Botnetzmonitoring – Waledac

Ben Stock

Universität Mannheim

14. September 2009

Übersicht

UNIVERSITÄT MANNHEIM

Übersicht

UNIVERSITÄT MANNHEIM

Übersicht

UNIVERSITÄT MANNHEIM

Übersicht

UNIVERSITÄT MANNHEIM

Übersicht

UNIVERSITÄT MANNHEIM

Was ist Waledac?

Einige Buzzwords

- Spambot
- Peer-to-Peer
- Verschlüsselte Kommunikation

UNIVERSITÄT MANNHEIM

Was ist Waledac?

Einige Buzzwords

- Spambot
- Peer-to-Peer
- Verschlüsselte Kommunikation

UNIVERSITÄT MANNHEIM

Was ist Waledac?

Einige Buzzwords

- Spambot
- Peer-to-Peer
- Verschlüsselte Kommunikation

UNIVERSITÄT MANNHEIM

Was interessiert uns an Waledac?

- Anzahl der Bots
- weltweite Verteilung
- Spamerfolg
- Schwachstellen?
- Storm Nachfolger?

UNIVERSITÄT MANNHEIM

Was interessiert uns an Waledac?

- Anzahl der Bots
- weltweite Verteilung
- Spamerfolg
- Schwachstellen?
- Storm Nachfolger?

UNIVERSITÄT MANNHEIM

Was interessiert uns an Waledac?

- Anzahl der Bots
- weltweite Verteilung
- Spamerfolg
- Schwachstellen?
- Storm Nachfolger?

UNIVERSITÄT MANNHEIM

Was interessiert uns an Waledac?

- Anzahl der Bots
- weltweite Verteilung
- Spamerfolg
- Schwachstellen?
- Storm Nachfolger?

UNIVERSITÄT MANNHEIM

Was interessiert uns an Waledac?

- Anzahl der Bots
- weltweite Verteilung
- Spamerfolg
- Schwachstellen?
- Storm Nachfolger?

UNIVERSITÄT MANNHEIM

Aufbau des Netzwerkes

- mindestens 3 Ebenen
  - unterste Ebene: **Spammer**
  - nächste Ebene: **Repeater** (auch Fast-Flux-Agents)
  - dritte Ebene: **Backend Server**
  - vierte Ebene: **Upper Tier Server**
- Nur Spammer und Repeater echtes P2P

UNIVERSITÄT MANNHEIM

Aufbau des Netzwerkes

- mindestens 3 Ebenen
  - unterste Ebene: **Spammer**
  - nächste Ebene: **Repeater** (auch Fast-Flux-Agents)
  - dritte Ebene: **Backend Server**
  - vierte Ebene: **Upper Tier Server**
- Nur Spammer und Repeater echtes P2P

UNIVERSITÄT MANNHEIM

Aufbau des Netzwerkes

- mindestens 3 Ebenen
  - unterste Ebene: **Spammer**
  - nächste Ebene: **Repeater** (auch Fast-Flux-Agents)
  - dritte Ebene: **Backend Server**
  - vierte Ebene: **Upper Tier Server**
- Nur Spammer und Repeater echtes P2P

UNIVERSITÄT MANNHEIM

Aufbau des Netzwerkes

- mindestens 3 Ebenen
  - unterste Ebene: **Spammer**
  - nächste Ebene: **Repeater** (auch Fast-Flux-Agents)
  - dritte Ebene: **Backend Server**
  - vierte Ebene: **Upper Tier Server**
- Nur Spammer und Repeater echtes P2P

UNIVERSITÄT MANNHEIM

Aufbau des Netzwerkes

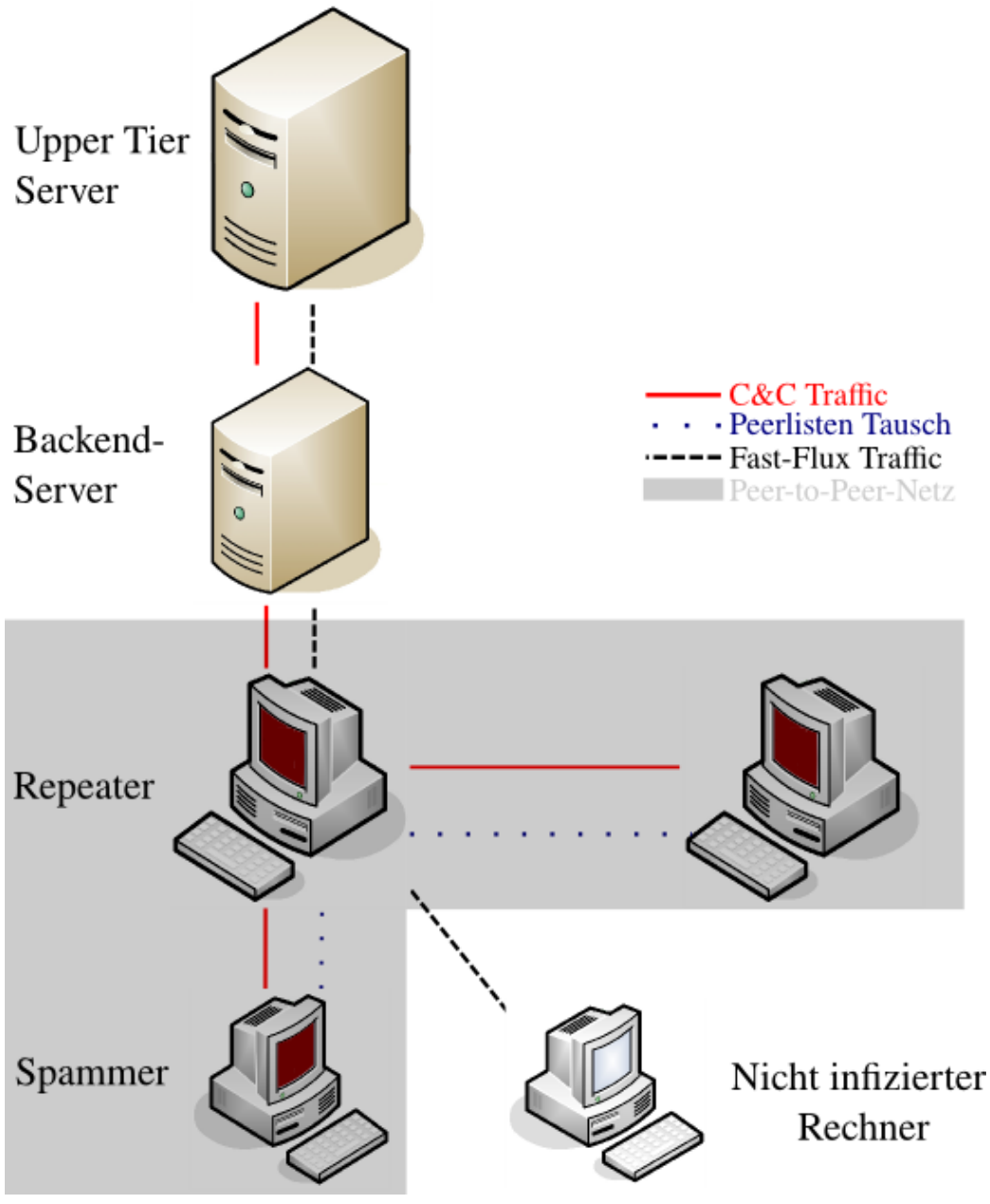
- mindestens 3 Ebenen
  - unterste Ebene: **Spammer**
  - nächste Ebene: **Repeater** (auch Fast-Flux-Agents)
  - dritte Ebene: **Backend Server**
  - vierte Ebene: **Upper Tier Server**
- Nur Spammer und Repeater echtes P2P

UNIVERSITÄT MANNHEIM

Aufbau des Netzwerkes

- mindestens 3 Ebenen
  - unterste Ebene: **Spammer**
  - nächste Ebene: **Repeater** (auch Fast-Flux-Agents)
  - dritte Ebene: **Backend Server**
  - vierte Ebene: **Upper Tier Server**
- Nur Spammer und Repeater echtes P2P

UNIVERSITÄT MANNHEIM


Upper Tier
Server
Backend-
Server
C&C Traffic
Peerlisten Tausch
Fast-Flux Traffic
Peer-to-Peer-Netz
Repeater
Spammer
Nicht infizierter
Rechner

