



Penetration Testing II  
Bachelor in Computer Science (BCS)

5. Semester

# Botnetze

- Funktion, Erkennung und Entfernung

von

Daniel Baier

---



## Gliederung

- Einführung
  - Definition
  - Übersicht von aktiven Botnetzen
  - Verwendungszweck
- Techniken
  - Infektion & Scanning
  - Kommunikation
  - Update
  - Verteidigung
- Erkennen und Entfernen
  - Infektionen von Bots erkennen und entfernen
  - Aufspüren von Botnetzen
- Ausblick



# Einführung



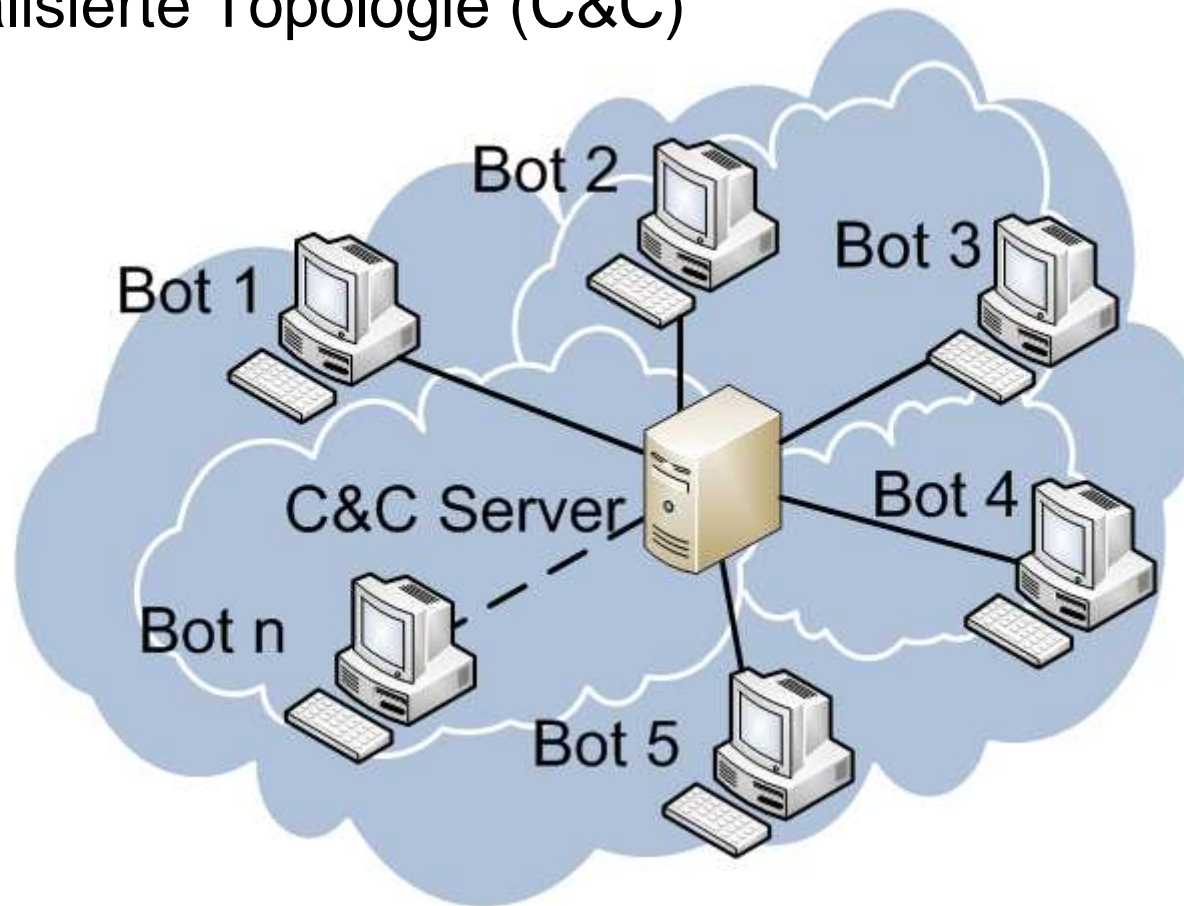
## Einführung: Definition

Bot nach Dunham und Melnick:

„Malicious code that acts like a remotely controlled „robot“ for an attacker, with both Trojan und worm capabilities. This term may refer to the code itself or to an infected computer, also known as a drone or zombie.“

