Seminararbeit

im Fach

Verteilte Systeme B

Weiterentwicklung des IPMapViewers

April 2009

Verfasser

Alexander Schuch
E-Mail: schuch@internet-sicherheit.de

Betreuer

Prof. Dr. Norbert Pohlmann
Christian J. Dietrich

Inhaltsverzeichnis

1 Übersicht

Um das Arbeiten mit dem IPMapViewer (vgl. Schuch / Gertzen 2007) weiter zu verbessern und effizienter zu gestalten, wurden zusätzliche Funktionen implementiert. Diese ermöglichen nun das Erstellen von Diagrammen und vereinfachen das Anlegen von IP-Tabellen durch den automatisierten Import von IP-Informationen in eine Datenbank. Auf die Realisierung dieser neuen Funktionen wird im zweiten Kapitel näher eingegangen.
Des Weiteren beschäftigt sich diese Arbeit mit der Trennung des Autonomen Systems von McColo vom Internet: McColo war eine Webhosting-Firma, die bekannt für ihre fragwürdigen Aktivitäten im Internet war. Am 11.11.2008 kam es zur Trennung der Verbindungen zu McColo durch dessen Peering-Parnter Hurricane Electric und Global Crossing. Somit war McColo quasi vom Internet isoliert, mit der Folge, dass das weltweite Spamaufkommen schlagartig deutlich sank. Im dritten Kapitel wird auf diesen Vorfall detailliert eingegangen.

2 Neue Funktionen des IPMapViewers

Der IPMapViewer wurde um Funktionen erweitert, die es dem Anwender einfacher machen ihn zu verwenden und es ermöglichen mit dem Tool neben IP-Maps (vgl. Kapitel 2 und 3 in Schuch / Gertzen 2007) auch Diagramme von IP-Tabellen zu generieren. Dazu wurde ein Diagramm-Generator, sowie eine Importfunktion implementiert. Im Folgenden wird auf diese beiden neuen Funktionen detailliert eingegangen.

2.1 Diagramm-Generator

Der IPMapViewer ist in erster Linie ein Programm zur Analyse und Visualisierung von großen IP-Tabellen. Bisher war es lediglich möglich die IP-Adressen in Form einer IP-Map darstellen zu lassen:

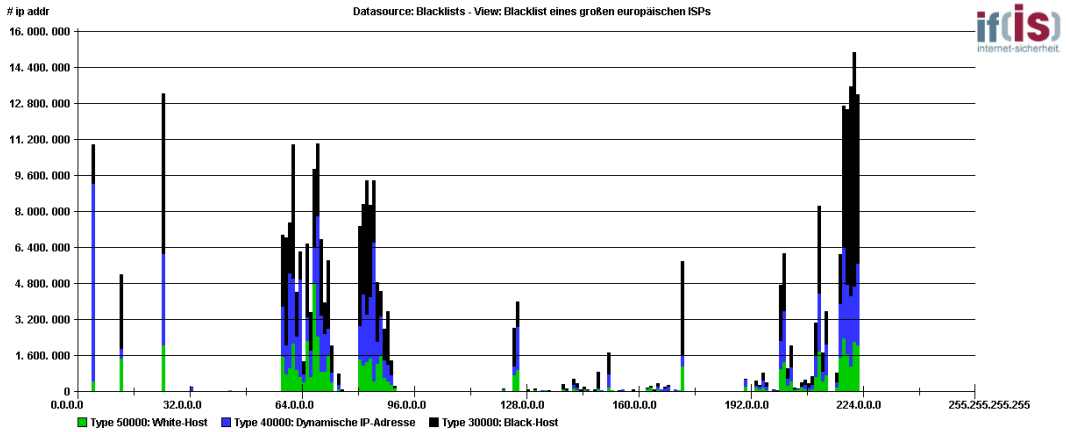

Abbildung 1: IP-Map einer Blacklist eines großen europäischen ISPs mit beispielhafter Typisierung der IP-Adressen.

Um einen schnellen Überblick über die Verteilung der verschiedenen IP-Adress-Typen in einer Tabelle/IP-Map zu ermöglichen, war es wünschenswert sich eine IP-Tabelle direkt als Kreis- bzw. Balkendiagramm auswerten und anzeigen lassen zu können. Diese Funktion wurde mit Hilfe der Java-Bibliothek JFreeChart (www.jfree.org/jfreechart) in den IPMapViewer implementiert. Jede IP-Map verfügt nun über einen Button, über den man in den dieser IP-Map zugehörigen Diagramm-Generator gelangt:

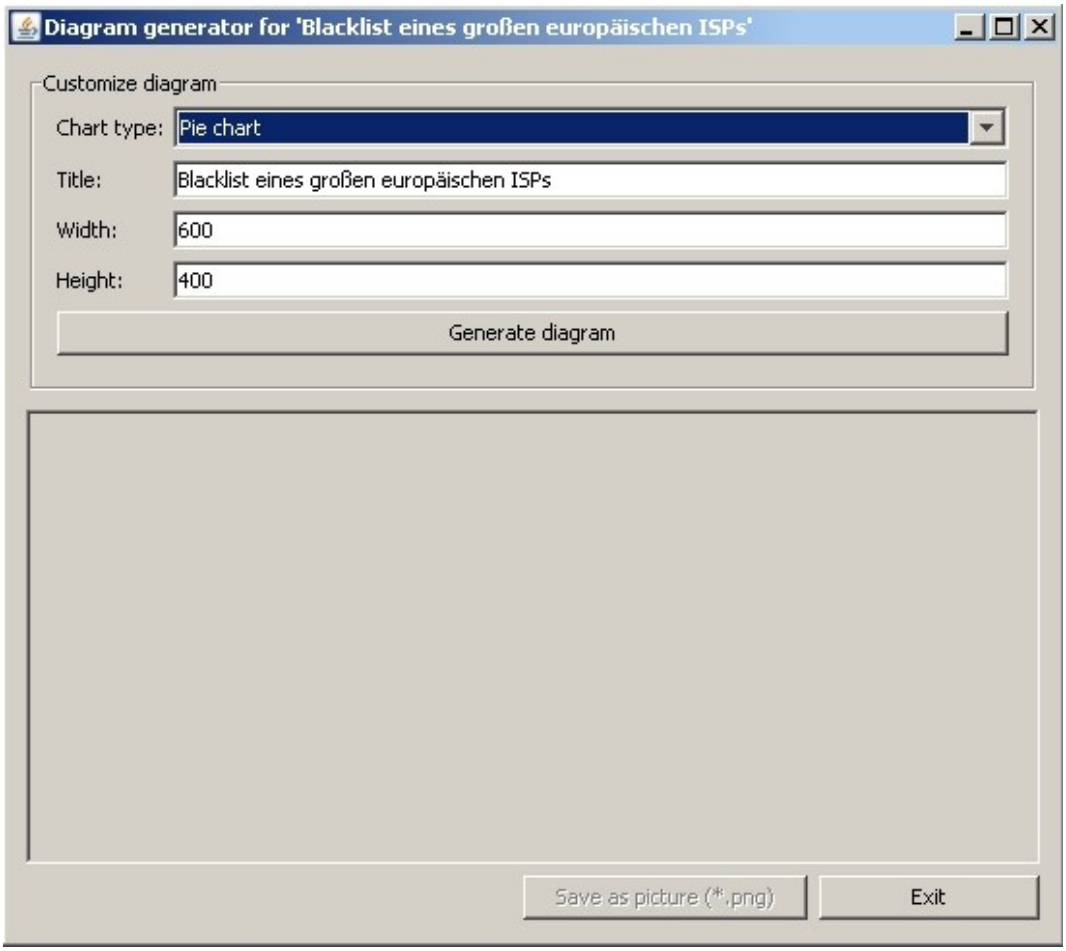

Abbildung 2: Startbildschirm des Diagramm-Generators.

In diesem Dialog hat der Anwender die Möglichkeit Einstellungen zum Erscheinungsbild des Diagramms vorzunehmen:

- Chart type: Diagrammtyp: Kreis- bzw. Balkendiagramm wählen
- Title: Überschrift des Diagramms.
- Width/Height: Breite/Höhe des Diagramms.

Über den „Generate diagram“-Button wird das Diagramm aus den Daten der IP-Map berechnet und im unteren Bildbereich des Dialogs entsprechend den eingestellten Parametern dargestellt. Das korrespondierende Kreis- und Balkendiagramm zu der in Abbildung 1 abgebildeten IP-Map ist den folgenden beiden Abbildungen 3 und 4 zu entnehmen:

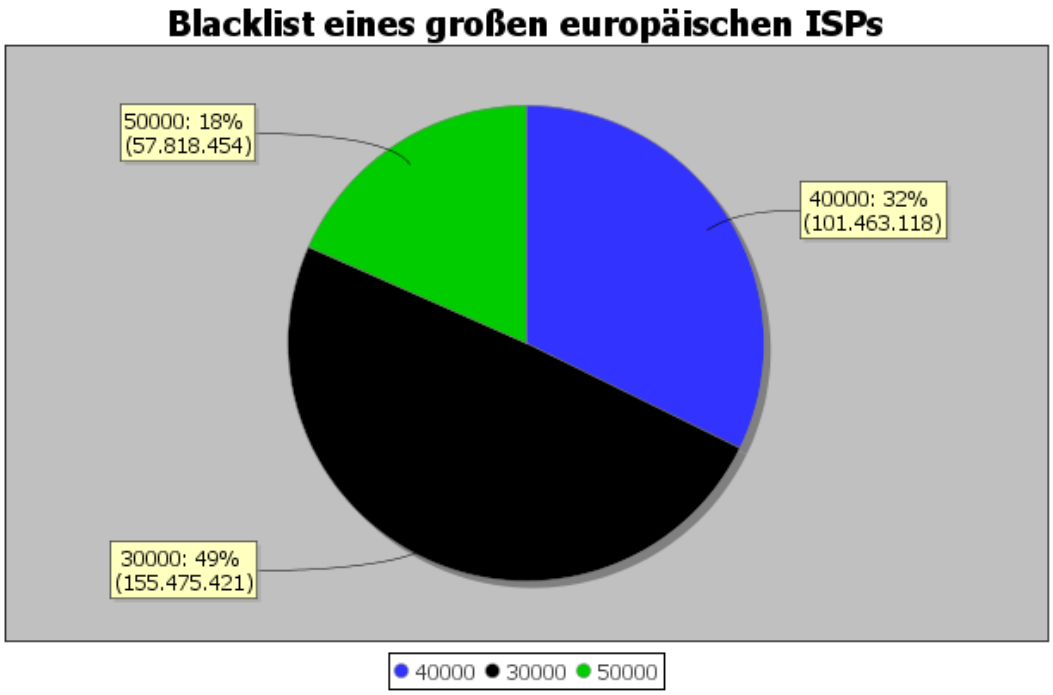

Abbildung 3: Kreisdiagramm der IP-Map aus Abbildung 1.

Die einzelnen Sektoren des Kreisdiagramms bekommen die selben Farben wie sie auch in der IP-Map haben.