Benutzte Technologien

- hybrides P2P-Netz als Topologie
- XML für Kommunikation
- Bzip2 zur Komprimierung
- RSA und AES zur Verschlüsselung
- HTTP als "unauffälliger" Kommunikationskanal
- Registry als Speicherort für z.B. Peerlisten und ID

UNIVERSITÄT MANNHEIM

Benutzte Technologien

- hybrides P2P-Netz als Topologie
- XML für Kommunikation
- Bzip2 zur Komprimierung
- RSA und AES zur Verschlüsselung
- HTTP als "unauffälliger" Kommunikationskanal
- Registry als Speicherort für z.B. Peerlisten und ID

UNIVERSITÄT MANNHEIM

Benutzte Technologien

- hybrides P2P-Netz als Topologie
- XML für Kommunikation
- Bzip2 zur Komprimierung
- RSA und AES zur Verschlüsselung
- HTTP als "unauffälliger" Kommunikationskanal
- Registry als Speicherort für z.B. Peerlisten und ID

UNIVERSITÄT MANNHEIM

Benutzte Technologien

- hybrides P2P-Netz als Topologie
- XML für Kommunikation
- Bzip2 zur Komprimierung
- RSA und AES zur Verschlüsselung
- HTTP als "unauffälliger" Kommunikationskanal
- Registry als Speicherort für z.B. Peerlisten und ID

UNIVERSITÄT MANNHEIM

Benutzte Technologien

- hybrides P2P-Netz als Topologie
- XML für Kommunikation
- Bzip2 zur Komprimierung
- RSA und AES zur Verschlüsselung
- HTTP als "unauffälliger" Kommunikationskanal
- Registry als Speicherort für z.B. Peerlisten und ID

UNIVERSITÄT MANNHEIM

Benutzte Technologien

- hybrides P2P-Netz als Topologie
- XML für Kommunikation
- Bzip2 zur Komprimierung
- RSA und AES zur Verschlüsselung
- HTTP als "unauffälliger" Kommunikationskanal
- Registry als Speicherort für z.B. Peerlisten und ID

UNIVERSITÄT MANNHEIM

Funktionen von Waledac

- Spam-Bot
  - intelligentes Templatesystem
  - Spamreports nach Ausführung
- Fast-Flux-Agent
  - primär für Verbreitung genutzt
  - theoretisch auch Phishing o.ä. möglich
- DDoS-Bot
  - implementiert, aber nicht beobachtet
- Harvesting von Zugangsdaten
- Harvesting von E-Mail-Adressen
  - werden ebenfalls im XML-Format an Botmaster geschickt

UNIVERSITÄT MANNHEIM

Funktionen von Waledac

- Spam-Bot
  - intelligentes Templatesystem
  - Spamreports nach Ausführung
- Fast-Flux-Agent
  - primär für Verbreitung genutzt
  - theoretisch auch Phishing o.ä. möglich
- DDoS-Bot
  - implementiert, aber nicht beobachtet
- Harvesting von Zugangsdaten
- Harvesting von E-Mail-Adressen
  - werden ebenfalls im XML-Format an Botmaster geschickt

UNIVERSITÄT MANNHEIM

Funktionen von Waledac

- Spam-Bot
  - intelligentes Templatesystem
  - Spamreports nach Ausführung
- Fast-Flux-Agent
  - primär für Verbreitung genutzt
  - theoretisch auch Phishing o.ä. möglich
- DDoS-Bot
  - implementiert, aber nicht beobachtet
- Harvesting von Zugangsdaten
- Harvesting von E-Mail-Adressen
  - werden ebenfalls im XML-Format an Botmaster geschickt

UNIVERSITÄT MANNHEIM

Funktionen von Waledac

- Spam-Bot
  - intelligentes Templatesystem
  - Spamreports nach Ausführung
- Fast-Flux-Agent
  - primär für Verbreitung genutzt
  - theoretisch auch Phishing o.ä. möglich
- DDoS-Bot
  - implementiert, aber nicht beobachtet
- Harvesting von Zugangsdaten
- Harvesting von E-Mail-Adressen
  - werden ebenfalls im XML-Format an Botmaster geschickt

UNIVERSITÄT MANNHEIM

Funktionen von Waledac

- Spam-Bot
  - intelligentes Templatesystem
  - Spamreports nach Ausführung
- Fast-Flux-Agent
  - primär für Verbreitung genutzt
  - theoretisch auch Phishing o.ä. möglich
- DDoS-Bot
  - implementiert, aber nicht beobachtet
- Harvesting von Zugangsdaten
- Harvesting von E-Mail-Adressen
  - werden ebenfalls im XML-Format an Botmaster geschickt

UNIVERSITÄT MANNHEIM

Funktionen von Waledac

- Spam-Bot
  - intelligentes Templatesystem
  - Spamreports nach Ausführung
- Fast-Flux-Agent
  - primär für Verbreitung genutzt
  - theoretisch auch Phishing o.ä. möglich
- DDoS-Bot
  - implementiert, aber nicht beobachtet
- Harvesting von Zugangsdaten
- Harvesting von E-Mail-Adressen
  - werden ebenfalls im XML-Format an Botmaster geschickt

UNIVERSITÄT MANNHEIM

Funktionen von Waledac

- Spam-Bot
  - intelligentes Templatesystem
  - Spamreports nach Ausführung
- Fast-Flux-Agent
  - primär für Verbreitung genutzt
  - theoretisch auch Phishing o.ä. möglich
- DDoS-Bot
  - implementiert, aber nicht beobachtet
- Harvesting von Zugangsdaten
- Harvesting von E-Mail-Adressen
  - werden ebenfalls im XML-Format an Botmaster geschickt

UNIVERSITÄT MANNHEIM

Funktionen von Waledac

- Spam-Bot
  - intelligentes Templatesystem
  - Spamreports nach Ausführung
- Fast-Flux-Agent
  - primär für Verbreitung genutzt
  - theoretisch auch Phishing o.ä. möglich
- DDoS-Bot
  - implementiert, aber nicht beobachtet
- Harvesting von Zugangsdaten
- Harvesting von E-Mail-Adressen
  - werden ebenfalls im XML-Format an Botmaster geschickt

UNIVERSITÄT MANNHEIM

Funktionen von Waledac

- Spam-Bot
  - intelligentes Templatesystem
  - Spamreports nach Ausführung
- Fast-Flux-Agent
  - primär für Verbreitung genutzt
  - theoretisch auch Phishing o.ä. möglich
- DDoS-Bot
  - implementiert, aber nicht beobachtet
- Harvesting von Zugangsdaten
- Harvesting von E-Mail-Adressen
  - werden ebenfalls im XML-Format an Botmaster geschickt

UNIVERSITÄT MANNHEIM

Funktionen von Waledac

- Spam-Bot
  - intelligentes Templatesystem
  - Spamreports nach Ausführung
- Fast-Flux-Agent
  - primär für Verbreitung genutzt
  - theoretisch auch Phishing o.ä. möglich
- DDoS-Bot
  - implementiert, aber nicht beobachtet
- Harvesting von Zugangsdaten
- Harvesting von E-Mail-Adressen
  - werden ebenfalls im XML-Format an Botmaster geschickt

UNIVERSITÄT MANNHEIM

Funktionen von Waledac

- Spam-Bot
  - intelligentes Templatesystem
  - Spamreports nach Ausführung
- Fast-Flux-Agent
  - primär für Verbreitung genutzt
  - theoretisch auch Phishing o.ä. möglich
- DDoS-Bot
  - implementiert, aber nicht beobachtet
- Harvesting von Zugangsdaten
- Harvesting von E-Mail-Adressen
  - werden ebenfalls im XML-Format an Botmaster geschickt