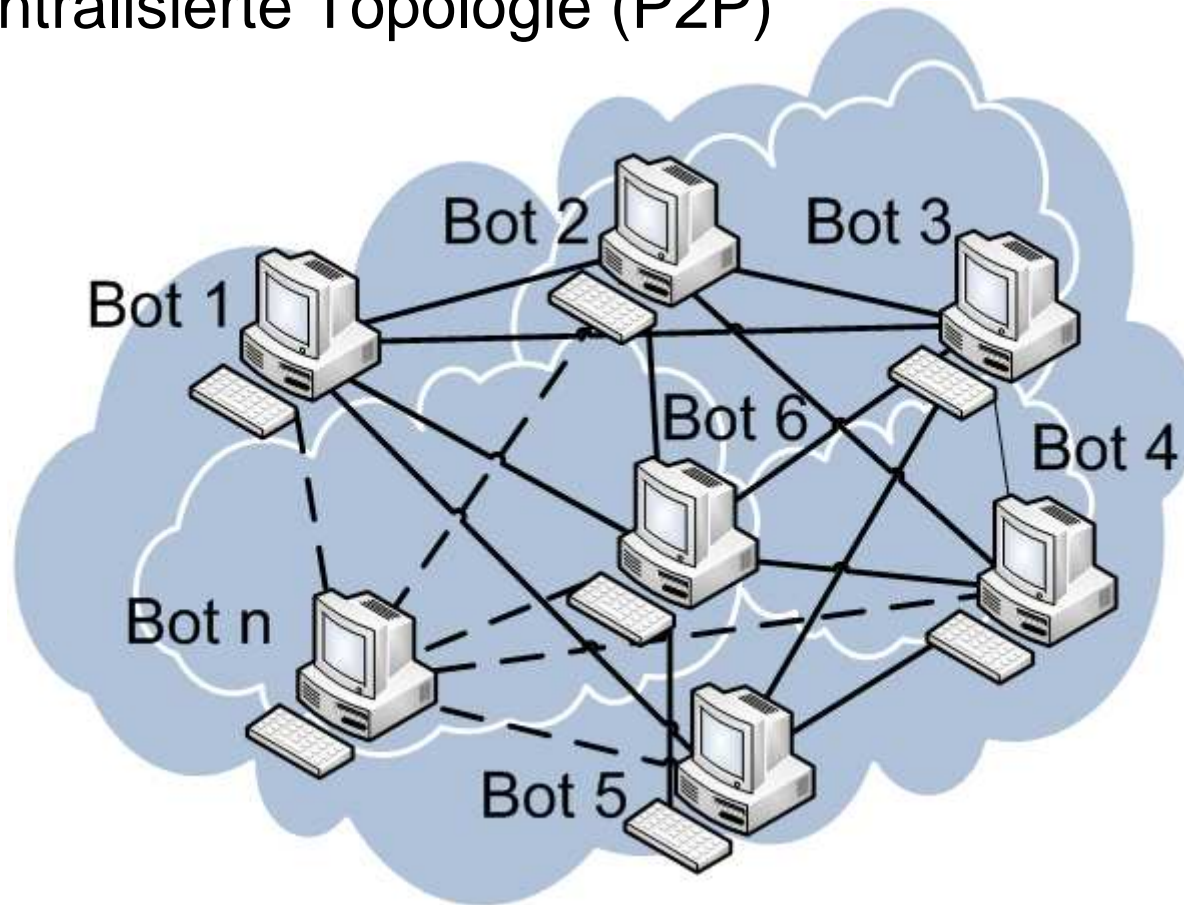
## Einführung: Definition

### Zentralisierte Topologie (C&C)



## Einführung: Definition

### Dezentralisierte Topologie (P2P)





## Einführung: Übersicht von aktiven Botnetzen

Name	Geschätzte Botzahl	Aliases
Conficker	9.000.000	DownUp, DownAndUp, DownAdUp, Kido
Rustock	1.200.000-2.000.000	RKRustok, Costrat
Cutwail	1.000.000-1.500.000	Pandex, Mutant
Grum	600.000-800.000	Tedroo
Bagle	600.000-800.000	?
Maazben	200.000-300.000	?
Festi	100.000-200.000	?
Kraken	80.000-120.000	Bobax
<i>Mega-D*</i>	<i>&lt; 100.000</i>	<i>Ozdok</i>
Xarvester	20.000-36.000	?

