

# Hintergrundstrahlung im Internet

Andreas Böh von Rostkron  
(rostkron@in.tum.de)

Seminar „Internet Measurement“,  
Technische Universität München

SS 2005 (Version vom 24. Juli 2005)

## Zusammenfassung

Dieses Papier handelt - aufbauend auf einer Studie mit dem Titel *“Characteristics of Internet Background Radiation”* [1] - von der Charakterisierung von ungewünschten Internetpaketen, die in großer Anzahl fortwährend auftreten. Dieser Effekt des beständigen Auftretens von nicht angeforderten Paketen wird Hintergrundstrahlung genannt. Um diese sinnvoll untersuchen zu können, benötigt man einerseits geeignete Filter, die die Unmengen an Paketen reduzieren. Andererseits sind automatische Antwortgeber, sog. Responder, hilfreich, die einen vorhandenen Server vortäuschen, um den eigentlichen Grund der versuchten Kontaktaufnahme zu enthüllen, der oft erst bei erfolgreicher Rückmeldung preisgegeben wird. Durch verschiedene Untersuchungen im Hinblick auf Protokoll, Applikation und oftmals spezielle Angriffe wird sich zeigen, dass es sich bei der großen Mehrheit der Pakete um Kontaktversuche von Würmern, Scannern oder Viren handelt sowie um Antwortpakete von DoS-Attacken.

## 1 Einleitung

In den vergangenen Jahren haben sich die grundlegenden Eigenschaften des Internet-Traffics verändert. Während in bisherigen Studien kaum die Rede von böartigem Traffic war, ist dieser heutzutage stets zugegen und stellt eine enorme Bedrohung für Unternehmen und Einzelpersonen dar. Nicht nur, dass sehr viele unerwünschte Pakete ein Netzwerk belasten, sondern es drohen insbesondere dann Gefahren, wenn ein Paket an eine Internetadresse geschickt wird, an der tatsächlich ein Computer vorhanden ist. Antwortet dieser auf das Paket, kommt ein Dialog zustande, und der Angreifer kann den Computer gezielt nach möglichen Schwachstellen untersuchen. So wird in Netzwerken häufig sukzessive jede vorstellbare IP-Adresse kontaktiert, um etwaig vorhandene Computer ausfindig zu machen. Im *Lawrence Berkley National Laboratory* (LBL) beispielsweise, einem kleinen Netzwerk (/24-Netzwerk genannt) mit  $2^8 = 256$  vollkommen ungenutzten Adressen, wurden an einem wahllos bestimmten Tag über 8 Millionen Verbindungsversuche von außerhalb verzeichnet - also mehr als 92 pro Sekunde.

Um den eigentlichen Zweck dieser so genannten Hintergrundstrahlung herauszufinden, ist eine detaillierte Betrachtung der ankommenden Pakete notwendig. Dass dabei tatsächlich nur ungewollte Pakete unter die Lupe genommen werden, wird dadurch gewährleistet, dass in dem untersuchten Netzwerk keine der IP-Adressen vergeben ist.

Diese Seminararbeit zeigt in Kapitel 2 kurz die Messmethoden mit den damit verbundenen Schwierigkeiten und den zugehörigen Lösungsansätzen auf. Während in Kapitel 3 die passive Messung der Pakete im Vordergrund steht und die gesammelten Daten nach unterschiedliche Kriterien ausgewertet werden, beschäftigt sich Kapitel 4 mit den Ergebnissen des aktiven Antwortens auf eingehende Kontaktversuche. Kapitel 5 handelt von der Charakterisierung der Quellrechner. In Kapitel 6 werden die Ergebnisse dieser Arbeit noch einmal abschließend zusammengefasst und es wird ein kurzer Ausblick gegeben.