UNIVERSITÄT MANNHEIM

Entwickelte Werkzeuge

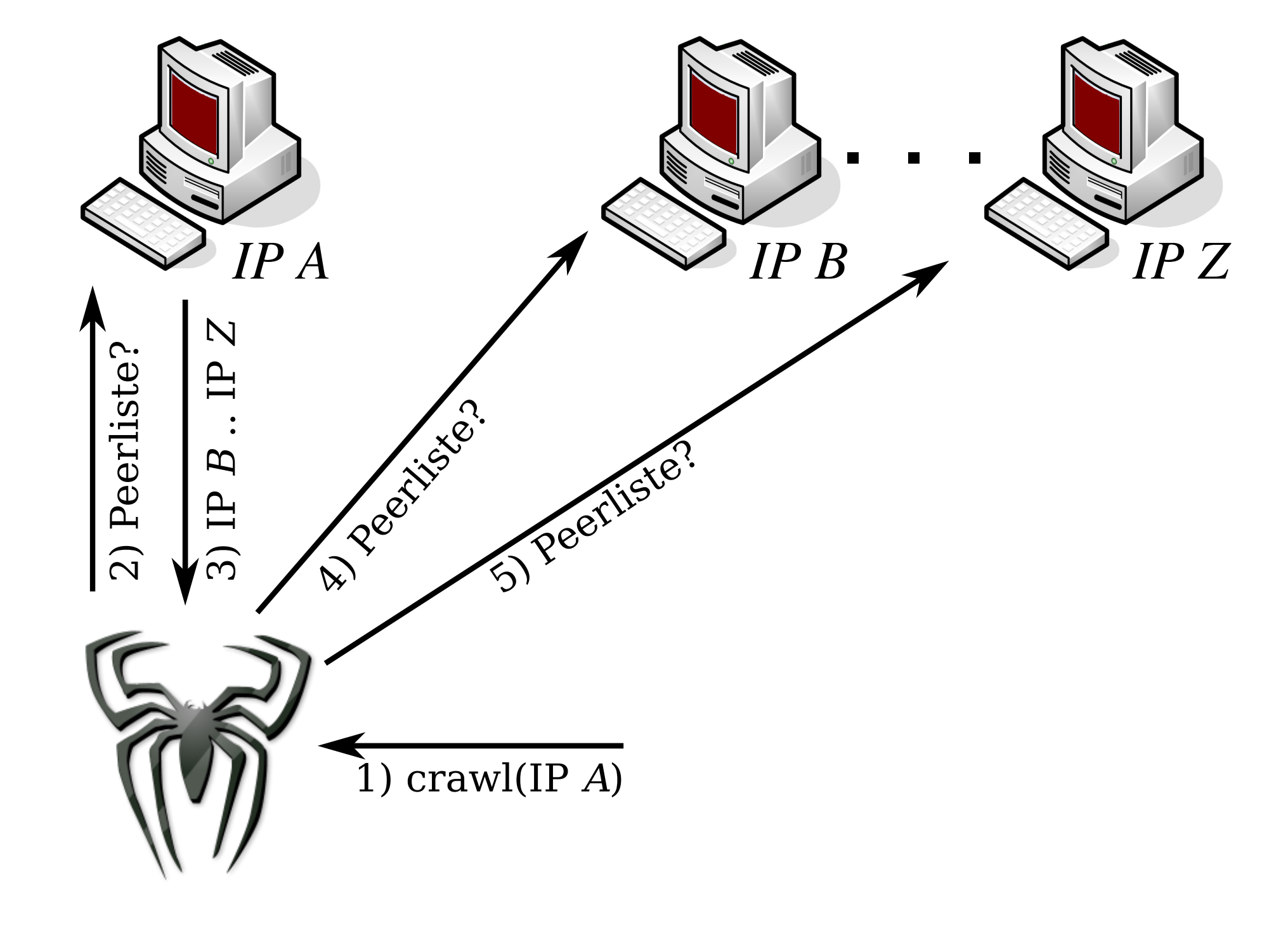
- **Repeater Crawler**: Suchen und Finden aller Repeater im Waledac-Botnetz
- **Walowdac**: Klon von Waledac, nur Kommunikationsfeatures

UNIVERSITÄT MANNHEIM

Entwickelte Werkzeuge

- **Repeater Crawler**: Suchen und Finden aller Repeater im Waledac-Botnetz
- **Walowdac**: Klon von Waledac, nur Kommunikationsfeatures

UNIVERSITÄT MANNHEIM


IP A
IP B
IP Z
2) Peerliste?
3) IP B .. IP Z
4) Peerliste?
5) Peerliste?
1) crawl(IP A)

Walowdac

- entwickelt in Python
- implementiert Kommunikationsfeatures von Waledac
- loggt Verbindungen und zusätzlich Informationen (Kampagne, Spam-Statistiken, ..)
- $\longrightarrow$ wirkt wie ein valider Repeater

UNIVERSITÄT MANNHEIM

Walowdac

- entwickelt in Python
- implementiert Kommunikationsfeatures von Waledac
- loggt Verbindungen und zusätzlich Informationen (Kampagne, Spam-Statistiken, ..)
- $\longrightarrow$ wirkt wie ein valider Repeater

UNIVERSITÄT MANNHEIM

Walowdac

- entwickelt in Python
- implementiert Kommunikationsfeatures von Waledac
- loggt Verbindungen und zusätzlich Informationen (Kampagne, Spam-Statistiken, ..)
- $\longrightarrow$ wirkt wie ein valider Repeater

UNIVERSITÄT MANNHEIM

Walowdac

- entwickelt in Python
- implementiert Kommunikationsfeatures von Waledac
- loggt Verbindungen und zusätzlich Informationen (Kampagne, Spam-Statistiken, ..)
- $\longrightarrow$ wirkt wie ein valider Repeater

UNIVERSITÄT MANNHEIM

Vorgehensweise bei der Messung

Idee

- Bringe möglichst viele Bots dazu, zum Walowdac zu verbinden
- Dazu: propagiere Adressen unter den Repeatern, die wiederrum die diese an Spammer entsprechend weiterleiten

Propagierung

- Waledac prüft nicht, ob IP bereits in der Liste ist
- ausschließlich ID ist Kriterium
  - wenige IPs, verschiedene IDs benutzen
  - viele Einträge, die auf Walowdac zeigen
- Repeater Crawler sendet Walowdac-Adressen
- Walowdac selbst antwortet mit Walowdac-Adressen

UNIVERSITÄT MANNHEIM

Vorgehensweise bei der Messung

Idee

- Bringe möglichst viele Bots dazu, zum Walowdac zu verbinden
- Dazu: propagiere Adressen unter den Repeatern, die wiederrum die diese an Spammer entsprechend weiterleiten

Propagierung

- Waledac prüft nicht, ob IP bereits in der Liste ist
- ausschließlich ID ist Kriterium
  - wenige IPs, verschiedene IDs benutzen
  - viele Einträge, die auf Walowdac zeigen
- Repeater Crawler sendet Walowdac-Adressen
- Walowdac selbst antwortet mit Walowdac-Adressen

UNIVERSITÄT MANNHEIM

Vorgehensweise bei der Messung

Idee

- Bringe möglichst viele Bots dazu, zum Walowdac zu verbinden
- Dazu: propagiere Adressen unter den Repeatern, die wiederrum die diese an Spammer entsprechend weiterleiten

Propagierung

- Waledac prüft nicht, ob IP bereits in der Liste ist
- ausschließlich ID ist Kriterium
  - wenige IPs, verschiedene IDs benutzen
  - viele Einträge, die auf Walowdac zeigen
- Repeater Crawler sendet Walowdac-Adressen
- Walowdac selbst antwortet mit Walowdac-Adressen

UNIVERSITÄT MANNHEIM

Vorgehensweise bei der Messung

Idee

- Bringe möglichst viele Bots dazu, zum Walowdac zu verbinden
- Dazu: propagiere Adressen unter den Repeatern, die wiederrum die diese an Spammer entsprechend weiterleiten

Propagierung

- Waledac prüft nicht, ob IP bereits in der Liste ist
- ausschließlich ID ist Kriterium
  - wenige IPs, verschiedene IDs benutzen
  - viele Einträge, die auf Walowdac zeigen
- Repeater Crawler sendet Walowdac-Adressen
- Walowdac selbst antwortet mit Walowdac-Adressen

UNIVERSITÄT MANNHEIM

Vorgehensweise bei der Messung

Idee

- Bringe möglichst viele Bots dazu, zum Walowdac zu verbinden
- Dazu: propagiere Adressen unter den Repeatern, die wiederrum die diese an Spammer entsprechend weiterleiten

Propagierung

- Waledac prüft nicht, ob IP bereits in der Liste ist
- ausschließlich ID ist Kriterium
  - wenige IPs, verschiedene IDs benutzen
  - viele Einträge, die auf Walowdac zeigen
- Repeater Crawler sendet Walowdac-Adressen
- Walowdac selbst antwortet mit Walowdac-Adressen

UNIVERSITÄT MANNHEIM

Vorgehensweise bei der Messung

Idee

- Bringe möglichst viele Bots dazu, zum Walowdac zu verbinden
- Dazu: propagiere Adressen unter den Repeatern, die wiederrum die diese an Spammer entsprechend weiterleiten