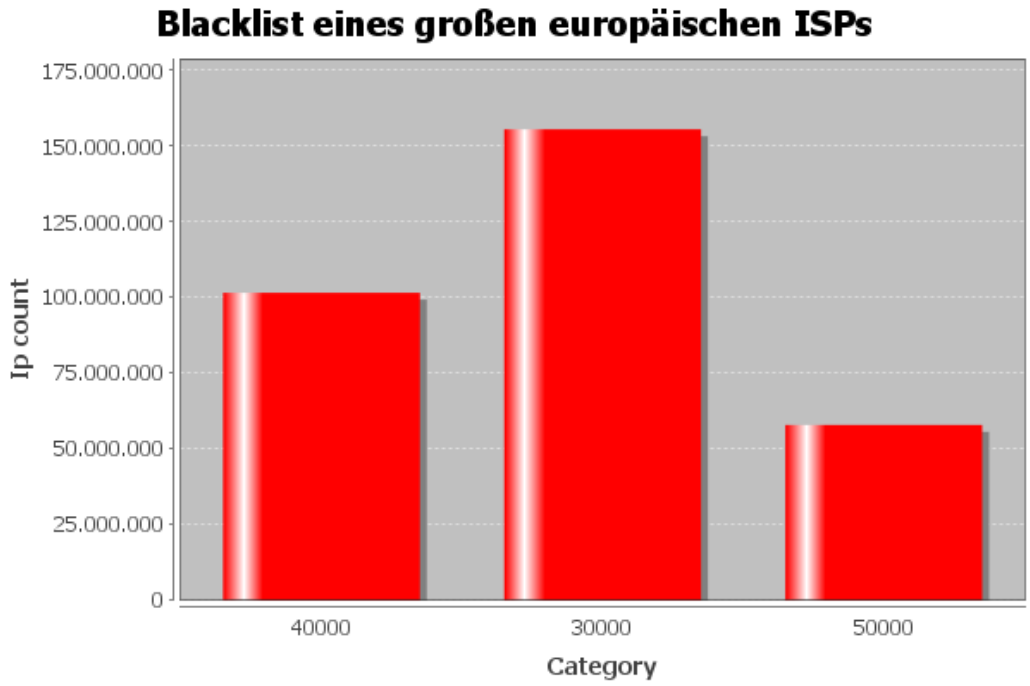

Abbildung 4: Balkendiagramm der IP-Map aus Abbildung 1.

Auf der x-Achse des Balkendiagramms sind die IP-Typen aufgetragen. Die y-Achse gibt an, wie viele IP-Adressen des entsprechenden Typs vorkommen. Über den „Save as picture (*.png)“-Button hat der Nutzer die Möglichkeit das Bild in der von ihm spezifizierten Größe (siehe Abbildung 2) im png-Format abzuspeichern.

Die Bibliothek JFreeChart bietet dem Benutzer diverse weitere Möglichkeiten, wie z.B. das direkte Ausdrucken eines Diagramms oder das Ändern der Hintergrund- und Rahmenfarbe des Diagramms. Auf diese Funktionen wird an dieser Stelle nicht näher eingegangen.

2.2 Importfunktion

Um den IPMapViewer verwenden zu können, ist es notwendig, dass die darzustellenden IP-Adressen in einer Tabelle in einem PostgreSQL-Datenbanksystem abgelegt sind. Eine solche Tabelle dient dem IPMapViewer als Datenquelle zum Generieren von IP-Maps. Es war also bislang erforderlich, dass der Nutzer weitestgehend über SQL-Kenntnisse verfügte:
Es muss eine Tabelle in einem entsprechenden Format (siehe hierzu auch Schuch / Gertzen 2007: 132) angelegt werden, welche dann im nächsten Schritt mit den IP-Adressen und evtl. weiteren zugehörigen IP-Informationen gefüllt wird. Solche zusätzlichen Informationen können beispielsweise der Typ der IP-Adresse oder ein Zeitstempel sein. Um diese Schritte für den Nutzer einfacher zu gestalten, wurde eine Importfunktion implementiert, die das Anlegen einer Tabelle, sowie das Hinzufügen der IP-Informationen automatisiert durchführt. Dazu wird nach wie vor der Zugang zu einer PostgreSQL-Datenbank, mit der Berechtigung Tabellen anlegen zu dürfen, benötigt. Weitere SQL-Kenntnisse sind nicht mehr erforderlich.
Die Struktur und der Inhalt der Tabelle, wird der Applikation durch eine simpel aufgebaute Textdatei vorgegeben: In der ersten Zeile dieser Textdatei stehen die Spaltennamen der Tabelle, jeweils durch einen Tabulator voneinander getrennt. In den folgenden Zeilen befinden sich die Daten der Tabellenzeilen, auch durch jeweils einen Tabulator voneinander getrennt.

Zur Verdeutlichung des Aufbaus dieser Datei folgt ein Beispiel:
Die Textdatei für eine Tabelle mit den zwei Spalten „ipaddress“ und „iptype“ und drei beispielhaften Datensätzen sieht folgendermaßen aus:

```
ipaddress<TABULATOR>iptype
10.10.10.10<TABULATOR>type A
20.20.20.20<TABULATOR>type B
30.30.30.30<TABULATOR>type A
```

Wurde eine Datenbank als Datenquelle im IPMapViewer angelegt (vgl. Schuch / Gertzen 2007: 114f.), so kann nun über den „Import table from *.txt“-Button die IP-Tabelle in dieser Datenbank auf einfache Art und Weise angelegt werden.