## 2 Messmethoden

In diesem Abschnitt werden die beiden Hauptwerkzeuge näher vorgestellt, mit deren Hilfe eine genaue Charakterisierung der Hintergrundstrahlung erst möglich ist:

### 1. Reduktion der enormen Masse von Internetpaketen

Vor dem Hintergrund, dass in einem /8-Netzwerk mit  $2^{24}$  ( $\approx 16,77$  Mio) IP-Adressen rund 30.000 unerwünschte Pakete pro Sekunde registriert werden, wird deutlich, dass hier eine Reduktion mit Hilfe von Filtern stattfinden muss. Dabei gibt es einen klassischen Trade-off zwischen der Reduktion des Verkehrs und dem dadurch bedingten Informationsverlust. Als sinnvollste von vier möglichen Varianten wurde die *Source-Destination-Filter*-Methode angesehen und für die Experimente innerhalb der Studie verwendet. Sie beruht auf der Annahme, dass an unterschiedlichen IP-Adressen, die von der gleichen Quelle kontaktiert werden, die gleichen Anfragen registriert werden. Diese Annahme bildet die Realität sehr gut ab; allein einige multi-Vektor-Würmer, die je IP-Adresse unterschiedliche Angriffe unternehmen, werden nur einmal und damit nicht in ihrer Gesamtheit erfasst.

### 2. Automatische Responder auf Applikationsebene

Nachdem die Hintergrundstrahlung - wie in der passiven Messung in [1], Abschnitt 4.1, herausgefunden wurde - überwiegend aus TCP/SYN Paketen besteht, müssen diese zuerst beantwortet und muss der entstehende Dialog so lange wie möglich aufrecht erhalten werden, um die einzelnen Typen der Strahlung voneinander abgrenzen zu können. Zu diesem Zweck wurden Responder für unterschiedliche Protokolle programmiert, die in der Lage sind, die Masse der ankommenden Pakete zu verarbeiten.

Die am häufigsten auftretenden Protokolle waren HTTP (Port 80), NetBIOS (Port 137/139), CIFS/SMB (Port 139/445), DCE/RPC (Port 135/1025) sowie Dameware (Port 6129). Darüber hinaus wurden Responder implementiert, die auf die Viren MyDoom (Port 3127) und Beagle (Port 2745) entsprechend reagieren.

Die Schwierigkeit bei der Implementierung solcher Responder liegt nicht allein darin, auf Pakete zu antworten, sondern vielmehr ist es wichtig, was geantwortet wird. Die meisten Quellen suchen nämlich nach bestimmten Versionen von Servern, da sie nur diese infizieren können. Erhalten sie eine falsche Antwort, kommt kein weiterer Dialog zustande.

Das folgende Beispiel zeigt einen Dialog, der einen Pufferüberlauf produziert. Erst durch das Antworten auf die erste „GET“-Anfrage kommt der Dialog zustande:

```

GET /
⇒ |200OK...Server : Microsoft – IIS/5.0|
SEARCH /
⇒ |411LengthRequired|
SEARCH /AAA... (URI length > 30KB)
⇒ (BufferOverflow)

```

Einige Angriffe können jedoch erst nach deutlich mehr als drei Anfragen als solche identifiziert werden. So lässt beispielsweise der SAMR-exe Virus erst nach zehn Runden Kommunikation das eigentliche Ziel, eine ausführbare Datei auf dem Zielrechner zu erzeugen und auszuführen, erkennen.

### 3 Passive Messung der Hintergrundstrahlung

Bei der rein passiven Messung von Paketen wird ausschließlich gemessen, ohne dass geantwortet wird. Die Auswertung der Ergebnisse erfolgt dann nach Protokoll und nach Port.

Um die Frage zu beantworten, wie viel Traffic in einer bestimmten Zeit auftritt und von welchem Typ dieser ist, wurden verschiedene Untersuchungen durchgeführt:

- Beobachtung eines /8 Class-A Netzwerks über eine Woche (11.03.04-18.03.04)
- Beobachtung im LBL Netzwerk von 10 zusammenhängenden /24 Netzwerken über eine Woche (28.04.04-05.05.04)
- Beobachtung eines /19-Netzwerks namens „UW-1“<sup>1</sup> über 80 Stunden (01.05.04-04.05.04)

Protokoll	Class A		LBL		UW-1	
	Rate	Prozent	Rate	Prozent	Rate	Prozent
TCP	130	88,5%	664	56,5%	928	95,0%
ICMP	0,376	0,3%	488	39,6%	4,0	4,2%
UDP	16,5	11,3%	45,2	3,8%	0,156	0,8%

