eine komplette Zeichenkette der URL oder als generalisierter regulärer Ausdruck dargestellt werden. Aus diesen Signaturen können dann sowohl aktuelle als zukünftige Spam-Mails identifiziert werden. Reguläre Ausdrücke bieten den Vorteil, dass man aus ihnen ähnliche (Spam-)URLs leicht ableiten kann und so eine bessere Identifizierung von Botnetz-Spam, der polymorphe URLs verwendet, möglich wird. Dadurch, dass zusätzlich auch die IP-Adressen der Hosts bekannt sind, können Spam-Mails, die einen unterschiedlichen Inhalt, aber die gleiche IP-Adresse besitzen, zuverlässiger ausgefiltert werden.

Das AutoRE-Framework besteht aus 3 Teilen:

- Dem URL-Preprocessor
- Dem Group-Selector
- Und dem Generator für reguläre Ausdrücke

Der URL-Preprocessor extrahiert URLs und andere relevante Daten aus den E-Mails und gruppiert diese nach Webdomains. Jede URL-Gruppe wird dann als ein potentieller Kandidat für die Identifizierung von Spam-Mails betrachtet. Der Group-Selector wählt diese Gruppen nach dem Kriterium der Größe des Zeitfensters aus. Je kleiner das Zeitfenster, desto höher die Wahrscheinlichkeit, dass es sich um eine Spam-Kampagne handelt. Ist eine Gruppe mit großer Wahrscheinlichkeit eine Spam-Kampagne, so übergibt der Group-Selector diese dem Generator für reguläre Ausdrücke.

Ein Flussdiagramm über die Funktionsweise von AutoRE ist in Abbildung 5 dargestellt.

3.2 URL-Preprocessing und URL-Gruppierung

Beim URL-Preprocessing werden die folgenden Informationen aus der E-Mail selektiert: URL-String, die IP-Adresse des Quellservers und der Zeitpunkt des Verschickens. Außerdem erhält jede E-Mail eine eindeutige ID. Dann werden die extrahierten URLs entsprechend der in der URL enthaltenen Webdomain gruppiert. Die Gruppierung nach Webdomains ist deshalb sinnvoll, weil die E-Mails einer Spam-Kampagne meist für das gleiche Produkt werben und daher meist auch die gleichen Seiten verweisen. So wird auch der Aufwand für das Finden von Signaturen stark reduziert.

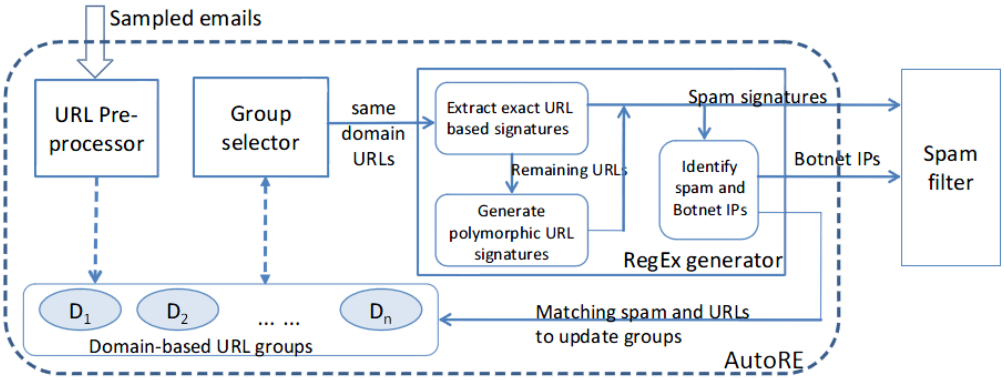

Abbildung 5: Flussdiagramm von AutoRE. *Bildquelle:* (XYA+08)