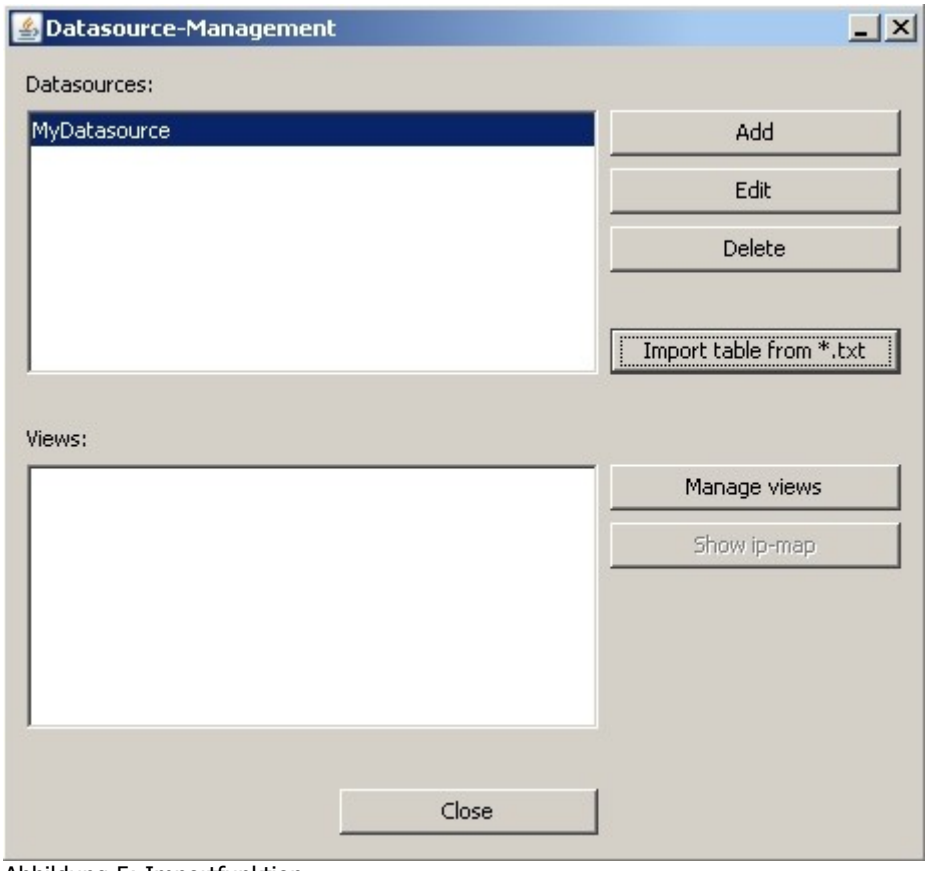

Abbildung 5: Importfunktion

Wird der Button betätigt, so erscheint ein Dialog zum Wählen der Textdatei, aus der die Tabelle generiert werden soll. Im nächsten Schritt gelangt man in den Importdialog:

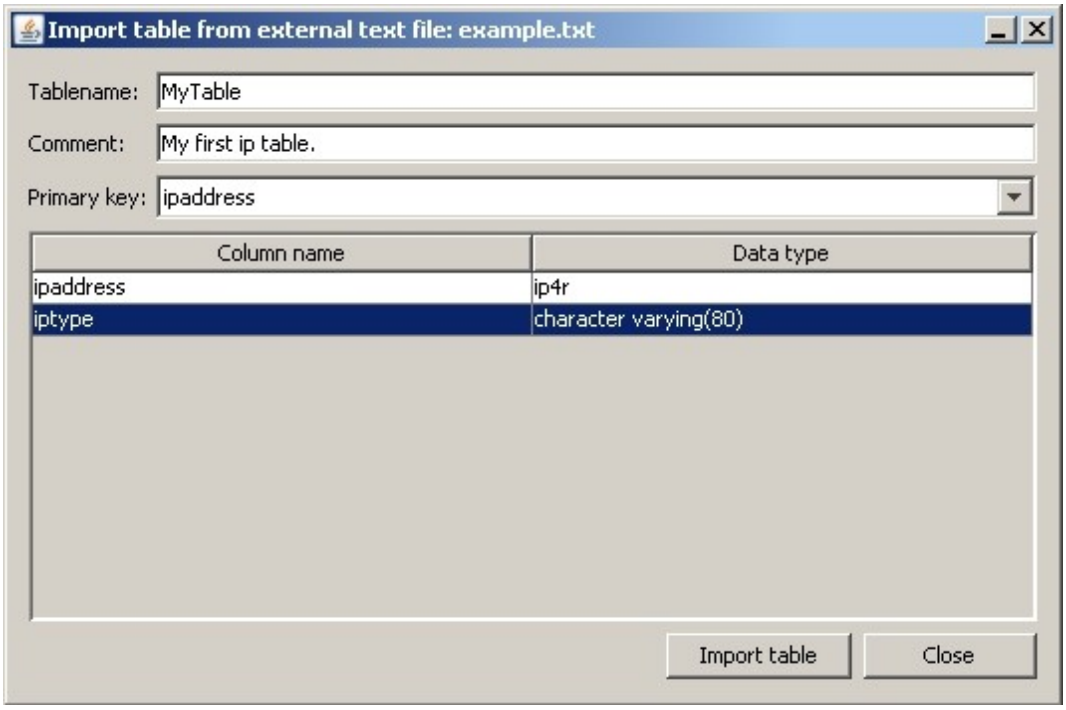

Abbildung 6: Importdialog

In diesem Dialog wird der Name der Tabelle, sowie ein optionales Kommentar festgelegt. In dem Kombinationsfeld „Primary key“ werden dem Benutzer alle Spaltennamen aus der Textdatei angezeigt. Über dieses Kombinationsfeld wird der Primärschlüssel der Tabelle, der einen Datensatz eindeutig identifiziert, festgelegt. Dieser ist in den meisten Fällen die IP-Adresse, weshalb die IP-Adress-Spalte in dem Kombinationsfeld entsprechend voreingestellt ist. In der Tabelle im unteren Bereich des Dialogs findet die Zuordnung von Spalte und Datentypen statt. In dem Beispiel in Abbildung 6 wird der Spalte „ipaddress“ der PostgreSQL-Datentyp für IP-Adressen (ip4r) zugewiesen. In der Spalte „iptype“ darf eine maximal 80 Zeichen lange Zeichenkette stehen, festgelegt durch den gewählten Datentyp „character varying(80)“.
Über den „Import table“-Button wird der Importvorgang abgeschlossen:
Die Tabelle wird den Angaben entsprechend erstellt und mit den IP-Informationen aus der Textdatei gefüllt. Von dieser Tabelle kann nun eine IP-Map erzeugt werden.

2.3 Fazit

Mit Hilfe der neuen Funktionen war es den anderen Seminarteilnehmern möglich ihre Ergebnisse auf einfache Art und Weise mit dem IPMapViewer zu importieren und darzustellen. Zu verweisen wäre hier auf die Seminararbeiten von Thomas Bottesch (Bottesch 2009) und Johannes Mrosek (Mrosek 2009).