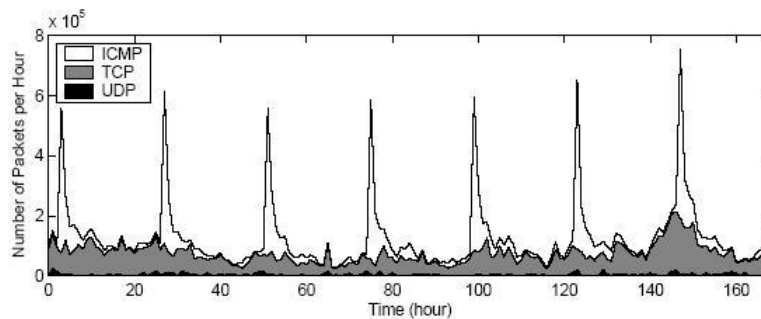
**Abbildung 1:** Traffic-Rate je Netzwerk, unterschieden nach Protokoll

Die in *Abbildung 1* angegebene Rate stellt die Anzahl der Pakete je Ziel-IP-Adresse je Tag dar und ist damit unabhängig von der eigentlichen Größe des Netzwerks. Es wird deutlich, dass TCP in allen drei Netzwerken dominiert. Die vergleichsweise geringe TCP-Rate im Class-A Netzwerk gegenüber der im UW-1 hängt vor allem mit der unterschiedlichen Messzeit zusammen. So war während der Messzeit des UW-1-Netzwerks u.a. der *Sasser-Wurm* [2] aktiv und trug erheblich zur Erhöhung der Rate bei. Aus der Grafik geht nicht hervor, dass es sich in 99% der TCP-Pakete um TCP/SYN-Pakete handelt. Diese treten in allen drei Netzwerken gut verteilt und regelmäßig auf (siehe *Abbildung 2*).

<sup>1</sup>Eines von zwei /19 UW Campus Class-B Netzwerken mit je  $2^{13} \approx 8.000$  Adressen

Im Gegensatz dazu stehen die ICMP-Pakete, die einmal pro Tag geballt auftreten und damit den in *Abbildung 2* sichtbaren Peak bilden. Dieser Ausschlag ist das Ergebnis einer kleinen Anzahl von Quellen, die jede einzelne IP-Adresse im Netzwerk scannen. Die geringe ICMP-Rate im Class-A Netzwerk (siehe *Abbildung 1*) ist wahrscheinlich darauf zurückzuführen, dass der *Welchia-Wurm* [3] dieses Netzwerk meidet ([1], Abschnitt 4.1). Wiederum in der Grafik nicht zu sehen ist, dass ICMP/echo-req 99,9% der ICMP-Pakete ausmachen.

UDP-Pakete treten im Vergleich so selten auf, dass sie in *Abbildung 2* nur am unteren Rand zu sehen sind. Dass die Rate im UW-1 noch viel niedriger als in den anderen beiden Netzwerken ist, ist u.a. damit zu begründen, dass sämtliche UDP-Pakete auf Port 1434 gefiltert werden. Damit bleiben sämtliche Angriffe des *Slammer-Wurms* [4] unberücksichtigt, der eben diesen Port 1434 verwendet.



**Abbildung 2:** Anzahl der Pakete pro Stunde im LBL-Netzwerk, unterschieden nach Protokoll

Betrachtet man die Anzahl der Quellen je Protokoll, ergibt sich folgendes Bild (siehe *Abbildung 3*), in dem wiederum TCP dominiert. Zu berücksichtigen ist dabei, dass eine Quell-IP auch Pakete unterschiedlicher Protokolle verschicken und dadurch mehrfach gezählt werden kann.

Protokoll	UW-1/2		LBL	
	#Quell-IPs	Prozent	#Quell-IPs	Prozent
TCP	759.324	87,9%	586.025	90,0%
ICMP	109.135	12,6%	64.120	9,8%
UDP	4.273	0,5%	4.360	0,7%

**Abbildung 3:** Trafficanalyse nach Anzahl der Quellen

Fokussiert man sich bei einer genaueren Untersuchung der obengenannten TCP/SYN-Pakete auf die kontaktierten Zielports, wird deutlich, dass über 80 Prozent der Pakete auf einen der acht in *Abbildung 4* gezeigten Ports abzielen. Die Summe der für diese Ports in einer Woche gemessenen Pakete im LBL-Netzwerk beträgt 12.037.064 von insgesamt 651.126 unterschiedlichen Quell-IPs.