Propagierung

- Waledac prüft nicht, ob IP bereits in der Liste ist
- ausschließlich ID ist Kriterium
  - wenige IPs, verschiedene IDs benutzen
  - viele Einträge, die auf Walowdac zeigen
- Repeater Crawler sendet Walowdac-Adressen
- Walowdac selbst antwortet mit Walowdac-Adressen

UNIVERSITÄT MANNHEIM

Vorgehensweise bei der Messung

Idee

- Bringe möglichst viele Bots dazu, zum Walowdac zu verbinden
- Dazu: propagiere Adressen unter den Repeatern, die wiederrum die diese an Spammer entsprechend weiterleiten

Propagierung

- Waledac prüft nicht, ob IP bereits in der Liste ist
- ausschließlich ID ist Kriterium
  - wenige IPs, verschiedene IDs benutzen
  - viele Einträge, die auf Walowdac zeigen
- Repeater Crawler sendet Walowdac-Adressen
- Walowdac selbst antwortet mit Walowdac-Adressen

UNIVERSITÄT MANNHEIM

Vorgehensweise bei der Messung

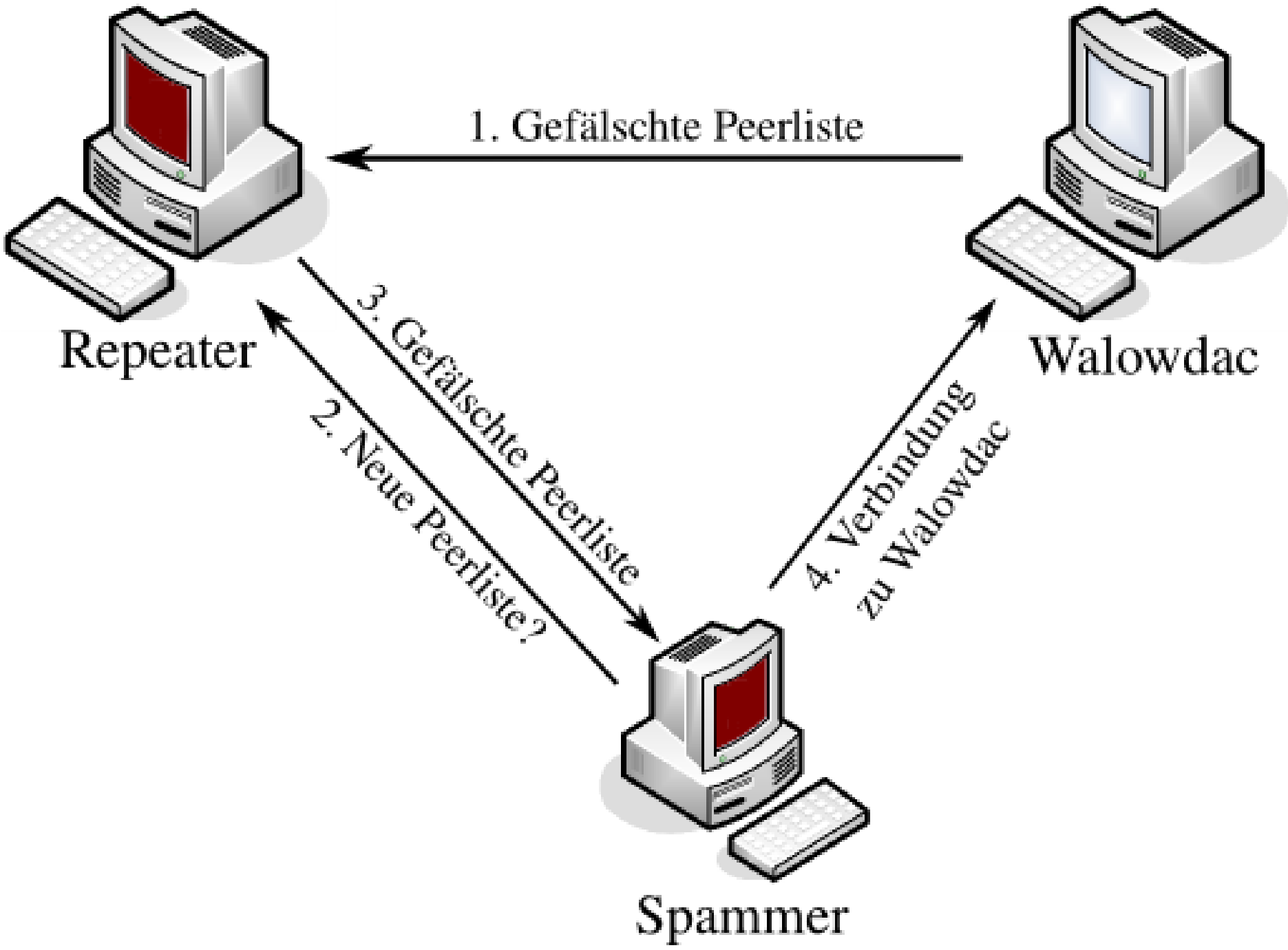
Idee

- Bringe möglichst viele Bots dazu, zum Walowdac zu verbinden
- Dazu: propagiere Adressen unter den Repeatern, die wiederrum die diese an Spammer entsprechend weiterleiten

Propagierung

- Waledac prüft nicht, ob IP bereits in der Liste ist
- ausschließlich ID ist Kriterium
  - wenige IPs, verschiedene IDs benutzen
  - viele Einträge, die auf Walowdac zeigen
- Repeater Crawler sendet Walowdac-Adressen
- Walowdac selbst antwortet mit Walowdac-Adressen

UNIVERSITÄT MANNHEIM


1. Gefälschte Peerliste
Repeater
Walowdac
3. Gefälschte Peerliste
2. Neue Peerliste?
4. Verbindung zu Walowdac
Spammer

Größenmessung des Botnetzes

Daten vom 22. Juli

- **Maximum: 110.917 IDs**
- aber: viele Kollissionen bei den IDs
- daher: ID und ASN als Kriterium
- **so berechnetes Maximum: 129.449**

UNIVERSITÄT MANNHEIM

Größenmessung des Botnetzes

Daten vom 22. Juli

- **Maximum: 110.917 IDs**
- aber: viele Kollissionen bei den IDs
- daher: ID und ASN als Kriterium
- **so berechnetes Maximum: 129.449**

UNIVERSITÄT MANNHEIM

Größenmessung des Botnetzes

Daten vom 22. Juli

- **Maximum: 110.917 IDs**
- aber: viele Kollissionen bei den IDs
- daher: ID und ASN als Kriterium
- so berechnetes Maximum: 129.449