3 Exkurs: McColo

McColo war ein US-amerikanischer Webhosting-Provider, der für seine Spammer-Freundlichkeit bekannt war. Das Unternehmen war ein sogenannter bullet-proof Hoster[1]. Kunden von McColo hatten somit die Möglichkeit Dienste im Internet anzubieten und Daten jeglicher Art hochzuladen, ohne dafür rechtlich belangt werden zu können.
Das haben sich Spammer zu Nutze gemacht, so dass neben diversen illegalen Inhalten auch Botnetz-Master-Server, die als Kommando- und Kontrollserver für hunderttausende kompromittierter PCs zum Verbreiten von Spam oder für Denial-of-Service-Angriffe dienten, bei McColo gehostet waren (vgl. Washington Post 2008a). Einige Quellen sprachen davon, dass McColo für bis zu drei Viertel des gesamten Spamversands im Internet verantwortlich gewesen sei.
Die beiden wichtigsten Internetprovider von McColo waren Global Crossing und Hurricane Electric. Diese kappten am 11.11.2008 die Leitungen zu McColo, nachdem sie von Sicherheitsexperten auf die illegalen Tätigkeiten aufmerksam gemacht wurden (vgl. iX 2008), sodass McColo komplett vom Internet isoliert wurde und somit seine Tätigkeiten eingestellt wurden.

Die folgenden Abbildungen, die mit Hilfe des Tools bgplay (http://bgplay.routeviews.org/bgplay) gemacht wurden, dokumentieren das Abschalten der Verbindungen:

1 „...Als bullet-proof hosted bezeichnet man einen Server, der aufgrund der lockeren Rechtslage am Aufstellungsstandort nicht durch Strafverfolgungsbehörden abgeschaltet werden kann. Zudem können die Betreiber dieses Servers unbekannt bleiben...“ (Institut für Internet-Sicherheit 2009).

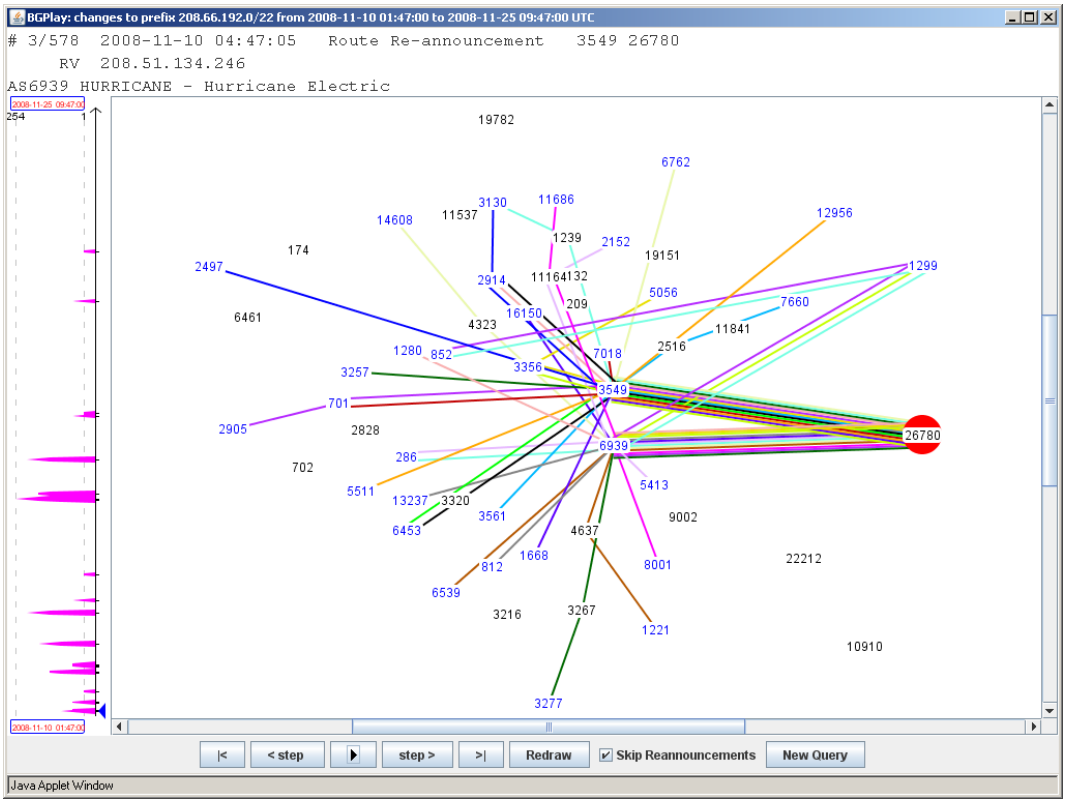

Abbildung 7: 10.11.2008: McColo vor der Abschaltung der Verbindungen durch Global Crossing und Hurricane Electric.