TCP Port	Anwendung	#Quell-IPs	#Pakete
445	CIFS/SMB	43,4%	19,7%
80	HTTP	28,7%	7,3%
135	DCE/RPC	19,1%	30,4%
1025	DCE/RPC	4,3%	5,8%
2745	Beagle-Virus	3,2%	3,6%
139	NetBIOS u. CIFS/SMB	3,2%	11,1%
3127	MyDoom-Virus	2,7%	3,2%
6129	Dameware	2,2%	2,4%

**Abbildung 4:** Am häufigsten kontaktierte Ports

## 4 Aktive Charakterisierung von TCP-Paketen

Da - wie im letzten Kapitel gesehen - TCP/SYN-Pakete absolut dominieren, die den ersten Schritt zu einer Kontaktaufnahme darstellen, stellt sich die Frage, welche eigentliche Absicht all diese Pakete verfolgen. Um das herausfinden zu können, werden automatische Responder eingesetzt. Wie oben bereits erwähnt müssen diese sowohl tausende Pakete pro Sekunde beantworten als auch richtige Antworten liefern, um den Dialog mit der Quelle aufrecht zu erhalten. Im Folgenden werden die vorrangigen Angriffe an den bekanntesten Ports vorgestellt. Anschließend erfolgt eine zeitliche Betrachtung ausgewählter Angriffe.

### 4.1 Angriffe an bekannten Ports

Kontaktiert eine Quelle einen Port, ist es üblich, dass zuerst eine oder mehrere Testpakete geschickt werden, bevor der eigentlich Zweck der Kommunikation enthüllt wird. Solch ein Testpaket kann ein Verbindungsauf- und -abbau sein, bei dem kein einziges Byte gesendet wird; auch ein HTTP "GET /"-Request ist durchaus üblich.

Welche Angriffe prominenter als andere sind, wird an der Anzahl der Quellen festgemacht, die diese anstoßen. Gegenüber einer Zählung von Paketen oder Bytes hat diese Variante den Vorteil, dass Filter am Ergebnis nichts ändern, geht man davon aus, dass eine Quelle den gleichen Angriff zu allen ihren Zielrechnern startet. Außerdem zeigt sich die Popularität einer Aktivität durch die Anzahl der Quellen und damit durch die Verbreitung im Internet.

Zur besseren Verständlichkeit werden in *Abbildung 5* einige Abkürzungen eingeführt, die bei der nachfolgenden Beschreibung der verschiedenen Angriffe an prominenten Ports entsprechend verwendet werden.

**TCP Port 80 (HTTP) und HTTP-Proxy Ports:** Die meisten Angriffe, die auf diesem Port registriert werden, richten sich gegen den Microsoft IIS Server. Eine Übersicht der verschiedenen Anfragen findet sich in *Abbildung 6*. Dominant ist dabei der *WebDAV-Pufferüberlauf-Angriff* [5], der in *Abbildung 5* als „/SrchAAA“ abgekürzt ist. Nach den

Port/Abkürzung	Aktivität
80/Get	„GET /“
80/GetSrch	„GET /“ „SEARCH /“
80/SrchAAA	„GET /“ „SEARCH /“ „SEARCH /AAA...“
80/Srch64K	„SEARCH / ... (65.536 Byte URI)“
445/Nego	445/tcp/[session negotiation only]
445/Locator	„\\ <ip> \IPC\$ \locator“; RPC exploit: Exploit1896a
445/Samr-exe	“\\ <dst-IP> \IPC\$ \samr“ “\\ <dst-IP> \IPC\$ \srvsvc“ CREATE FILE: „[...] .exe“
445/Samr	“\\ <dst-IP> \IPC\$ \samr“
445/Srvsvc	“\\ <dst-IP> \IPC\$ \srvsvc“