\* wurde 11.09 von FireEye übernommen

## Einführung: Übersicht von aktiven Botnetzen

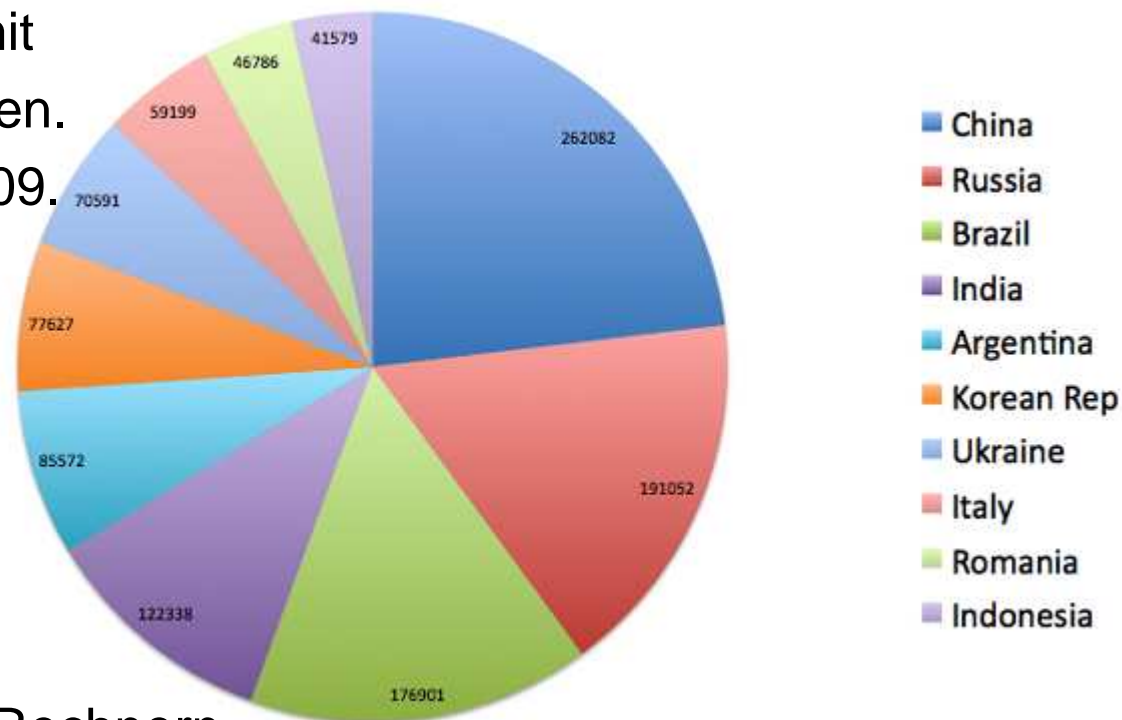
Bots die 2007 von der Shadowserver Foundation beobachtet wurden





## Einführung: Übersicht von aktiven Botnetzen

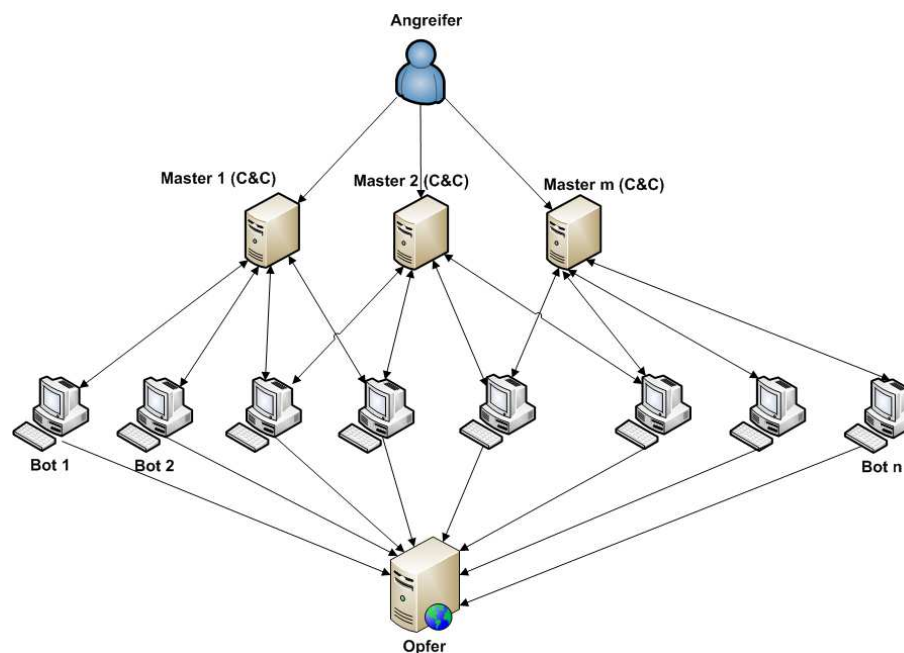
Die Top 10 Länder mit  
Conficker Infizierungen.  
Stand 29. Januar 2009.



Deutschland ist auf  
Platz 190 mit 23881  
Conficker infizierten Rechnern.

## Einführung: Verwendungszweck

- Data Mining
- DDoS
- Datendiebstahl
- Löschen von Hinweisen
- Proxy und Anonymisierer
- Ransomware
- Rekrutieren von Bots
- Reporting
- Spamming & Phishing
- Verteilung von illegalen Inhalten
- ...