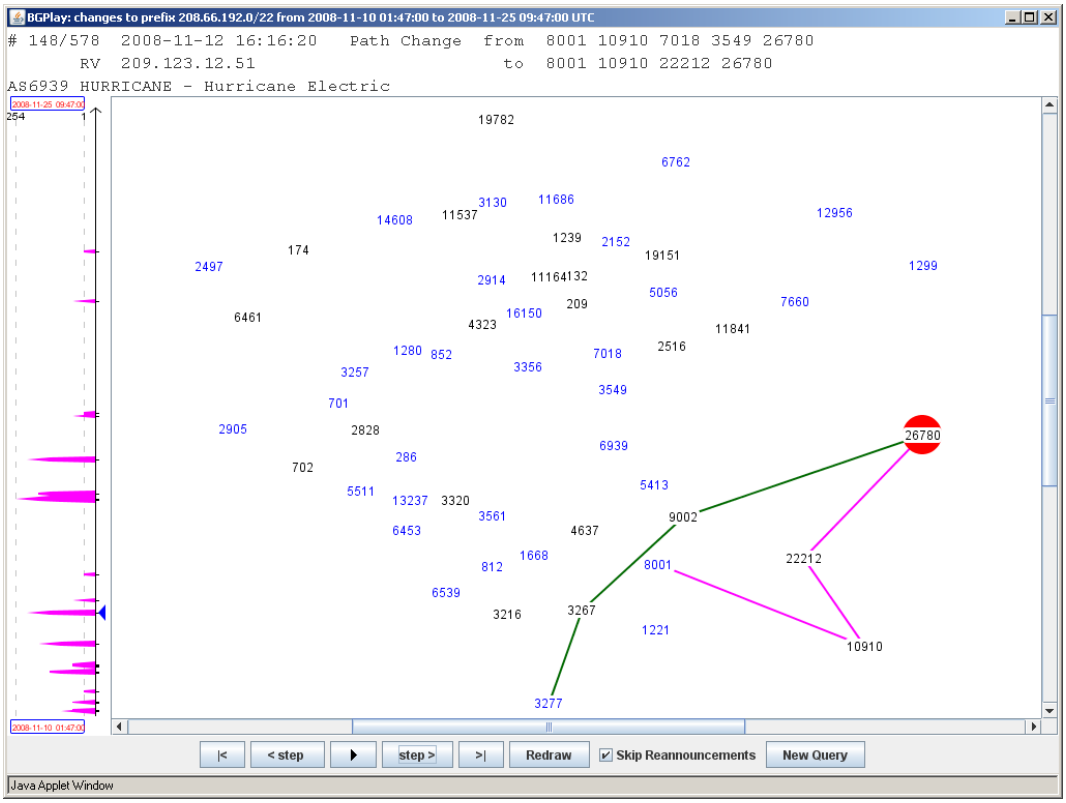

Abbildung 8: 12.10.2008: McColo nach dem Abschalten der Verbindungen durch Global Crossing und Hurricane Electric.

Abbildung 7 wurde am 10.11.2008 erstellt und zeigt die Pfade des Autonomen Systems McColo (AS26780) vor dem Abschalten der Verbindungen durch Global Crossing (AS3549) und Hurricane Electric (AS6939).
Die Grafik die in Abbildung 8 dargestellt ist, wurde am 12.11.2008 nach dem Abschalten der Verbindungen erstellt. Es ist gut zu erkennen, dass McColo quasi vollständig vom Internet entkoppelt wurde.

Die Abschaltung machte sich dadurch bemerkbar, dass das globale Spamaufkommen schlagartig mehr als halbiert wurde. Dies zeigte beispielsweise eine Statistik der Plattform SpamCop[2]:

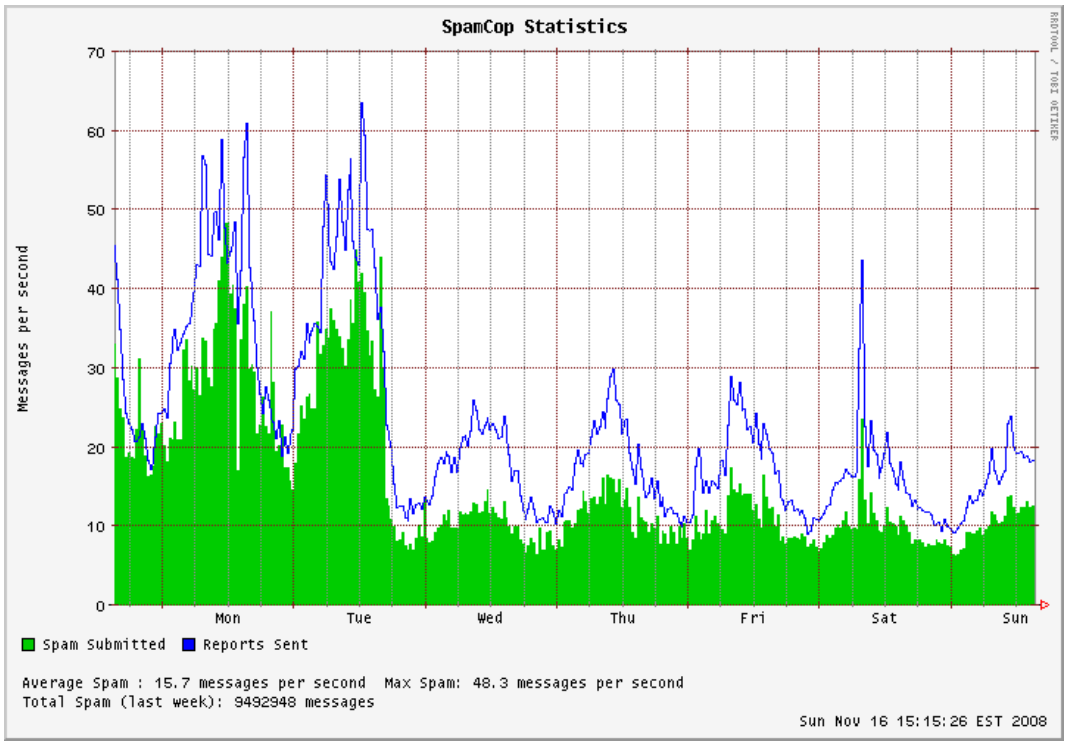

Abbildung 9: Spam-Report von SpamCop vom 10.11.2008 bis zum 16.11.2008 (Quelle: (www.spamcop.net).

Ebenso ist dies an der Zahl der DNS-Abfragen, die am Blacklist-Slave der NiX-Spam-Blacklist im Institut für Internet-Sicherheit beobachtet werden konnte, zu erkennen:

2 SpamCop ist ein kostenloser Spam-Reporting Service, der es Empfängern von unerwünschten E-Mails erlaubt, die ISPs der Absender der Spammails darüber zu informieren. SpamCop selbst nutzt diese Informationen, um selbst Blacklisten gegen Spammer zu generieren (vgl. Wikipedia: SpamCop 2009).