**Abbildung 5:** Abkürzungen für häufige Anfragen

ersten beiden Testpaketen mit „GET /“ und „SEARCH /“ wird ein erneuter *SEARCH* /-Request - diesmal mit einer langen URI von oftmals 33.208 Bytes - gesendet, der mit „/AAAA...“ beginnt, um den Pufferüberlauf herbeizuführen. Bemerkenswert dabei ist, dass sich die URIs jeweils in mehreren hundert Bytes voneinander unterscheiden und der Unterschied nicht durch Verschiebung zustande kommt. Darüberhinaus bestehen die URIs außer aus ein paar Dutzend Unicode-Zeichen, die in der Nähe des Anfangs positioniert sind, ausschließlich aus Kleinbuchstaben. Es entsteht der Eindruck, dass die URIs mit dem „Venetian“-Tool [6] kriert und nach Unicode-Encodierung (Einfügen eines Bytes 0 an jedem zweiten Byte) ausführbarer x86 Code werden. Außer diesem gibt es weitere WebDAV-Angriffe, wie zum Beispiel den „Srch64K“ von Agobot [7], der eine feste URI der Größe 65.536 Byte im *SEARCH* /-Request sendet.

Auch die beiden älteren IIS Würmer, *Nimda* und *Code Red II*, finden sich nach wie vor. Ebenso tritt häufig ein „*OPTIONS* /“, gefolgt von einem „*PROPFIND*“-Request auf. Da beide Requests kurz sind, wirken sie wie Testpakete. Jedoch konnte bisher deren Intention nicht gänzlich geklärt werden. Man vermutet, dass es sich um eine Art Scanner handelt, der eine Liste von skriptfähigen Dateien durch das Senden von „*translate: f*“ [8] im Header des HTTP-Requests anfordert.

Anfrage	LBL	UW	Class A
Get	5,1%	2,9%	4,6%
GetSrch	5,2%	93,2%	93,4%
SrchAAA	84,2%	—	—
Srch64K	0,9%	1,1%	0,0%
CodeRed	0,6%	0,4%	0,5%
Nimda	0,2%	0,1%	0,2%
Other	3,8%	2,3%	1,3%

**Abbildung 6:** Anfragen auf Port 80 (Responder im UW und Class A antworteten nicht auf „*SEARCH* /“, um die großen „SrchAAA“-Requests zu vermeiden)

**TCP Port 135/1025 (DCE/RPC):** Über Port 135 ist der Pufferüberlauf-Angriff auf den *Microsoft-Windows-DCOM-RPC-Dienst*[9] möglich. Diese Schwachstelle nutzen unter anderem der *Welchia*- und der *Blaster*-Wurm aus. Während der erstere seltsamerweise nur im LBL-Netzwerk auftrat, wurde letzterer in allen drei untersuchten Netzwerken gesichtet.

**TCP Port 139/445 (CIFS):** Port 139 ist der „NetBIOS Session Service Port“ und wird auf Windowssystemen für CIFS (= Common Internet File System) [10] über NetBIOS verwendet. Port 445 ist dagegen für CIFS über TCP. Quellen, die sich gleichzeitig mit beiden Ports verbinden, bevorzugen Port 445 und beenden die Verbindung mit Port 139, wodurch viele leere Verbindungen entstehen. Da es zahlreiche Windows-Dienste gibt, die CIFS verwenden, gibt es eine große Auswahl an Angriffen auf diesen beiden Ports. Eine entsprechende Übersicht findet sich in *Abbildung 7*. Hauptsächlich handelt es sich dabei entweder um „Pufferüberlauf-RPC“-Angriffe oder um den Versuch, ausführbare Dateien auf den Zielrechner hochzuladen.