# Techniken

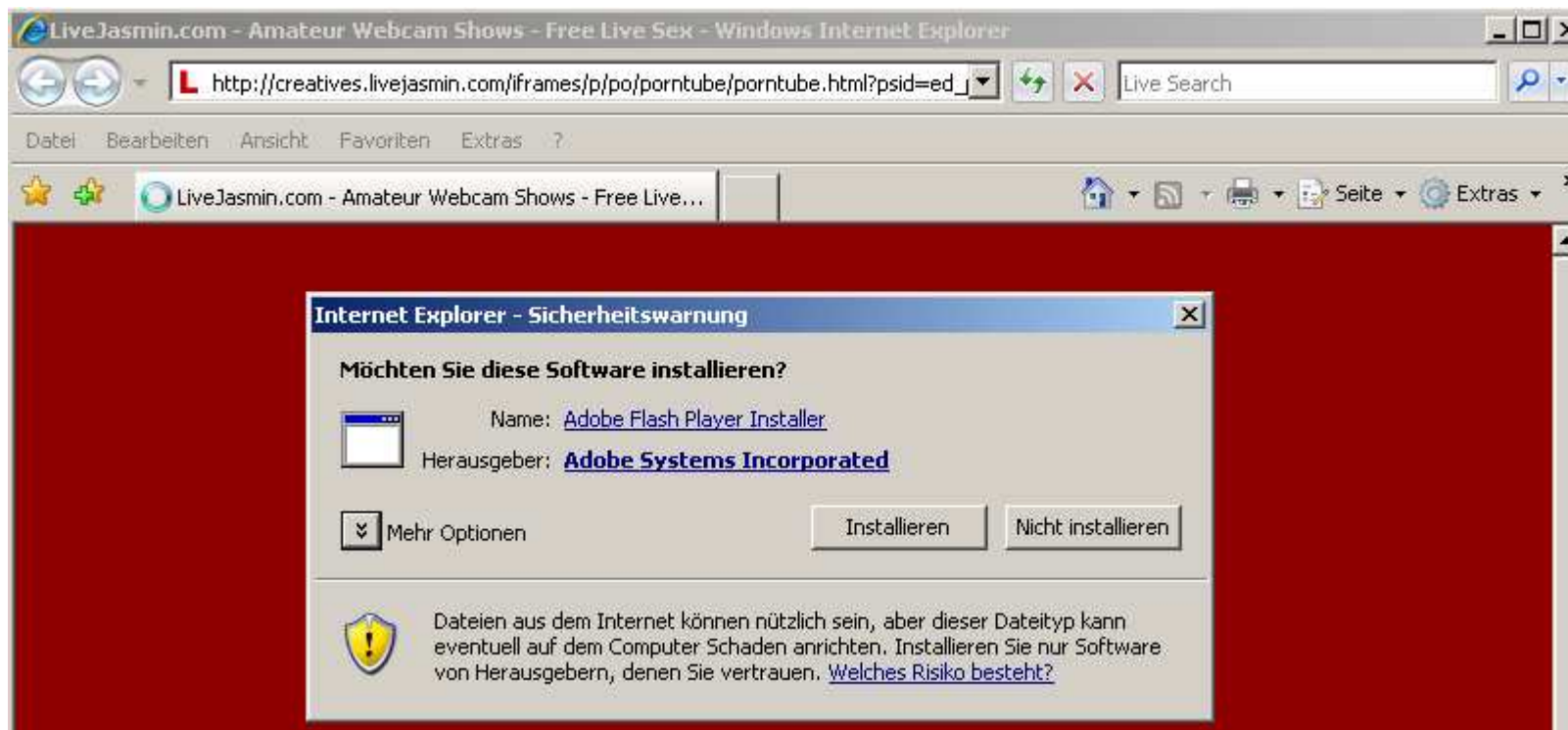
## Techniken: Infektion & Scanning

2 Klassen von Infektionen:

- Infektion mittels Social Engineering: Interagieren mit dem Benutzer direkt
  - ✓ Drive-by-download/Drive-by-infection
  - ✓ Benutzer wird zum Ausführen verleitet (z.B. E-Mail Anhang)
  
- Automatisierte Infektion: Benötigt keine menschliche Interaktion
  - ✓ Local Exploit
  - ✓ Remote Exploit

# Techniken: Infektion & Scanning

Beispiel für Social Engineering (Drive-by-download)





# Techniken: Infektion & Scanning

## Beispiel für Remote Exploit (MPack)

Server time/date snapshot: 1-Jan-2010 23:41:00  
127.0.0.1 (Unknown country)

**MPack v0.99 stats**

[Clear Stat](#)

Exploit group	Attacked total	Attacked uniq
IE XP ALL	1	1
QuickTime	0	0
Win2000	0	0
Firefox	0	0
Opera7	0	0

Traffic	total	uniq
Total traff	5	1
Exploited	0	0
Loads count	0	0
Loader response	0%	0%
<b>Efficiency</b>	<b>0%</b>	<b>0%</b>

Browser	total
---------	-------

Module	state
Statistic type	Textfile-based
User blocking	OFF
Country blocking	OFF
Visual base	javascript

(c) 2007 DreamCoders, k0d.biz  
MPack software is created solely for test purposes. You are prohibited to use it in conditions violating local or international laws. Authors hold no responsibility for any damage, d



# Techniken: Infektion & Scanning

## „Scanning-Engine“

- In jeden Bot implementiert
- Nur definierte Scannen
- Unterschiedliche Scanning-Strategien:
  - ✓ Hit-list Scanning
  - ✓ Topological Scanning
  - ✓ Flash Scanning
  - ✓ Permutation Scanning
  - ✓ Passive Scanning