UNIVERSITÄT MANNHEIM

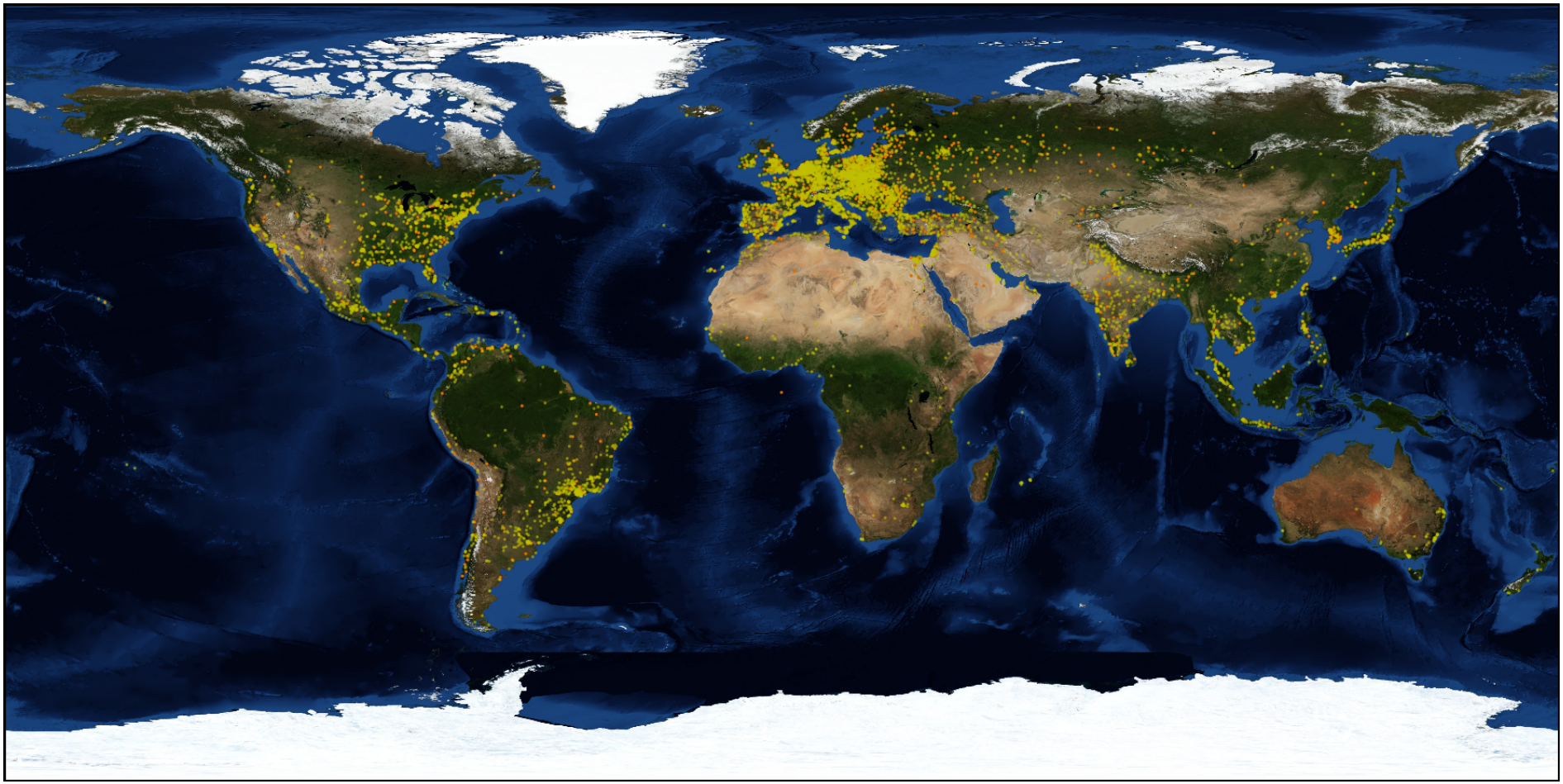
Größenmessung des Botnetzes

Daten vom 22. Juli

- **Maximum: 110.917 IDs**
- aber: viele Kollissionen bei den IDs
- daher: ID und ASN als Kriterium
- **so berechnetes Maximum: 129.449**

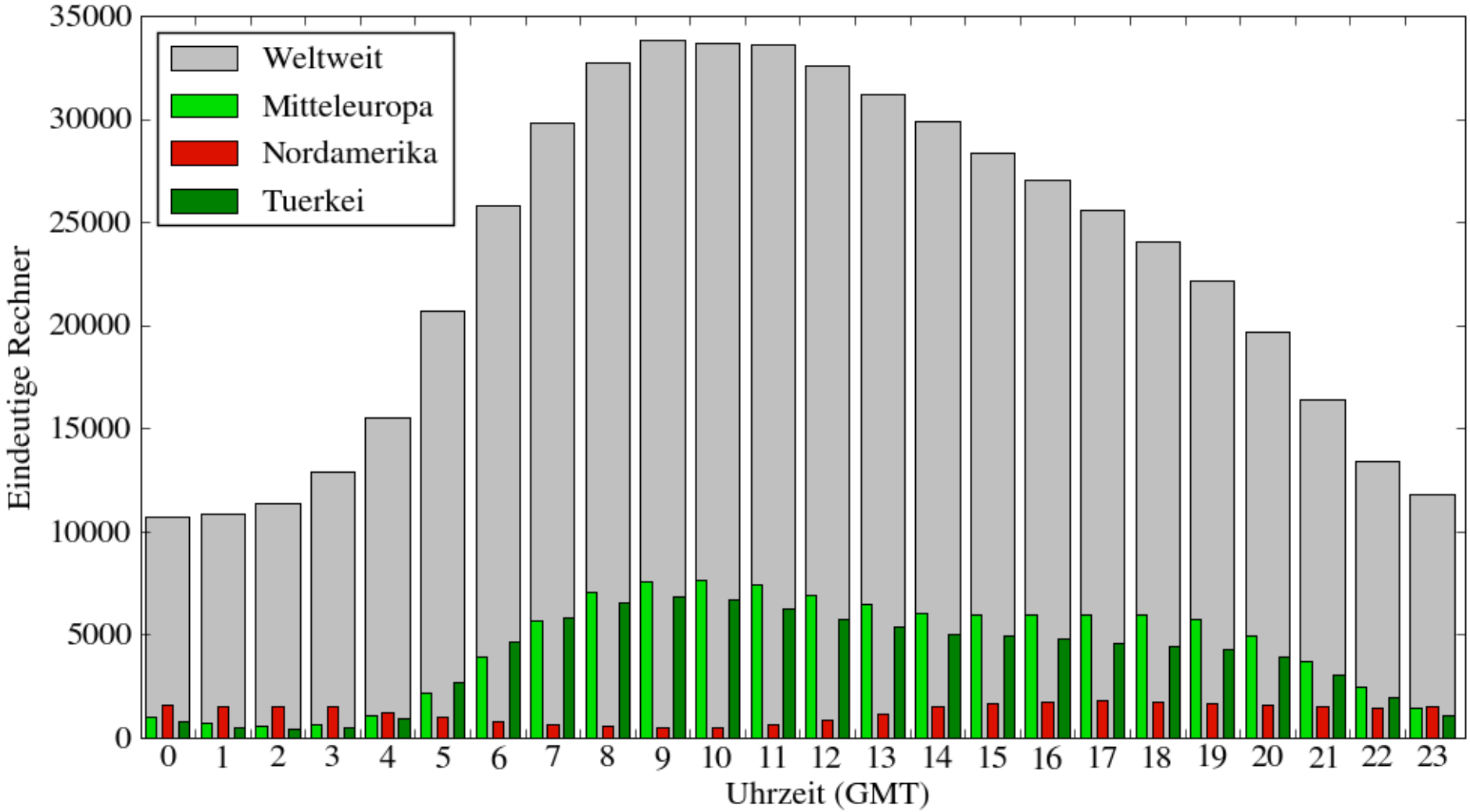
UNIVERSITÄT MANNHEIM

Verteilung über die Weltkarte



UNIVERSITÄT MANNHEIM

Verteilung der laufenden Bots am 22. Juli



UNIVERSITÄT MANNHEIM

Erkenntnisse

- jeden Tag mindestens 38.000 IDs
- vergleichweise wenige Verbindungen aus
  - Nordamerika
  - Asien
- Grund: erhöhte Netzwerk-Latenz + Walowdac-Latenz
- $\longrightarrow$ offenbar immer noch untere Schranke

UNIVERSITÄT MANNHEIM

Erkenntnisse

- jeden Tag mindestens 38.000 IDs
- vergleichweise wenige Verbindungen aus
  - Nordamerika
  - Asien
- Grund: erhöhte Netzwerk-Latenz + Walowdac-Latenz
- $\longrightarrow$ offenbar immer noch untere Schranke

UNIVERSITÄT MANNHEIM

Erkenntnisse

- jeden Tag mindestens 38.000 IDs
- vergleichweise wenige Verbindungen aus
  - Nordamerika
  - Asien
- Grund: erhöhte Netzwerk-Latenz + Walowdac-Latenz
- $\longrightarrow$ offenbar immer noch untere Schranke

UNIVERSITÄT MANNHEIM

Erkenntnisse

- jeden Tag mindestens 38.000 IDs
- vergleichweise wenige Verbindungen aus
  - Nordamerika
  - Asien
- Grund: erhöhte Netzwerk-Latenz + Walowdac-Latenz
- $\longrightarrow$ offenbar immer noch untere Schranke

UNIVERSITÄT MANNHEIM

Erkenntnisse

- jeden Tag mindestens 38.000 IDs
- vergleichweise wenige Verbindungen aus
  - Nordamerika
  - Asien
- Grund: erhöhte Netzwerk-Latenz + Walowdac-Latenz
- $\longrightarrow$ offenbar immer noch untere Schranke

UNIVERSITÄT MANNHEIM

Erkenntnisse

- jeden Tag mindestens 38.000 IDs
- vergleichweise wenige Verbindungen aus
  - Nordamerika
  - Asien
- Grund: erhöhte Netzwerk-Latenz + Walowdac-Latenz
- $\longrightarrow$ offenbar immer noch untere Schranke

UNIVERSITÄT MANNHEIM

Windows Versionen (18. Juni - 28. Juli)