Nach dem Preprocessing ist möglich, dass die eine Mail, deren URLs auf verschiedene Webdomains verweisen, dann meist auch zu mehreren Gruppen gehört. Jedoch kann eine Spam-Mail logischerweise auch nur zu einer Spam-Kampagne gehören. Man muss also herausfinden, welche hinter welcher dieser Gruppen sich tatsächlich eine Spam-Kampagne verbirgt. Als Kriterium verwendet AutoRE dabei das Zeitfenster, in dem die Mails der Gruppe versendet wurden. Dabei wird iterativ vorgegangen. Mit jeder Iteration wählt der Group-Selector die URL-Gruppe mit der stärksten zeitlichen Korrelation zwischen der Menge an verteilten Absendern aus. Das heißt, wenn eine große Anzahl an IP-Adressen in innerhalb eines kleinen Zeitintervalls eine Spam-Mail versendet, handelt es sich hierbei mit großer Wahrscheinlichkeit um eine Spam-Kampagne.

3.3 Signatur-Generierung

Der Generator für die regulären Ausdrücke gibt für eine Menge von URLs mit der gleichen Domain zwei Arten von Signaturen zurück: vollständig-URL-basierte Signaturen und Signaturen basierend auf regulären Ausdrücken. Erstere erkennen nur die Spam-E-Mails, die einen identischen URL-String enthalten. Letztere sind weitaus flexibler, denn sie stellen eine Verallgemeinerung des gegebenen URL-Strings dar und können so auch polymorphe URLs mit einer niedrigen Rate an False-Positives erkennen. Die Rate an False-Positives kann so um das 30-fache reduziert werden. Beide Signaturen besitzen drei Kriterien, die beim Ableiten einer Signatur berücksichtigt werden müssen: Die Verteilung im IP-Adressraum, die Größe des Zeitfensters und vor allem im bei auf regulären Ausdrücken basierenden Signaturen von Bedeutung: die Wahrscheinlichkeit, mit der ein URL-String zu einer gegebenen Signatur passt. Die Größe des Zeitfensters liegt dabei bei unter 5 Tagen. Das bedeutet, dass eine Gruppe von Mails mit übereinstimmenden URLs innerhalb von 5 Tage versendet sein sollte. Die Signaturen der stark übereinstimmenden Spam-Mails beschreiben somit die Eigenschaften, die Botnetz-Spam kennzeichnen und geben so auch Aufschluss über die Beschaffenheit des Botnetzes.

3.4 Automatische URL-Generierung anhand regulärer Ausdrücke

Für die automatische URL-Generierung mittels regulärer Ausdrücke wird als Eingabe eine Menge von polymorphen URLs, die auf die gleiche Webdomain verweisen, benötigt. Für die Generierung der Signatur wird hier ein Schlüsselwort-basierter Signaturbaum erstellt, der Kandidaten für infrage kommende reguläre Ausdrücke bereitstellt. Zuerst wird dabei eine Menge von Substrings (mit mindestens zwei Zeichen) aus den Kandidaten erstellt. Jeder Substring ist dabei ein Knoten im Baum. Die Wurzel des Baumes der String der Webdomain. Solch ein Baum kann dabei auch für eine polymorphe URL mehrere URLs generieren.

Diese Kandidaten werden dann danach bewertet, ob sie spezifisch genug sind. Dafür muss beantwortet werden, welche Kombination von häufig auftretenden Substrings tatsächlich eine Signatur bilden. Dabei mit am häufigsten auftretenden Substring begonnen, der sowohl in einem engen Zeitintervall als auch über viele IP-Adressen hinweg verteilt auftritt. Danach wird die Signatur inkrementell erweitert, wodurch sie immer spezifischer wird. Für jeden Substring werden so alle möglichen Substrings abgeleitet und deren Häufigkeit abgeschätzt. Auf die genaue algorithmische Betrachtung des Findens der Substrings und der Konstruktion des Signaturbaums wird nicht näher eingegangen. Es sei an dieser Stelle auf das Paper (AKO04) verwiesen. Ein Beispiel für einen Signaturbaum ist in Abbildung 6 dargestellt.