Angriff	LBL	UW	Class A
445/empty	2,4%	1,3%	0,9%
445/Nego	3,3%	2,4%	3,7%
445/Locator	72,7%	89,4%	89,3%
445/Samr-exe	11,6%	1,8%	1,1%
445/Samr	2,7%	0,8%	0,6%
445/Srvsvc	1,1%	0,4%	0,8%
445/Epmapper	0,8%	0,3%	0,0%
Other	5,4%	3,7%	3,5%

**Abbildung 7:** Angriffe auf Port 445

**TCP Port 6129 (Dameware):** Ein Administrations-Tool für Windowssysteme namens *Dameware Remote Control* verwendet diesen Port 6129. Frühe Versionen besitzen eine „buffer overrun“-Verletzbarkeit. Um diese auszunutzen, fordert der Quellrechner zuerst die Version des Betriebssystems durch eine 40 Byte lange Mitteilung an. Anschließend folgt der Angriff mit Hilfe einer 5.096 Bytes langen Anfrage, die den „buffer overrun“ zur Folge hat.

Während der Untersuchung wurden viele Verbindungen von Seiten der Hosts abgebrochen. Man vermutet, dass die Quellrechner gleichzeitig Anfragen an viele verschiedene Adressen schicken und diejenige angreifen, die als erste antwortet. Die anderen Verbindungen werden dann getrennt bzw. kommen gar nicht erst zustande.

**TCP Port 3127/2745/4751 (Virus Backdoors):** Diese Ports stellen die „Türen“ der Viren *MyDoom* und *Beagle* dar. Bei den meisten Verbindungen auf Port 3127 besteht der Header aus fünf festen Bytes, gefolgt von einer oder mehreren ausführbaren Windows-Datei-Uploads. Diese ausführbaren Programme scannen die TCP Ports 3127, 135 und 445.

Auf Port 2745 wird hauptsächlich die FTP-URL „ftp://bla:bla@<src-IP>:<port>/bot.exe \0“ übertragen, meistens nach zwei Testpaketen. Auf Port 4751 erhält man nach dem Header eine kryptische (=nicht interpretierbare) 24 Byte Nachricht und anschließend wird der Dialog beendet.

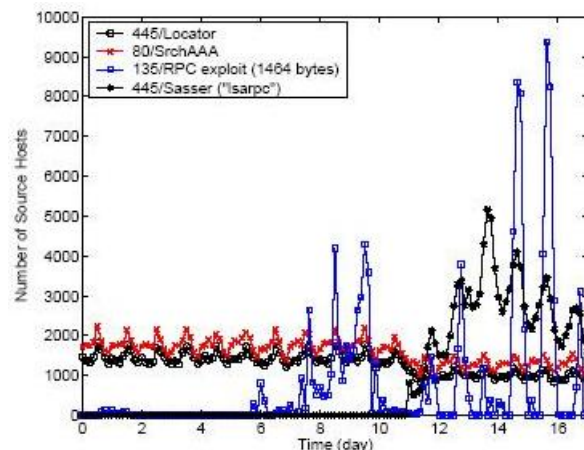


Abbildung 8: Angriffe im LBL-Netzwerk in der Zeit vom 20.04. bis 07.05.2004

**TCP Port 1981/4444/9996 (Folgeports):** Während einige Würmer wie beispielsweise *CodeRed* oder *Slammer* innerhalb einer übermittelten Codeanweisung vollständig enthalten sind, infizieren andere Würmer wie zum Beispiel *Blaster* oder *Sasser* ihre Opfer in zwei Schritten: das erste Stück Code sorgt dafür, dass auf einem bestimmten anderen Port auf weitere Anweisungen gewartet wird. Dieser Code wird dann anschließend angewiesen, ein Programm vom Host zu laden und auszuführen. Als ein Beispiel dienen folgende Zeilen, die häufig auf Port 4444, dem Folgeport für den *Blaster*-Wurm, zu sehen sind:

```
tftp -i <src-IP> GET msblast.exe
start msblast.exe
msblast.exe
```

Ähnliche Zeilen finden sich auf Port 1981 für *Agobot* und Port 9996 für *Sasser*, die jeweils eine Datei namens „bot.exe“ herunterladen und ausführen wollen. Alternativ zu der bisher genannten Möglichkeit, dass auf einem bestimmten Port auf weitere Anweisungen gewartet wird, gibt es noch die Variante, dass das zuerst übermittelte Stück Code die Verbindung trennt und sofort vom Zielrechner den Host auf einem beliebigen anderen Port anwählt (ähnlich einem Rückruf). Dadurch wird es erheblich schwerer, die weitere Kommunikation zu überwachen (oder zu unterbinden), da der genutzte Port nicht mehr bekannt ist.