Versionscode	genutzt von	Anzahl	Anteil
5.1.2600	XP (32 Bit)	10899	90,2%
6.0.6001	Vista (SP1), Server 2008	678	5,6%
6.0.6000	Vista	353	2,9%
6.0.6002	Vista SP2, Server 2008 (SP2)	78	0,6%
5.2.3790	XP (64 Bit), Server 2003	39	0,3%
5.0.2195	2000	27	0,2%

- nur für ca. 10% der gemessenen Bots
- über alle Betriebssysteme verteilt

UNIVERSITÄT MANNHEIM

Windows Versionen (18. Juni - 28. Juli)

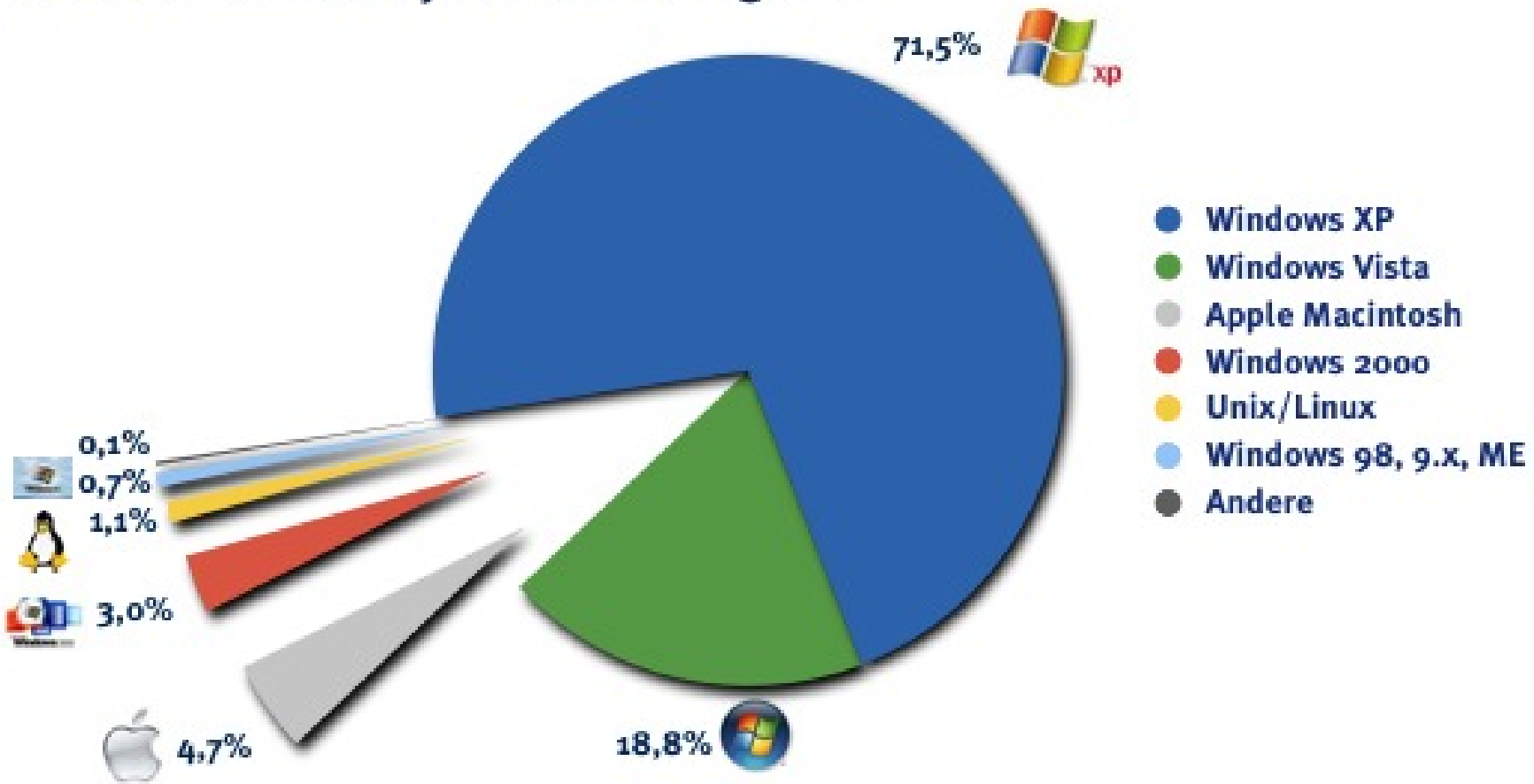
Versionscode	genutzt von	Anzahl	Anteil
5.1.2600	XP (32 Bit)	10899	90,2%
6.0.6001	Vista (SP1), Server 2008	678	5,6%
6.0.6000	Vista	353	2,9%
6.0.6002	Vista SP2, Server 2008 (SP2)	78	0,6%
5.2.3790	XP (64 Bit), Server 2003	39	0,3%
5.0.2195	2000	27	0,2%

- nur für ca. 10% der gemessenen Bots
- über alle Betriebssysteme verteilt

UNIVERSITÄT MANNHEIM

Windows Vista abgeschlagen - Nutzer vertrauen weiter Windows XP

Installierte Betriebssysteme im Vergleich



Basis: Internet-Gesamtnutzerschaft; 27. WWW-Benutzer-Analyse W3B

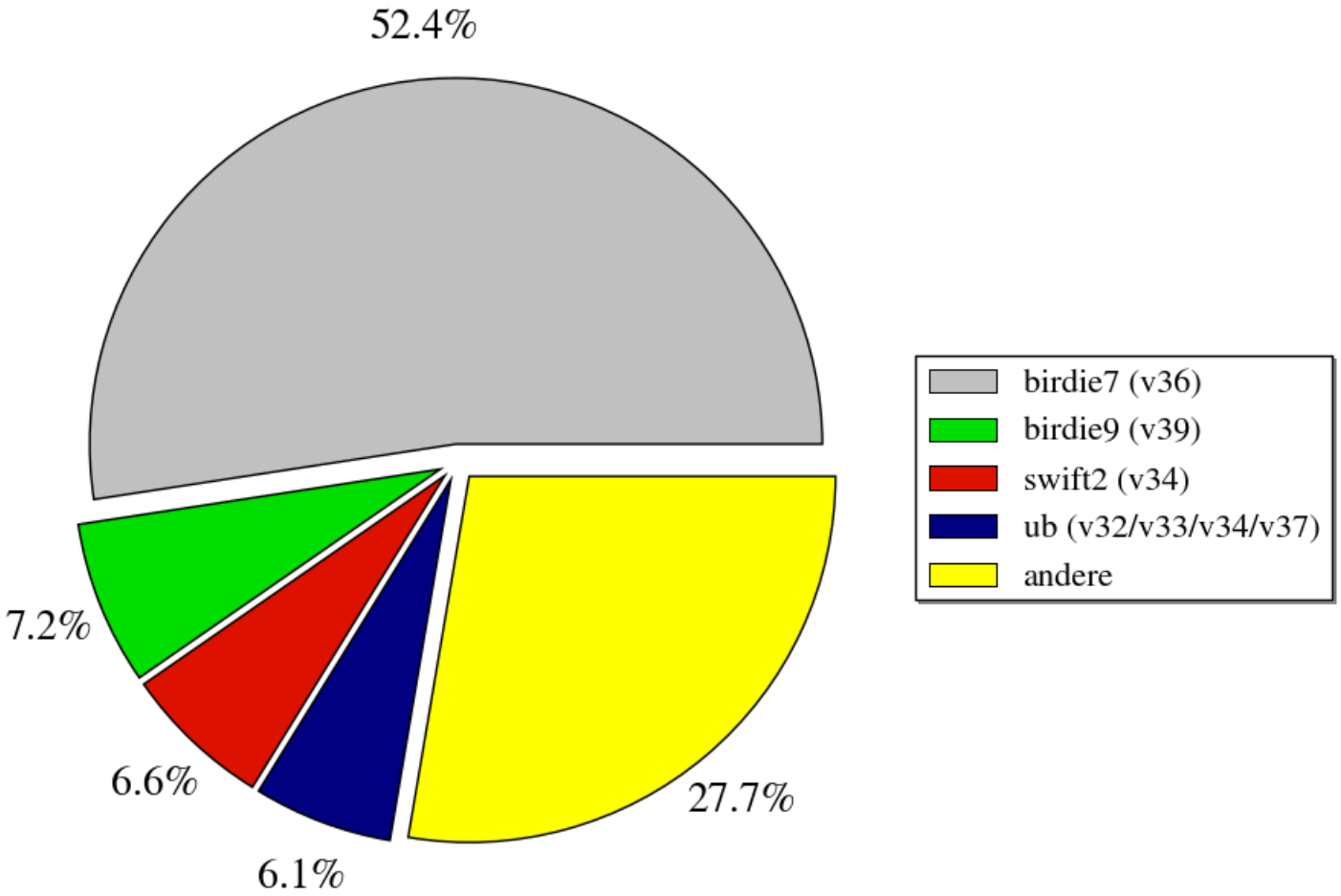
UNIVERSITÄT MANNHEIM

Waledac Versionen

Versionscode	31.7.2009 (65924 Bots)	9.9.2009 (74280 Bots)
< 33	114 (0,17%)	86 (0,12%)
33	440 (0,67%)	270 (0,36%)
34	**20718 (31,43%)**	9344 (12,58%)
35	51 (0,08%)	36 (0,05%)
36	**35572 (53,96%)**	10547 (14,20%)
37	2658 (4,03%)	362 (0,49%)
39	5681 (8,62%)	1650 (2,22%)
40	689 (1,05%)	69 (0,09%)
41-45	0 (0,00%)	8174 (11,00%)
46	0 (0,00%)	**43742 (58,89%)**