Abschließend werden aus den Schlüsselwort-basierten Signaturen durch *Generalisierung* und *Verfeinerung* reguläre Ausdrücke abgeleitet. Bei der Verfeinerung werden die Signaturen anhand der Anordnung, Länge und Zeichen der Schlüsselwörter unterteilt. Dieser Schritt ist wichtig, um die Qualität der URL-Signaturen zu erhöhen und False-Positive-Rate gering zu halten. Hingegen wird bei der Generalisierung versucht, sich ähnelnde Signaturen wieder zusammenzufassen. Dadurch wird der benötigte Rechenaufwand bei der Erkennung von Botnetz-Spam verringert.

3.5 Bewertung der Signaturenqualität

Durch die Generalisierung kann es passieren, dass Signaturen entstehen, die nicht spezifisch genug sind. Solche Signaturen besitzen dann eine niedrige Qualität. Um die Qualität abzuschätzen, muss die Wahrscheinlichkeit, dass eine zufällig gewählte Zeichenkette zur einer Signatur passt, quantitiv ausgedrückt werden können. Dafür wird die Metrik der *Entropie-Reduzierung* verwendet. Der Ansatz stammt aus der Informationstheorie.

Gegeben seien ein regulärer Ausdruck e und $B_e(u)$ sowie $B(u)$ für die erwartete Anzahl an Bits, die zur Kodierung einer zufälligen Zeichenkette mit bzw. ohne Signatur notwendig sind. Die Entropie-Reduzierung ist definiert als Differenz dieser beiden Bitanzahlen $d(e) = B(u) - B_e(u)$ und bezieht sich auf die Wahrscheinlichkeit $P(e)$, dass eine beliebige Zeichenkette mit der erwarteten Länge durch einen regulären Ausdruck e dargestellt werden kann, der reguläre Ausdruck e aber nicht mit der Zeichenkette identisch sein darf. Diese Wahrscheinlichkeit lässt sich folgendermaßen definieren:

$$P(e) = \frac{2^{B_e(u)}}{2^{B(u)}} = \frac{1}{2^{B(u)-B_e(u)}} = \frac{1}{2^{d(e)}}$$

Die Entropie-Reduzierung $d(e)$ eines regulären Ausdrucks e hängt von der Größe des Zeichensatzes und der erwarteten Länge der Zeichenkette ab. Deshalb benötigt eine spezifische Signatur zur Kodierung weniger Bits und $d(e)$ wird somit größer.

Dadurch ist es möglich, Signaturen, deren Entropie-Reduzierung einen vorher festgelegten Schwellwert überschreitet (im AutoRE beträgt dieser 90) und somit zu allgemein gehalten sind, zu verwerfen und eine hohe Signaturqualität zu gewährleisten.

3.6 Identifizierung der Botnetze

Mit der Signatur-Generierung ist es möglich, die Spam-Kampagnen zu erkennen und zu klassifizieren. Nun soll mit deren Hilfe das Botnetz selbst identifiziert werden. Das AutoRE-Framework konnte dabei 7.721 Botnetz-basierte Spamkampagnen identifizieren mit einer Reichweite von 340.050 IP-Adressen und 5.916 Autonomen Systemen (ASes). Autonome Systeme sind grob betrachtet Blöcke von IP-Adressen, die meist einem Internet-Provider oder einem größeren Unternehmen zugeordnet sind. Als Testgrundlage für die Identifizierung diente dabei ein Datensatz von 5.382.460 im November