## Techniken: Kommunikation

2 Klassen der Kommunikation:

- Verbindungsaufnahme (Nachhause-Telefonieren)
  - ✓ Verbindungsmethoden eines Bots zum C&C
  - ✓ Methoden des Bot-Herders um „Herde zu hüten“
  
- Kommunikationsprotokolle (Inter-Botnet Kommunikation)
  - ✓ Bots untereinander
  - ✓ Bots mit C&C



## Techniken: Kommunikation

### Verbindungsaufnahme (Nachhause-Telefonieren)

- Hart kodierte IP Adresse  
Bullet Proof Hosting → z.B. Russian Business Network
- DynDNS
- P2P → abhängig von P2P Technologie
- Fast-Flux Netzwerke

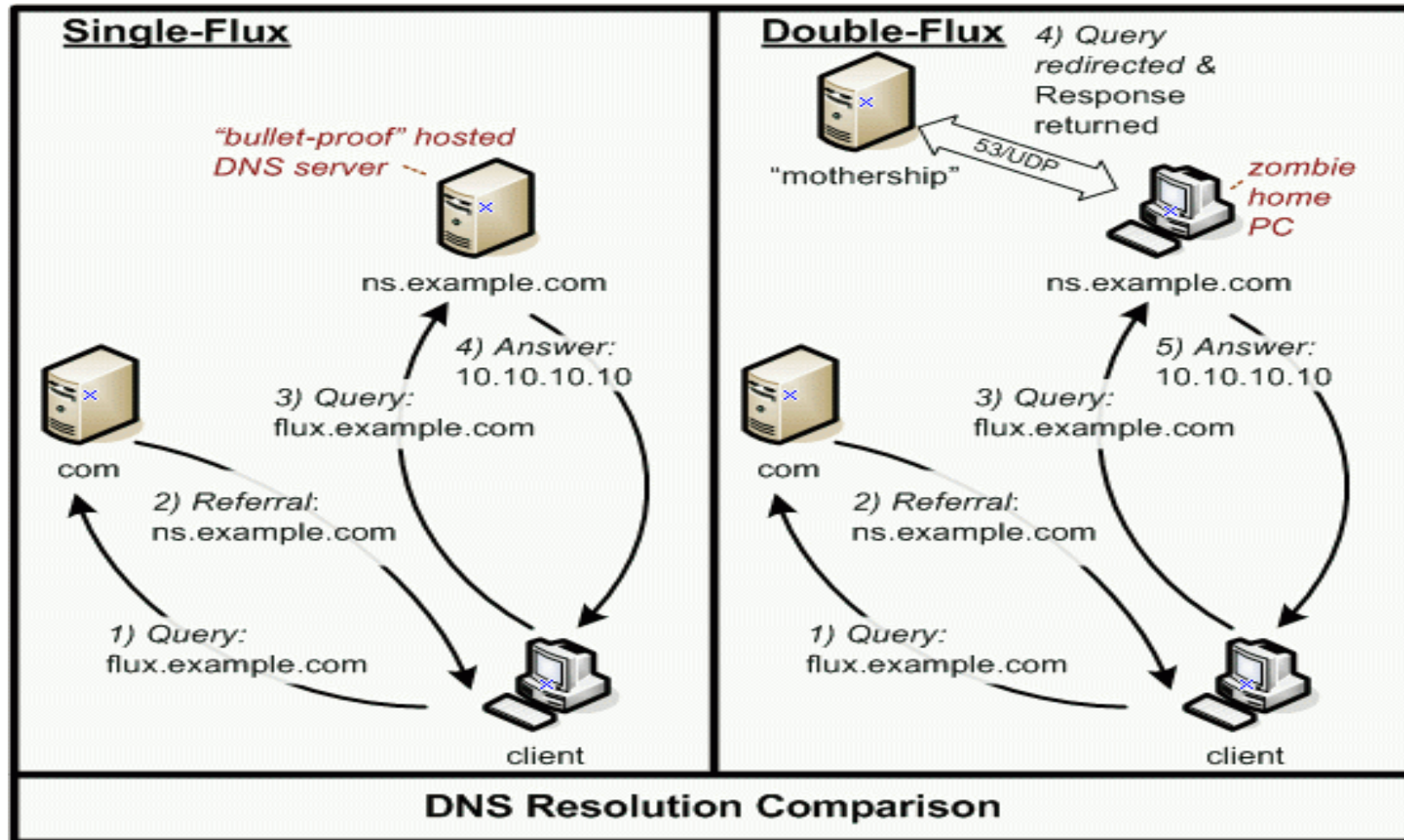


## Techniken: Kommunikation

- Fast-Flux Netzwerke
  - Single Flux Netzwerke:
    - ✓ Nur Änderung des DNS *A Resource Records*!
    - ✓ Steuerung durch TTL, z.B. alle 3 Min. neue IP
  - Double Flux Netzwerke:
    - ✓ Änderung des A und NS Resource Records
- Bsp. Single Flux:

Domain	Dateadded (UTC)	IP address	Hostname	AS number	Country	Counter
painkee.com	2009-12-31 13:54:11	79.114.22.215	79-114-22-215.rdsnet.ro	8708		1
painkee.com	2009-12-31 13:29:28	82.34.216.67	cpc3-gill8-0-0-cust66.basl.cable.virginmedia.com	5089		5
painkee.com	2009-12-31 13:28:26	217.255.197.22	pD9FFC516.dip.t-dialin.net	3320		7
painkee.com	2009-12-31 12:59:54	84.31.123.34	cp520492-a.dbsch1.nb.home.nl	9143		10

# Techniken: Kommunikation



## Techniken: Kommunikation

### Kommunikationsprotokolle (Inter-Botnet Kommunikation)

2 Arten

- ✓ Push:
  - Andauernde Verbindung zum C&C
  - C&C entscheidet Zeitpunkt neuer Kommandos
- ✓ Pull:
  - Gelegentliche Verbindung zum C&C
  - Bot erfragt neue Kommandos

## Techniken: Kommunikation

Protokoll	Push	Pull	Beispiel
HTTP		X	Twitter
IM	X		ICQ, Jabber
IRC	X		UnrealIRCd
P2P	X	X	Overnet (Kademlia)
VoIP	X	X	theoretisch
Andere	X	X	Eigenes oder ICMP





## Techniken: Update

- Patching (Bugfix) → beheben von Fehlern
- Ändern der Binärdatei
  - ✓ Folge: Signaturänderung
  - ✓ Ziel: Entdeckung durch Antiviren Programmen (AV) vermeiden
- Feature Adding
  - ✓ Exploit Archiv aktualisieren/vergrößern
  - ✓ Nachladen von neuen Mechanismen
  - ✓ Ändern der Kommunikation z.B. von IRC → IM

## Techniken: Verteidigung

- Beenden/Deaktivieren ungewollter Programme (z.B. AV)
- Verstecken (Rootkit Techniken)
- Angriffe auf Forscher (meist DDoS)

“When Researchers tried to understand the working of the Storm botnet DDoS Attacks were made on the hosts which they worked on.” [Krogoth 2008]

## Techniken: Verteidigung

Vereinfachtes Beispiel einer AV Detection anhand F-Secure's BugBear.B Analyse

```
void KillAV()
{
    #ifdev Win32
    const char AV_FilenamesToKill = { "_AVP32.EXE", "_AVPCC.EXE", "_AVPM.EXE",
                                     "ACKWIN32.EXE", "ANTI-TROJAN.EXE", "WFINDV32.EXE",
                                     [...],
                                     "ZONEALARM.EXE", NULL }
    for(int i = 0; AV_FilenamesToKill[i] != NULL ;++i)
        KillProcess(AV_FilenamesToKill[i]);

    #else
    KillProcess("tcpdump");
    KillProcess("ethereal");
    KillProcess("wireshark");
    #endif
}
```





# Erkennen und Entfernen

## Erkennen und Entfernen: Infektionen von Bots erkennen

2 Methoden:

- Lokale (local detection)
  - ✓ Manuelle Erkennung
  - ✓ AV
  - ✓ Host-Based Intrusion Detection System (HIDS)
  
- Netzwerk (network detection)
  - ✓ Klassische Netzwerk Analyse
  - ✓ Kommunikationsanalyse
  - ✓ Kommunikationssignatur Analyse



# Erkennen und Entfernen: Infektionen von Bots erkennen

## Kommunikationsanalyse am Beispiel von Wireshark

The screenshot shows the Wireshark interface with a list of network packets. The filter is set to 'http'. The list contains several entries, with the following details visible:

Time	Source	Destination	Protocol	Info
0.000321	...6.68	41.249.111.20	HTTP	HTTP/1.1 400 Bad Request (text/html)
0.001838	...6.68	41.201.40.60	HTTP	HTTP/1.1 400 Bad Request (text/html)
0.002621	...6.68	142.177.28.119	HTTP	HTTP/1.1 400 Bad Request (text/html)
0.003207	...6.68	213.60.214.245	HTTP	HTTP/1.1 400 Bad Request (text/html)
0.004107	...6.68	84.227.129.91	HTTP	HTTP/1.1 400 Bad Request (text/html)
0.004123	217.95.191.243	...6.80	HTTP	GET /new_design/images/content_footer_bg.jpg HTTP/1.1
0.004212	...6.68	77.250.255.68	HTTP	HTTP/1.1 400 Bad Request (text/html)
0.006214	89.61.199.84	...6.80	HTTP	GET /new_design/images/statusicon/post_old.gif HTTP/1.1
0.008621	...6.68	91.6.236.115	HTTP	HTTP/1.1 400 Bad Request (text/html)
0.009072	...6.68	89.140.175.255	HTTP	HTTP/1.1 400 Bad Request (text/html)
0.009697	...6.68	41.209.135.19	HTTP	HTTP/1.1 400 Bad Request (text/html)
0.010321	...6.68	89.140.175.255	HTTP	HTTP/1.1 400 Bad Request (text/html)
0.012342	91.0.219.188	...6.2	HTTP	GET /www/delivery/ajs.php?zoneid=74&cb=16016281827&loc=