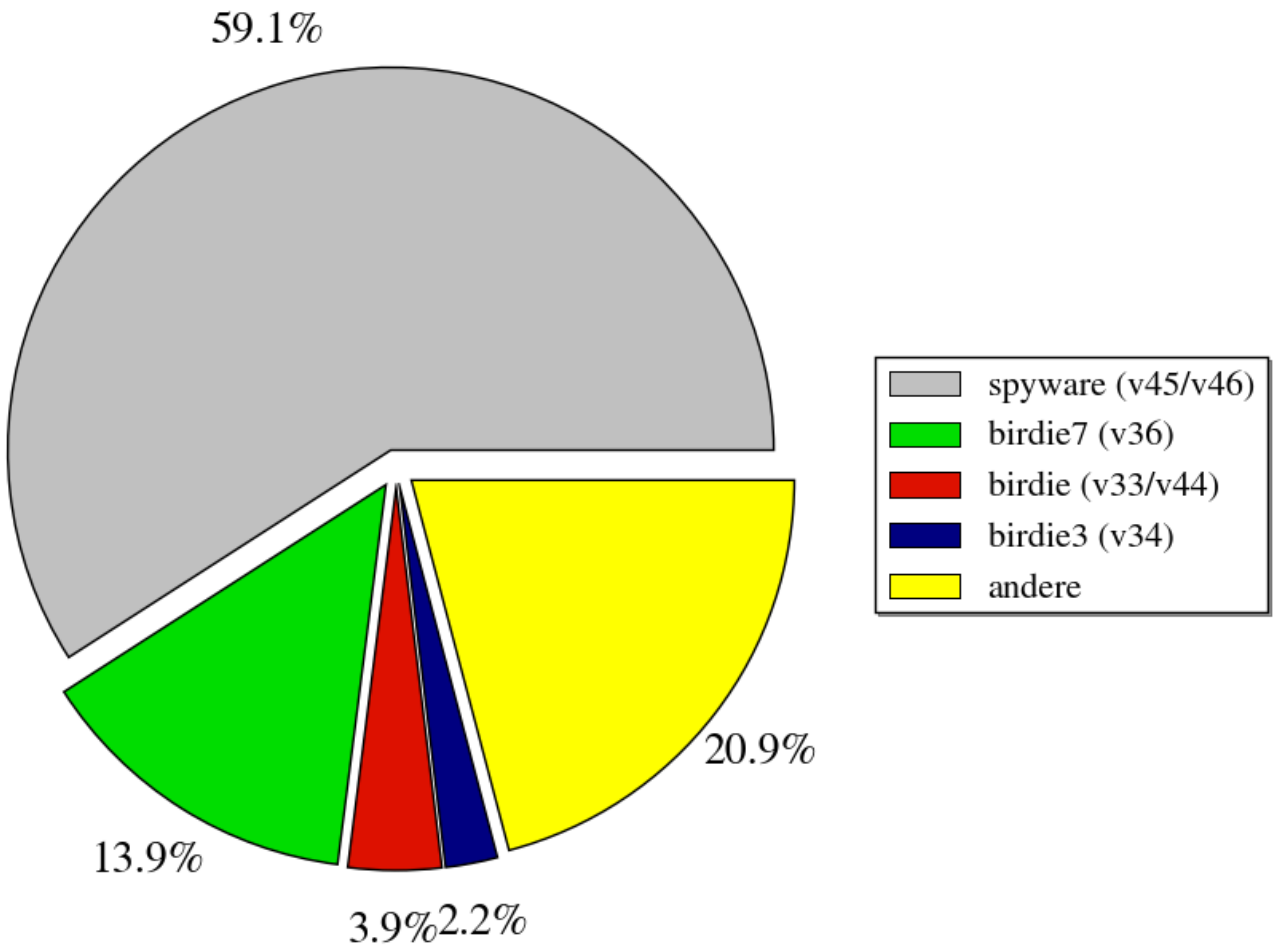
UNIVERSITÄT MANNHEIM

Verbreitungsgrad der Kampagnen (31. Juli)



UNIVERSITÄT MANNHEIM

Verbreitungsgrad der Kampagnen (9. September)



UNIVERSITÄT MANNHEIM

Spammenge und -erfolg

- Versuch von ESET: 6500 E-Mails pro Stunde möglich
- Auswertung der Spamreports: 10 Prozent Zustellungsrate
- jederzeit mindestens 10.000 Bots online
- $10.000 \times 0.1 \times 6500 \times 24 = 156.000.000$ zugestellte E-Mails am Tag!
- zu Spitzenzeiten 30.000 Bots

UNIVERSITÄT MANNHEIM

Spammenge und -erfolg

- Versuch von ESET: 6500 E-Mails pro Stunde möglich
- Auswertung der Spamreports: 10 Prozent Zustellungsrate
- jederzeit mindestens 10.000 Bots online
- $10.000 \times 0.1 \times 6500 \times 24 = 156.000.000$ zugestellte E-Mails am Tag!
- zu Spitzenzeiten 30.000 Bots

UNIVERSITÄT MANNHEIM

Spammenge und -erfolg

- Versuch von ESET: 6500 E-Mails pro Stunde möglich
- Auswertung der Spamreports: 10 Prozent Zustellungsrate
- jederzeit mindestens 10.000 Bots online
- $10.000 \times 0.1 \times 6500 \times 24 = 156.000.000$ zugestellte E-Mails am Tag!
- zu Spitzenzeiten 30.000 Bots

UNIVERSITÄT MANNHEIM

Spammenge und -erfolg

- Versuch von ESET: 6500 E-Mails pro Stunde möglich
- Auswertung der Spamreports: 10 Prozent Zustellungsrate
- jederzeit mindestens 10.000 Bots online
- $10.000 \times 0.1 \times 6500 \times 24 = 156.000.000$ zugestellte E-Mails am Tag!
- zu Spitzenzeiten 30.000 Bots

UNIVERSITÄT MANNHEIM

Spammenge und -erfolg

- Versuch von ESET: 6500 E-Mails pro Stunde möglich
- Auswertung der Spamreports: 10 Prozent Zustellungsrate
- jederzeit mindestens 10.000 Bots online
- $10.000 \times 0.1 \times 6500 \times 24 = 156.000.000$ zugestellte E-Mails am Tag!
- zu Spitzenzeiten 30.000 Bots

UNIVERSITÄT MANNHEIM

Überschreiben der Repeaterlisten

- maximal 500 Einträge werden in Registry gespeichert
- normaler Fall: Repeater schickt in Antwort 100 Einträge
- Frage: was passiert, wenn 500 Einträge geschickt werden?
- $\longrightarrow$ komplette Liste wird überschrieben
- funktioniert analog bei verschiedenen Längen der Repeaterlisten
- $\longrightarrow$ Übernahme des Netzes einfach (und legal) möglich

UNIVERSITÄT MANNHEIM

Überschreiben der Repeaterlisten

- maximal 500 Einträge werden in Registry gespeichert
- normaler Fall: Repeater schickt in Antwort 100 Einträge
- Frage: was passiert, wenn 500 Einträge geschickt werden?
- $\longrightarrow$ komplette Liste wird überschrieben
- funktioniert analog bei verschiedenen Längen der Repeaterlisten
- $\longrightarrow$ Übernahme des Netzes einfach (und legal) möglich