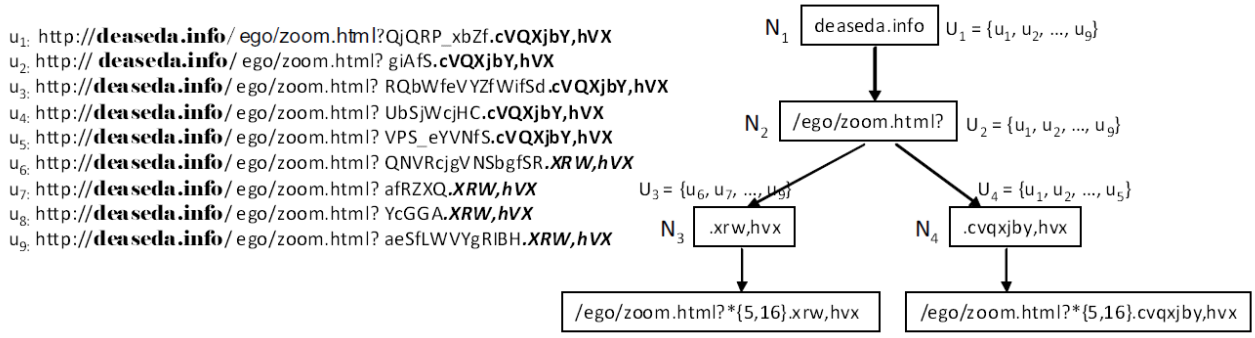

Abbildung 6: Links sind die eingebenen URLs und rechts ist der daraus konstruierte Signaturbaum zu sehen. *Bildquelle:* (XYA+08)

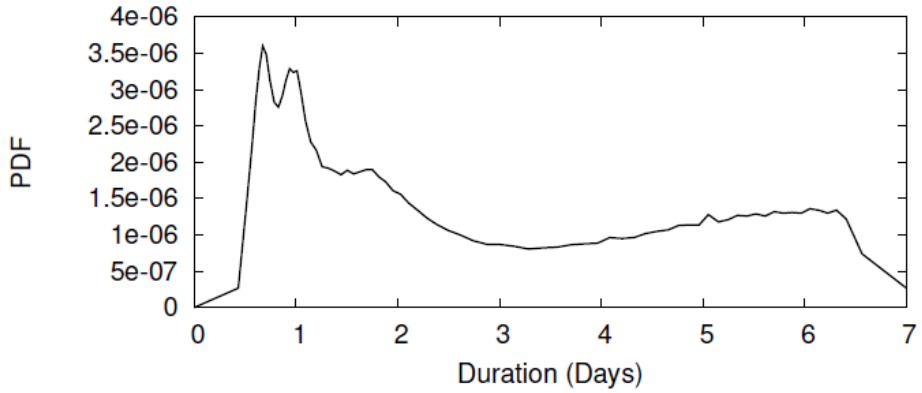

Abbildung 7: Die Wahrscheinlichkeitverteilung für den Wechsel der IP-Adresse. Die meisten IP-Adressen ändern sich jeden Tag. *Bildquelle:* (ZDSW08)

2006, Juni 2007 und Juli 2007 gesammelten Mails (Sampling-Rate 1:25000). Die Rate der False-Positives liegt bei unter 0.002. Zu beachten ist, dass das AutoRE-System nicht in Echtzeit arbeitet und die Sampling-Rate sehr niedrig ist.

Mit der Spam-Kampagne gibt ein Botnetz wie bereits gesehen viele Informationen über sich preis: IP-Adressen, Sendezeitpunkte und URLs.

Jede Spamkampagne wird als eine Sequenz von Ereignissen repräsentiert und Ereignis stellt eine Spam-Mail dar, die zur Spam-Kampagne gehört. Ein nicht-triviales und wichtiges Problem für Identifikation ist die Beantwortung der Frage, ob zwei Spam-Kampagnen zu einem gemeinsamen Botnetz gehören. Um sie zu beantworten, betrachtet man die versendeten Nachrichten aus den Spam-Kampagnen und überprüft, ob diese eine signifikante Verbindung zueinander aufweisen. Ist dies der Fall, handelt es sich mit großer Wahrscheinlichkeit auch um das gleiche Botnetz. Diese Verbindung kann mathematisch beschrieben werden.