Below the list, the packet details pane shows the following information for the selected packet:

- Internet Protocol Version 4, Src: HewlettP\_c5:40:16 (00:1f:29:c5:40:16), Dst: JuniperN\_cd:c8:29 (00:1d:b5:cd:c8:29)
- Transmission Control Protocol, Src: ...6.68 (...6.68), Dst: 213.60.214.245 (213.60.214.245)
- Hypertext Transfer Protocol, Src Port: http (80), Dst Port: megardsvr-port (3571), Seq: 1, Ack: 1, Len: 392
- Text Transfer Protocol
- HTTP/1.1 400 Bad Request\r\n

## Erkennen und Entfernen: Infektionen von Bots erkennen

- Werkzeuge zum Entfernen von Bots:
  - McAfee Stinger [[Link](#)]
  - Microsoft Windows Defender [[Link](#)]
  - Spybot – Search & Destroy [[Link](#)]
  - TrojanHunter [[Link](#)]
  - SwatIt [[Link](#)]
  - Trojan Defence Suite [[Link](#)]
  
- Dennoch:
  - Vertrauenswürdigkeit ?
  - Neuinstallation!

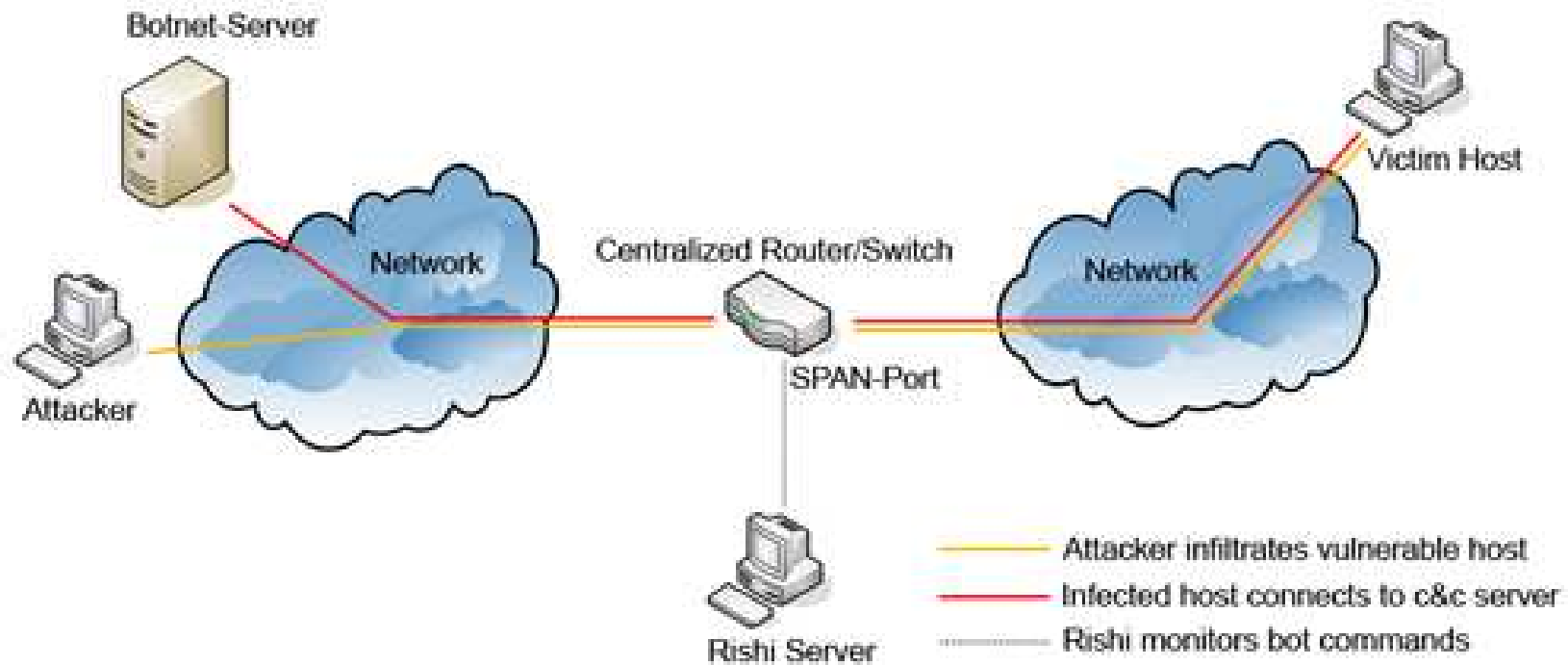


## Erkennen und Entfernen: Aufspüren von Botnetzen

- Einige Botnet-Detection Frameworks
  - IRCd, öffentlich (z.B. DDD + GnuWorld)
  - IRCd, privat (z.B. Rishi an der RWTH Aachen)
  - E-Mail (CipherTrust ZombieMeter; Spamhaus XBL; jeder Andere)
  - Diverses (Darknet, Network Telescope o. Internet Motion Sensor)
  - Honeypots (z.B. honeyd oder Glastopf)
  - AV/Managed network sensing (Sophos)
- Problem: Teure Überwachung