## 4.2 Zeitliche Betrachtung von Angriffen

Abbildung 8 zeigt die Veränderung der Anzahl an Hosts über einen Zeitraum von 18 Tagen für vier verschiedene Angriffe. Dabei fällt zum einen die Stabilität und Ähnlichkeit der Anzahl an Quellen für „80/SrchAAA“ und „445/Locator“ auf. Dies ist nicht verwunderlich, da beide Angriffe sehr wahrscheinlich vom gleichen Wurm kommen. Zum anderen zeigen die übrigen beiden Angriffe *Exploit1464* und *Sasser* weitaus größere Ausschläge. Allen vier gemeinsam ist, dass die Zahl der Aktivitäten jeweils um 12:00 Uhr mittags Ortszeit ansteigt, was allerdings nur schwer erklärbar ist.

## 5 Charakteristik der Quellen

Im Gegensatz zu den bisherigen Betrachtungsweisen liegt das Augenmerk in diesem Kapitel auf den Quellen. Fasst man die verschiedenen Anfragen einer Host-IP zusammen, ergibt sich ein aussagekräftiges Gesamtbild, welches sich nach den drei Dimensionen 1) Ports, 2) Ziel-Netzwerke und 3) Zeit genauer untersuchen lässt, worüber im Folgenden auch berichtet wird. Dass einem Host durch DHCP im Lauf der Zeit eine andere IP-Adresse zugewiesen werden kann, ist bekannt, wird aber in diesem Fall aufgrund fehlender alternativer Messmöglichkeiten vernachlässigt.

### 5.1 Hostrechner und simultan oder sukzessiv kontaktierte Ports

Nur ausschließlich einen RPC-Angriff zu untersuchen, wird in der Regel den dahinterstehenden Wurm nicht enthüllen. Erst die Betrachtung der anderen Host-Ports macht die Identifizierung des Angreifers möglich. So wird in diesem Beispiel durch einen Folge-request auf Port 4444 mit „tftp msblast.exe“ klar, dass der vorangegangene RPC-Angriff durch den *Blaster*-Wurm ausgeführt wurde. Am häufigsten treten multi-port-requests bei Viren auf, die sich über NetBIOS/SMB(CIFS) verbreiten. Diese scannen oft gleichzeitig die Ports 139 und 445, da diese für den angestrebten Zweck alternativ verwendet werden können. Ein weiteres Beispiel ist beim Angriff auf die Microsoft DCE/RPC Schwachstelle [9] zu sehen: Der Angriff erfolgt sowohl über Port 135 als auch durch eine gleichzeitige Verbindung zur *Epmapper Pipe* über die Ports 139 und 445 ([1], Abschnitt 6.1).

### 5.2 Gleiche Quellen in unterschiedlichen Netzwerken

Eine Analyse der IP-Adressen in den drei Netzwerken und ein anschließender Abgleich führt zu dem in *Abbildung 9* sichtbaren Ergebnis, dass das LBL- und das UW-Netzwerk eine überraschend große Schnittmenge an Quellrechnern aufweisen: Knapp die Hälfte der Host-IPs im LBL-Netzwerk findet sich auch im UW-1-Netzwerk wieder. Deutlich geringer ist die Schnittmenge zwischen Class A und LBL, obwohl in das Class A-Netzwerk viel mehr Quell-IPs Pakete schicken als in das UW-1-Netzwerk. Durch eine weitere Un-

Angriff	LBL	UW-1	Class A	$LBL \cap UW$	$LBL \cap Class A$
Alle	31K	276K	582K	15K	6,5K
Srch+Loc	76%	85%	57%	75%	91%
Samr-exe	1.601	2.111	2.012	1.634	116
Witty	72	241	162	61	18

**Abbildung 9:** Quellen im Netzwerk-Vergleich

tersuchung wird bestätigt, dass die identifizierten Hosts in den verschiedenen Netzwerken tatsächlich auch die gleichen Aktivitäten unternehmen, abgesehen von einer Besonderheit: Neben einigen tausend SrchAAA- und Locator-Quellen in jeweils dem gleichen Netzwerk finden sich nahezu 2.000 SrchAAA-Host-IPs in einem Netzwerk und die dazugehörigen Locator-Host-IPs in einem anderen. Die Quellen scheinen offenbar zufällig zu entscheiden, ob sie entweder eine SrchAAA- oder eine Locator-Anfrage (aber nicht beides) zu einer bestimmten Zieladresse schicken.