Gegeben sind ein Ereignis (IP_1, t_1) von einer Spamkampagne SC_1 und ein Ereignis (IP_2, t_2) von einer Spamkampagne SC_2. IP_n ist die IP-Adresse eines Rechners und grob betracht ist t_n ein Zeitpunkt eines Ereignisses, das mit der IP-Adresse IP_n verknüpft ist. Allerdings gibt tritt auch hier das in Abschnitt 2 kurz beschriebene Problem der dynamischen IP-Adressen auf. Wichtig ist, dass es für die nun folgende mathematische Beschreibung von Bedeutung ist, dass ein Computer seine IP-Adresse innerhalb eines bestimmten Zeitfensters $t_2 - t_1$ behält oder ändert und dass diese Wahrscheinlichkeit durch eine Funktion gegeben ist. Eine typische Wahrscheinlichkeitsverteilung dafür ist in Abbildung 7 dargestellt. Dabei lässt sich erkennen, dass dieser Wechsel bei den meisten IP-Adressen bereits

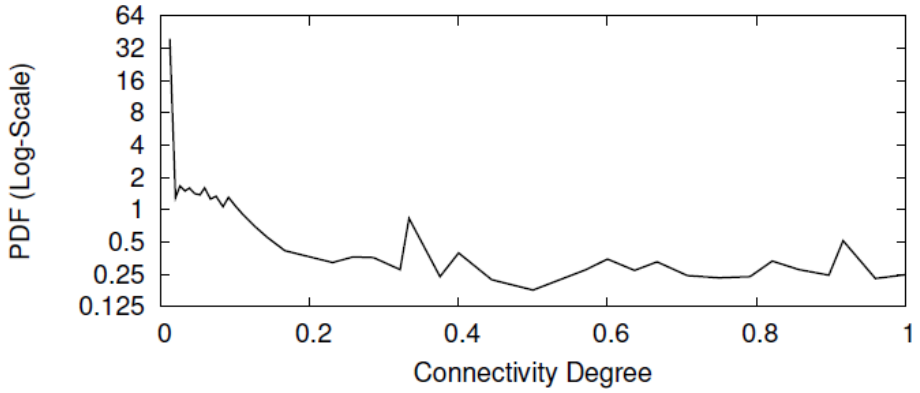

Abbildung 8: Die Wahrscheinlichkeitverteilung für den Konnektivitätsgrad W. Anhand der mittleren Werten lässt sich ein guter Schwellwert ableiten, ab wann zwei Spam-Kampagnen zum gleichen Botnetz gehören. *Bildquelle:* (ZDSW08)

nach einem Tag eintritt. Für genauere Informationen verweise ich auch hier auf die beiden Papers (ZDSW08) und (XYA+07).

Die Funktion $w(t_1,t_2)$ beschreibt die Wahrscheinlichkeit, mit der ein Computer seine IP-Adresse über das Zeitinterval $[t_1,t_2]$. Das Gegenereignis ist dementsprechend die Wahrscheinlichkeit $1 - w(t_1,t_2)$, welche beschreibt, dass der Computer seine IP-Adresse im genannten Zeitinterval ändert. Mit der Funktion w lässt sich später auch die Größe des Botnetzes abschätzen. Dann gibt es noch den Sonderfall 0, der auftritt, wenn eine IP-Adresse sich nicht im Zeitintervall $[t_1,t_2]$ befindet.

Für alle Ereignisse in der Spamkampagne SC_1 lässt sich der Anteil der miteinander verbundenen Ereignisse durch die Funktion W abschätzen. W ist folgendermaßen definiert:

$$W = \frac{\sum_i \max_j \left[w\left(t_i,t_j\right) \ or \left(1 - w\left(t_i,t_j\right)\right) \ or \ 0 \right]}{|SC_1|}$$