## Erkennen und Entfernen: Aufspüren von Botnetzen

IRC-Botnetz-Erkennung an der RWTH Aachen mit Rishi



## Erkennen und Entfernen: Aufspüren von Botnetzen

Alternative: DynDNS-Based Detection nach Dagon

➤ 3LD. SLD. TLD  
↓ ↓ ↓  
botnet.example.com

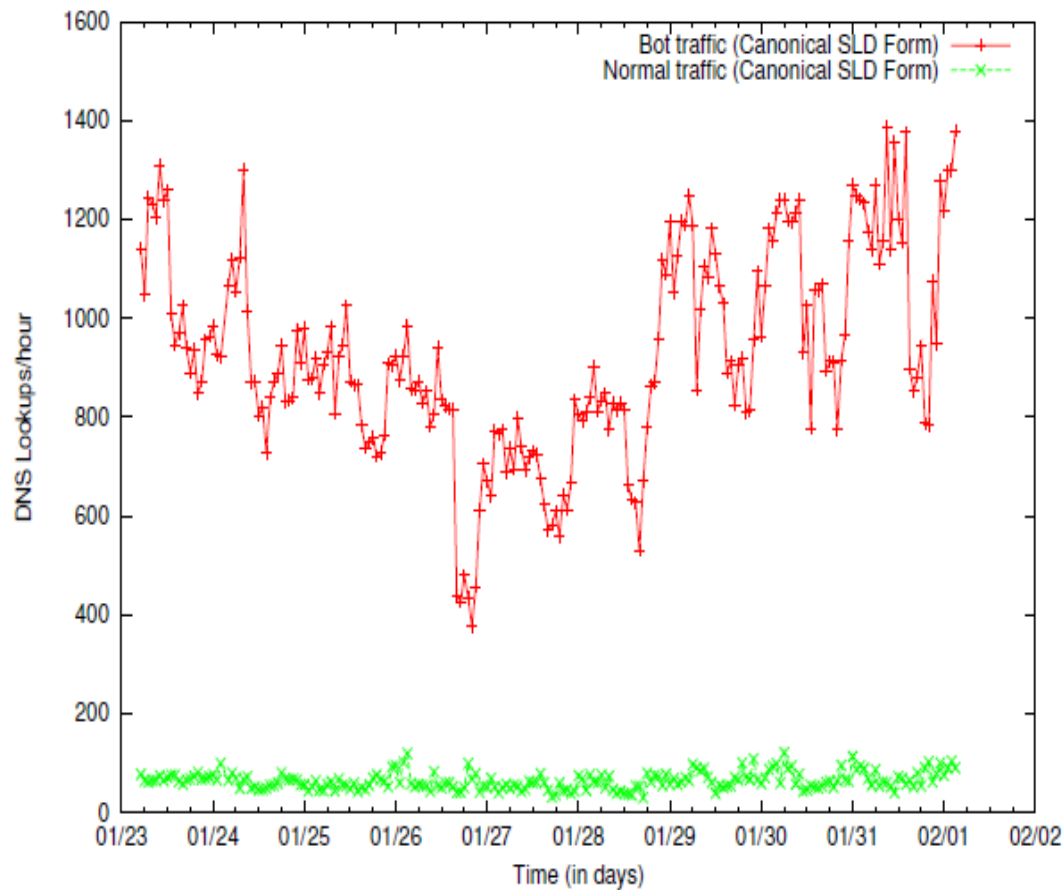
➤ Canonical DNS Request Rate:

$$C_{SLD_i} = R_{SLD_i} + \sum_{j=1}^{|SLD_i|} R_{3LD_j}$$

➤  $\triangleq$  Aufsummierung der Kinder SLD<sub>i</sub>

# Erkennen und Entfernen: Aufspüren von Botnetzen

Als DynDNS Kunden neigen Botnetze Subdomains zu nutzen



SLD/3LD-Kennzahlen zur Identifikation von Botnetz-Verkehr





# Ausblick

## Ausblick

Botnetzen nach wie vor ein aktuelles Thema:

- Malware as Service (Amazon EC2; Google App Engine)
- PC nicht mehr einzige betroffene Architektur
- 23.11.2009 erstes iPhone Botnet (iKee.B)
- Errichtung eines „Callcenters zur Bekämpfung von Botnetzen“ von BSI und eco

iKee.A  
Wurm:





**Haben Sie noch Fragen?**

**Vielen Dank für Ihre Aufmerksamkeit!**