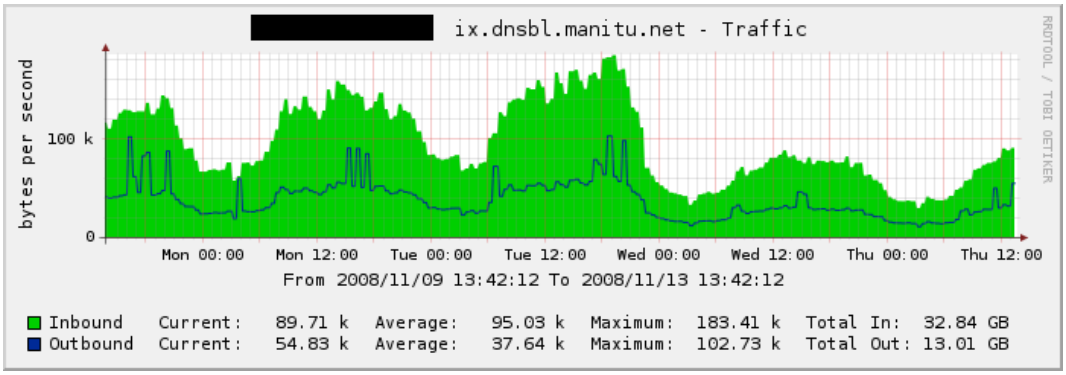

Abbildung 10: Statistik über die Zahl der DNS-Abfragen am Blacklist-Slave der NiX-Spam-Blacklist im Zeitraum vom 09.11. bis 13.11.2008 (Institut für Internet-Sicherheit 2008).

Die Anzahl der Anfragen – und somit der Mailverkehr auf den abfragenden Mailservern – lag am Dienstagabend ab 22:00 Uhr CET um mehr als die Hälfte niedriger als an den vorherigen Tagen. Etliche große Botnetze hatten scheinbar durch das McColo-Aus wesentliche Server verloren.
Dies stellte auch MessageLabs (www.messagelabs.com) fest. Deren Analysen ergaben, dass die Aktivitäten von „Mega-D“ um 80 Prozent, die von „Srizbi“ um 60 Prozent und die von „Rustock“ um 50 Prozent abgenommen hatten. Alle drei gehören zu den größten Botnetzen weltweit (vgl. ZDNet 2008).

Die Washington Post berichtete darüber, dass bei IronPort – einer Firma für E-Mail-Sicherheit – sogar nachmittags am 11.11.2008 ein Alarm ausgelöst wurde, weil das Spamaufkommen plötzlich um über zwei Drittel sank. Sie dachten zunächst, dass es sich um ein technisches Problem ihrerseits handeln würde und suchten nach dem Fehler, bis sie dann erfahren haben, dass es daran lag, dass McColo vom Netz genommen wurde (vgl. Washington Post 2008b).

Ganze zehn Tage lang blieb das globale Spamaufkommen auf dem niedrigen Niveau. Dies ist an der folgenden Abbildung, wieder anhand der Anzahl der Abfragen an den Blacklist-Slave der NiX-Spam-Blacklist, sehr gut zu erkennen:

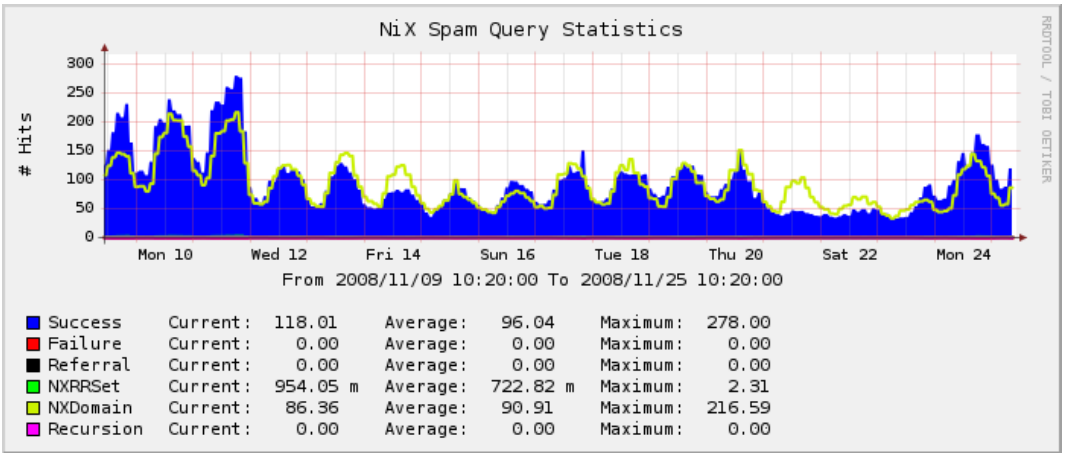

Abbildung 11: Statistik über die Zahl der DNS-Abfragen am Blacklist-Slave der NiX-Spam-Blacklist im Zeitraum vom 09.11. bis 25.11.2008 (Institut für Internet-Sicherheit 2008).

Im Zeitraum vom 21. bis 23.11.2008 ist ein deutliches Tief zu erkennen. In einer News auf Heise Online wird von einem Jahrestief der Spam-Aktivität gesprochen. Der Grund dafür liege wohl darin, dass die Betreiber der verbliebenen Botnetze in diesem Zeitraum mit DDoS-Angriffen demonstriert hätten und deshalb scheinbar nur sehr wenig Kapazität für das Versenden von Spam übrig blieb (vgl. Heise 2008).
Seit dem 25.11.2008 konnte beobachtet werden, dass die globale Anzahl an Spam-Nachrichten wieder stark zunahm und sich dem ehemaligen hohen Niveau annäherte. Die Freude über die Entlastung der E-Mail-Postfächer war somit leider nur von kurzer Dauer.