Die Indizes i und j repräsentieren hierbei Ereignisse auf den IP-Adressen aus SC_1 und SC_2. Der *Konnektivitätsgrad* W liegt dabei im Interval $[0,1]$. Wenn W einen großen Wert annimmt, bedeutet dies, dass ein großer Anteil an Ereignissen aus SC_1 mit denen aus SC_2 verknüpft ist. Wie das Diagramm in Abbildung 8 erkennen lässt, sind die meisten Werte von W sehr klein und nur wenige Werte besitzen eine mittlere Größe. Die größeren Werte von W stellen zwei unterschiedliche Spam-Kampagnen aus dem gleichen Botnetz dar. Anhand der mittleren Werten lässt sich ein guter Schwellwert ableiten, ab wann zwei Spam-Kampagnen zum gleichen Botnetz gehören und deren Ereignisse so gemeinsam betrachtet werden können. Ein Schwellwert mit einem Wert von 0.2 liefert dabei gute Ergebnisse (ZDSW08).

Neben der Ähnlichkeit zweier Spam-Kampagnen kann man mit dem Konnektivitätsgrad auch das Verhalten der Botnetz-Controller einschätzen. Wenn ein Botnetz-Controller für eine Spam-Kampagne immer alle Bots verwendet, so lässt sich beobachten, dass jede Spam-Kampagne einen Konnektivitätsgrad von $W = 1$ besitzt. Jedoch benutzen die Botnetz-Controller für eine Spam-Kampagne immer nur einen gewissen Anteil an verfügbaren Bots.

Sind die Botnetze identifiziert, so kann man verschiedene Beobachtungen machen, welche ich im folgenden Abschnitt vorstelle.

4 Beobachtungen

4.1 Spam-Sendeverhalten

Die Dauer einer Spam-Kampagne ist als die Zeitspanne zwischen der ersten und der letzten E-Mail aus der Kampagne definiert. Wie bereits in Abschnitt 2 und Abbildung 3 gezeigt wurde, enden die meisten Spam-Kampagnen bereits nach 12 Stunden. Die Dauer Spam-Kampagne unterscheidet sich meist von der Lebensdauer eines Botnetzes, da Spammer häufig das gleiche Botnetz für mehrere Spam-Kampagnen verwenden. Die Mails der Spam-Kampagnen werden mit einer Standardabweichung von 1,81 Stunden fast simultan versendet. Die Anzahl an Spam-Nachrichten pro Bot reicht von 10 bis über Tausend.

Betrachtet man die Hosts der Botnetze individuell, so lässt sich kein eindeutiges Sendemuster erkennen und man kann sie somit nicht von normalen E-Mail-Hosts unterscheiden. Zusätzlich wurde festgestellt, dass der Inhalt der E-Mails sich sehr stark unterscheidet, obwohl die E-Mails oft die gleichen URL-Signaturen besitzen. Für das Erkennen von Sendemustern versucht man, die Botnetz-Hosts mit den drei Parametern *Verbindungen pro Sekunde*, *Empfängeranzahl* und der *Häufigkeit von nicht-existenten Empfängern* in Cluster zu gruppieren, dadurch die Sendedaten zu modellieren und dann mit Hilfe neu auftretender Sendemuster zu lernen und das Modell zu verbessern. Dabei kommt ein Gaußsches Modell zum Einsatz. In der Studie (XYA$^+$08) wurde festgestellt, dass die meisten Botnetz-Hosts sich sehr gut zu Clustern gruppieren lassen und es nur wenige Botnetz-Hosts gibt, deren Mails in Empfängeranzahl und Verbindungen pro Sekunde stark abweichend sind.

Außerdem wurde beobachtet, dass 60% der Spam-Mails von langlebigen Botnetzen stammen. Wäre es der Fall, dass für jede Spam-Kampagne ein Botnetz verwendet würde, wäre es wenig sinnvoll, Spam-Filter zu benutzen, weil man das Verhalten kaum abschätzen kann. In der Praxis ist es jedoch nicht der Fall und deshalb ist auch sinnvoll, das Verhalten der Botnetze zu beobachten.