## 6 Zusammenfassung

Seit einigen Jahren ist ein zunehmender Versand von nicht angeforderten Internetpaketen zu verzeichnen. Diese neue Dimension des Internet-Traffics, die sich durch eine komplexe Struktur und rasche Veränderungsgeschwindigkeit, einen hohen Automatisierungsgrad und häufig auch durch Bösartigkeit auszeichnet, ist bisher nicht ausreichend systematisch beobachtet und charakterisiert worden. Die oben erwähnte Studie [1] stellt einen ersten und wichtigen Schritt dar, das Phänomen der Hintergrundstrahlung detailliert zu untersuchen. Sie basiert auf der Analyse von vier ungenutzten Netzwerken im IPv4-Adressraum.

Durch die Entwicklung von Filtern und Respondern ist es gelungen, ankommende Pakete nicht nur zu messen, sondern diese sogar zu beantworten und auf diese Weise einen Dialog mit dem Host herzustellen. Dies ermöglicht eine deutlich genauere Charakterisierung der Anfrage als eine rein passive Messung. So konnten vielen TCP/SYN-Paketen konkrete Verursacher zugeordnet und eine detaillierte Betrachtung häufig genutzter Ports und der dort registrierbaren Angriffe ermöglicht werden. Auch über die Hosts konnte umfangreiches Datenmaterial gesammelt werden.

Diese Studie stellt - wie bereits erwähnt - nur einen Anfang dar, den ersten Schritt in eine bisher viel zu wenig erforschte Richtung. Künftig gilt es, die hier gesammelten Erkenntnisse als Grundlage für weitere und noch detailliertere Untersuchungen zu nehmen, um die Thematik der „Hintergrundstrahlung“ mit den damit verbundenen Gefahren den Usern zunehmend ins Bewusstsein zu bringen und letztlich auch in ihrer Komplexität weiter durchdringen zu können.

## Literatur

- [1] R.Pang, V.Yegneswaren, P.Barford, V.Paxson, L.Peterson:  
*Characteristics of Internet Background Radiation;*  
<http://www.imconf.net/imc-2004/papers/p27-pang.pdf>
  
- [2] W32 Sasser.Worm.  
<http://securityresponse.symantec.com/avcenter/venc/data/w32.sasser.worm.html>
  
- [3] W32 Welchia.Worm.  
<http://securityresponse.symantec.com/avcenter/venc/data/w32.welchia.worm.html>
  
- [4] D.Moore, V.Paxson, S.Savage, C.Shannon, S.Staniford, N.Weaver:  
*The spread of the sapphire/slammer worm.*  
<http://www.calda.org/outreach/papers/2003/sapphire/sapphire.html>
  
- [5] Microsoft Windows 2000 WebDAV buffer overflow vulnerability (MS03-001)  
<http://www.securityfocus.com/bid/7116>
  
- [6] C.Anley:  
*Creating arbitrary shellcode in unicode expanded strings*, January 2002  
<http://www.nextgenss.com/papers/unicodebo.pdf>
  
- [7] W32 Agobot IB.  
<http://www.sophos.com/virusinfo/analyses/trojagobotib.html>
  
- [8] Microsoft IIS 5.0 „translate: f“ source disclosure vulnerability, April 2004  
<http://www.securityfocus.com/bid/1578/discussion>
  
- [9] Microsoft Windows DCOM RPC interface buffer overrun vulnerability (MS03-026)  
<http://www.securityfocus.com/bid/8205>
  
- [10] Common Internet File System  
[http://www.snia.org/tech\\_activities/CIFS/CIFS-TR-1p00\\_FINAL.pdf](http://www.snia.org/tech_activities/CIFS/CIFS-TR-1p00_FINAL.pdf)