Sehr interessant ist, dass am 15.11.2008 festgestellt werden konnte, dass McColo kurzzeitig wieder am Internet über das Autonome System TeliaNet Global Network (AS1299) angebunden war:

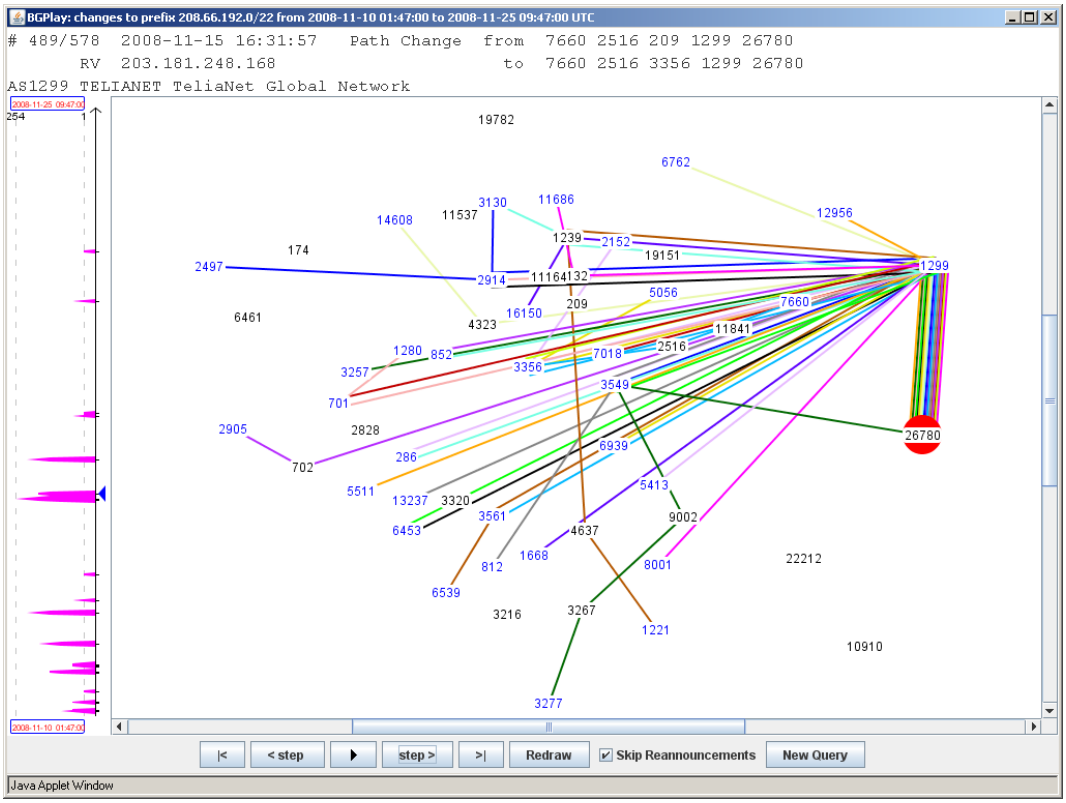

Abbildung 12: 15.11.2008:McColo war nach der Abschaltung kurze Zeit über das Autonome System von TeliaNet Global Network wieder online.

Es ist sehr gut möglich, dass in dieser Zeit die Master-Server der Botnetze von den Besitzern auf andere IP-Adressen umkonfiguriert wurden, sodass sie schon nach kurzer Zeit wieder aktiv zum Instruieren von kompromittierten PCs für die Spamverbreitung eingesetzt werden konnten (vgl. Institut für Internet-Sicherheit 2008).

Anhang

Literaturverzeichnis

Heise 2008 – Heise Online, 2008: Spam fällt auf Jahrestief – http://www.heise.de/newsticker/Spam-faellt-auf-Jahrestief--/meldung/119321, abgerufen am 21.04.2009

Institut für Internet-Sicherheit 2008 – Institut für Internet-Sicherheit, 2008: Die McColo-Geschichte aus der Spam-Perspektive – http://www.internet-sicherheit.de/forschung/aktuelle-projekte/e-mail-verlsslichkeit/spam-analyse/, abgerufen am 22.04.2009

Institut für Internet-Sicherheit 2009 – Institut für Internet-Sicherheit, 2009: Glossar: bullet-proof hosted – http://www.internet-sicherheit.de/service/glossar/eintrag/eintrag-detail/bullet-proof-hosted/?type=0&cHash=63d3540116, abgerufen am 21.04.2009

iX 2008 – Heise Online, 2008: US-Provider ziehen Spam-Schleuder den Stecker – http://www.heise.de/ix/US-Provider-ziehen-Spam-Schleuder-den-Stecker--/news/meldung/118804, abgerufen am 21.04.2009

Washington Post 2008a – The Washington Post, 2008: Host of Internet Spam Groups Is Cut Off – http://www.washingtonpost.com/wp-dyn/content/article/2008/11/12/AR2008111200658.html?sid=ST2008111200662&s_pos=, abgerufen am 21.04.2009

Washington Post 2008b – The Washington Post, 2008: Spam Volumes Drop by Two-Thirds After Firm Goes Offline – http://voices.washingtonpost.com/securityfix/2008/11/spam_volumes_drop_by_23_after.html, abgerufen am 21.04.2009

Wikipedia: SpamCop 2009 – Wikipedia.org, 2009: Artikel: SpamCop – http://en.wikipedia.org/wiki/Spamcop, abgerufen am 21.04.2009

ZDNet 2008 – ZDNet.de, 2008: Webhoster-Aus versetzt Botnetz schweren Schlag – http://www.zdnet.de/news/wirtschaft_sicherheit_security_webhoster_aus_versetzt_botnetz_schweren_schlag_story-39001024-39198981-1.htm, abgerufen am 22.04.2009

Bottesch, Thomas, 2009: Weiterentwicklung des Verificationservers

Mrosek, Johannes, 2009: Das LAS als Datenquelle für den IP-Map-Viewer

Schuch, Alexander / Gertzen, Bernd, 2007: Plattformunabhängiges Visualisierungstool zur Darstellung typisierter IP-Adressbereiche

Abbildungsverzeichnis