4.2 Größe und Verbreitung der Botnetze

Anhand der gegebenen IP-Adressen und der Spam-Mails lässt sich auch die Größe der Botnetze mathematisch abschätzen. Die Größe der Botnetze variiert sehr stark. Ein Botnetz kann nur wenige, aber unter Umständen auch bis zu Zehntausende Computer umfassen. Die Hälfte der Botnetze umfasst über 1000 Computer. Dabei zeigte sich, dass große Botnetze meist weniger und kleinere Botnetze meist mehr Spam pro Bot versenden. Außerdem sind meist nicht alle Bots im Botnetz aktiv. Über 80% der Botnetze nutzen weniger als die Hälfte ihrer Bots gleichzeitig. Dabei spielt die Größe des Botnetzes keine Rolle.

Botnetze erstrecken sich meist über den gesamten Erdball. In den Studien zeigte sich, dass die Hälfte der Botnetze Computer in über 30 Ländern kontrollieren, manche sogar in über 100 Ländern. Die geographische Verteilung von Botnetzen gibt auch Aufschluss darüber, inwieweit die Botnetz-Controller in der Lage sind, PCs zu übernehmen und somit zu steuern.

4.3 IP-Adressen der Botnetze

Bei den erkannten Botnetzen wurde beobachtet, dass die IP-Adressen typischerweise über eine große Anzahl an autonomen System verteilt sind und jedes autonome System besitzt nur eine kleine Anzahl an Rechnern, die zum Botnetz gehören.

Im Durchschnitt sind 69% der IP-Adressen ist dynamisch, was bedeutet, dass Rechner, die sich über eine dynamische IP-Adresse ins Netz einwählen, ein bevorzugtes Ziel für Botnetz-Infektionen sind. In der Studie (XYA$^+$08) wurde außerdem beobachtet, dass sich der Anteil der Hosts mit dynamischen IP-Adressen erhöht.

5 Fazit

In der Studie von (XYA+08) wurde das AutoRE-Framework für die Erkennung von Botnetzen anhand von Spam-Mails vorgestellt. AutoRE benötigt keine vorklassifizierten Eingabedaten, weiße Listen oder andere Trainingsdaten. Die URLs der Spam-Mails werden anhand von regulären Ausdrücken mit Signaturen gekennzeichnet (auch unter Berücksichtigung des Zeitpunkt des Versendens und der IP-Adressen) und der Spam wird in Kampagnen eingeteilt. Die Autoren der Studie erwarten, dass die generierten Signaturen für spätere Zwecke sinnvoll eingesetzt werden können.

Das AutoRE-Framework wurde aufgrund der niedrigen Sampling-Rate (1:25000) nicht unter realistischen Bedingungen getestet, dennoch konnten so Botnetze zweifelsfrei identifiziert werden. Ob das Framework auch in Echtzeit funktioniert, wurde ebenfalls nicht getestet, aber laut der Autoren der Studie besitzt es das Potential dazu. Zwei offene Frage sind, wie sich das Auto-RE-System tatsächlich unter Realbedingungen verhält und ob es Echtzeit-fähig ist.

Ein weiteres Ergebnis der Studie ist, dass aus den erzeugten Signaturen, Botnetze und deren Spam eindeutig identifiziert und charakterisiert werden können. Außerdem können daraus auch nützliche Informationen wie Größe, Spam-Sendeverhalten und die IP-Adressen der Botnetze abgeleitet werden, was Schwerpunkt der Studie (ZDSW08) war. Dadurch können Botnetze lokalisiert und gezielt bekämpft werden. Eine Information, die bisher nicht in Betracht gezogen wurde, aber auch Rückschlüsse auf die Botnetz-Aktivität zulässt, ist das Betreten und Verlassen der IRC-Channels, die von den Botnetz-Controllern zur Steuerung der Botnetze verwendet werden.

Zur Identifizierung werden die Eigenschaften der weiten geographischen Verteilung und das geringe Zeitfenster beim Versenden der Spam-Mails berücksichtigt. Nun könnte es passieren, dass eine große Firma legitime E-Mails als Werbung oder Newsletter verschickt und das System die Absender fälschlicherweise als Botnetz erkennt. Jedoch sind bei einer großen Firma im Gegensatz zu einem Botnetz nur wenige autonome Systeme im Spiel, wodurch diese legitimen Werbemails von Botnetz-Spam unterschieden werden können. Ein anderes Szenerio für False-Positives wäre, wenn viele Benutzer sich gegenseitig E-Mails schicken, die populäre URLs enthalten. Jedoch dürften solche Ereignisse laut den Autoren der Studie nur äußerst selten auftreten.

Die Verschleierung der Spam-Mails wird durch URL-Signatur-Generierung stark erschwert oder gar fast unmöglich gemacht. Zur weiteren Verschleierung der Spam-Mails können Techniken der URL-Weiterleitung eingesetzt werden. Hier werden scheinbar zusammenhangslose URLs generiert, die auf ein gemeinsames Ziel verweisen. Dies wurde in der Studie (XYA+08) nicht berücksichtigt, aber es wurde bereits ein Lösungsansatz vergeschlagen, der darin besteht, dass man den Pfade der Weiterleitung bei Signaturgenerierung berücksichtigt.

In beiden Studien konnte gezeigt werden, dass die Botnetz-Hosts im Internet weitläufig verteilt sind und dass das Sendemuster einzeln betrachtet nicht von normalen Servern zu unterscheiden ist. Deshalb stellt auch das Auffinden von Botnetz-Hosts immer noch eine schwierige Aufgabe dar.

Allerdings wurde bei beiden Studien überhaupt nicht berücksichtigt, wie hoch der Anteil der Botnetze ist, die Spam aussenden, denn nur solche können mit den beschriebenen Methoden überhaupt erst identifiziert werden. Außerdem wurden in beiden Studien den immer häufiger in Social-Networks wie MySpace oder Facebook auftretenden Spam und Spam, der via Instant-Messaging-Protokolle wie ICQ oder Skype versendet wird, nicht berücksichtigt; es wurden lediglich Datensätze von zufällig ausgesuchten E-Mails von diversen E-Mail-Providern als Testobjekte verwendet.

Fasst man die beiden Studien zusammen, so ist es durch mathematische Techniken und maschinellem Lernen in hervorragender Weise gelungen, Botnetz-Spam von legitimen E-Mails zu unterscheiden und durch den Spam die Botnetze zu identifizieren und zu charakterisieren.

Literatur

[AKO04] ABOUELHODA, Mohamed I. ; KURTZ, Stefan ; OHLEBUSCH, Enno: Replacing suffix trees with enhanced suffix arrays / Universität Ulm. 2004. – Forschungsbericht

[Kam08] KAMLUK, Vitaly: *Botnetze - Geschäfte mit Zombies*. Mai 2008. – http://www.viruslist.com/de/analysis?pubid=200883611

[Wat09] WATERS, Darren: *Spam overwhelms e-mail messages*. 2009. – http://news.bbc.co.uk/2/hi/technology/7988579.stm

[Wik06] WIKIPEDIA: *Ablauf der Entstehung und Verwendung von Botnetzen*. 2006. – http://de.wikipedia.org/w/index.php?title=Datei:Zombie-process.pngfiletimestamp=20060728173916

[XYA+07] XIE, Yinglian ; YU, Fang ; ACHAN, Kannan ; GILLUM, Eliot ; GOLDSZMIDT, Moises ; WOBBER, Ted: How Dynamic are IP Addresses? / Microsoft Research. 2007. – Forschungsbericht

[XYA+08] XIE, Yinglian ; YU, Fang ; ACHAN, Kannan ; PANIGRAHY, Rina ; HULTEN, Geoff ; OSIPKOV, Ivan: Spamming Botnets: Signatures and Characteristics / Microsoft Research, Silicon Valley. 2008. – Forschungsbericht

[ZDSW08] ZHUANG, Li ; DUNAGAN, John ; SIMON, Daniel R. ; WANG, Helen J.: Characterizing Botnets from Email Spam Records / U.C. Berkley. 2008. – Forschungsbericht