UNIVERSITÄT MANNHEIM

Überschreiben der Repeaterlisten

- maximal 500 Einträge werden in Registry gespeichert
- normaler Fall: Repeater schickt in Antwort 100 Einträge
- Frage: was passiert, wenn 500 Einträge geschickt werden?
- $\longrightarrow$ komplette Liste wird überschrieben
- funktioniert analog bei verschiedenen Längen der Repeaterlisten
- $\longrightarrow$ Übernahme des Netzes einfach (und legal) möglich

UNIVERSITÄT MANNHEIM

Überschreiben der Repeaterlisten

- maximal 500 Einträge werden in Registry gespeichert
- normaler Fall: Repeater schickt in Antwort 100 Einträge
- Frage: was passiert, wenn 500 Einträge geschickt werden?
- $\longrightarrow$ komplette Liste wird überschrieben
- funktioniert analog bei verschiedenen Längen der Repeaterlisten
- $\longrightarrow$ Übernahme des Netzes einfach (und legal) möglich

UNIVERSITÄT MANNHEIM

Überschreiben der Repeaterlisten

- maximal 500 Einträge werden in Registry gespeichert
- normaler Fall: Repeater schickt in Antwort 100 Einträge
- Frage: was passiert, wenn 500 Einträge geschickt werden?
- → komplette Liste wird überschrieben
- funktioniert analog bei verschiedenen Längen der Repeaterlisten
- → Übernahme des Netzes einfach (und legal) möglich

UNIVERSITÄT MANNHEIM

Überschreiben der Repeaterlisten

- maximal 500 Einträge werden in Registry gespeichert
- normaler Fall: Repeater schickt in Antwort 100 Einträge
- Frage: was passiert, wenn 500 Einträge geschickt werden?
- $\longrightarrow$ komplette Liste wird überschrieben
- funktioniert analog bei verschiedenen Längen der Repeaterlisten
- $\longrightarrow$ Übernahme des Netzes einfach (und legal) möglich

UNIVERSITÄT MANNHEIM

Überschreiben der Repeaterlisten

- maximal 500 Einträge werden in Registry gespeichert
- normaler Fall: Repeater schickt in Antwort 100 Einträge
- Frage: was passiert, wenn 500 Einträge geschickt werden?
- $\longrightarrow$ komplette Liste wird überschrieben
- funktioniert analog bei verschiedenen Längen der Repeaterlisten
- $\longrightarrow$ Übernahme des Netzes einfach (und legal) möglich

UNIVERSITÄT MANNHEIM

Abstürze

- bei Tests wiederholt Abstürze
- Ursache: keine Fehlerbehandlung bei Entschlüsselung
- $\longrightarrow$ falsch-verschlüsselte Pakete bringen Waledac zum Absturz
- Kombinierbar mit vorigem Angriff - ethisch und rechtlich aber fraglich

UNIVERSITÄT MANNHEIM

Abstürze

- bei Tests wiederholt Abstürze
- Ursache: keine Fehlerbehandlung bei Entschlüsselung
- $\longrightarrow$ falsch-verschlüsselte Pakete bringen Waledac zum Absturz
- Kombinierbar mit vorigem Angriff - ethisch und rechtlich aber fraglich

UNIVERSITÄT MANNHEIM

Abstürze

- bei Tests wiederholt Abstürze
- Ursache: keine Fehlerbehandlung bei Entschlüsselung
- $\longrightarrow$ falsch-verschlüsselte Pakete bringen Waledac zum Absturz
- Kombinierbar mit vorigem Angriff - ethisch und rechtlich aber fraglich

UNIVERSITÄT MANNHEIM

Abstürze

- bei Tests wiederholt Abstürze
- Ursache: keine Fehlerbehandlung bei Entschlüsselung
- $\longrightarrow$ falsch-verschlüsselte Pakete bringen Waledac zum Absturz
- Kombinierbar mit vorigem Angriff - ethisch und rechtlich aber fraglich

UNIVERSITÄT MANNHEIM

Fazit

- Größe des Botnetzes liegt deutlich über bisherigen Schätzungen
  - weiterhin nur untere Schranke (z.B. wenig Verbindungen aus den USA)
- viele Ähnlichkeiten zum Storm-Wurm – wahrscheinlich Nachfolger
  - Templatesystem
  - Reporting
  - Verbreitungskampagnen
- Angriffsmöglichkeiten zur Übernahme des Botnetzes

UNIVERSITÄT MANNHEIM

Fazit

- Größe des Botnetzes liegt deutlich über bisherigen Schätzungen
  - weiterhin nur untere Schranke (z.B. wenig Verbindungen aus den USA)
- viele Ähnlichkeiten zum Storm-Wurm – wahrscheinlich Nachfolger
  - Templatesystem
  - Reporting
  - Verbreitungskampagnen
- Angriffsmöglichkeiten zur Übernahme des Botnetzes

UNIVERSITÄT MANNHEIM

Fazit

- Größe des Botnetzes liegt deutlich über bisherigen Schätzungen
  - weiterhin nur untere Schranke (z.B. wenig Verbindungen aus den USA)
- viele Ähnlichkeiten zum Storm-Wurm – wahrscheinlich Nachfolger
  - Templatesystem
  - Reporting
  - Verbreitungskampagnen
- Angriffsmöglichkeiten zur Übernahme des Botnetzes

UNIVERSITÄT MANNHEIM

Fazit

- Größe des Botnetzes liegt deutlich über bisherigen Schätzungen
  - weiterhin nur untere Schranke (z.B. wenig Verbindungen aus den USA)
- viele Ähnlichkeiten zum Storm-Wurm – wahrscheinlich Nachfolger
  - Templatesystem
  - Reporting
  - Verbreitungskampagnen
- Angriffsmöglichkeiten zur Übernahme des Botnetzes

UNIVERSITÄT MANNHEIM

Fazit

- Größe des Botnetzes liegt deutlich über bisherigen Schätzungen
  - weiterhin nur untere Schranke (z.B. wenig Verbindungen aus den USA)
- viele Ähnlichkeiten zum Storm-Wurm – wahrscheinlich Nachfolger
  - Templatesystem
  - Reporting
  - Verbreitungskampagnen
- Angriffsmöglichkeiten zur Übernahme des Botnetzes

UNIVERSITÄT MANNHEIM

Fazit

- Größe des Botnetzes liegt deutlich über bisherigen Schätzungen
  - weiterhin nur untere Schranke (z.B. wenig Verbindungen aus den USA)
- viele Ähnlichkeiten zum Storm-Wurm – wahrscheinlich Nachfolger
  - Templatesystem
  - Reporting
  - Verbreitungskampagnen
- Angriffsmöglichkeiten zur Übernahme des Botnetzes

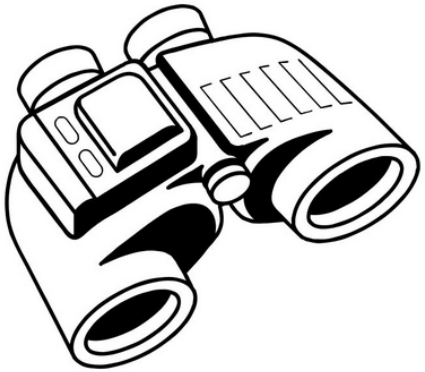
UNIVERSITÄT MANNHEIM

Fazit

- Größe des Botnetzes liegt deutlich über bisherigen Schätzungen
  - weiterhin nur untere Schranke (z.B. wenig Verbindungen aus den USA)
- viele Ähnlichkeiten zum Storm-Wurm – wahrscheinlich Nachfolger
  - Templatesystem
  - Reporting
  - Verbreitungskampagnen
- Angriffsmöglichkeiten zur Übernahme des Botnetzes

UNIVERSITÄT MANNHEIM

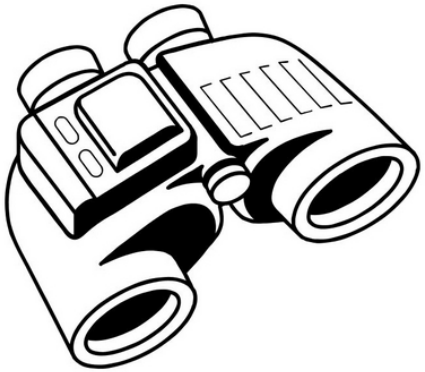
Ausblick



- in den letzten Wochen gab es fast 10 neue Versionen
  - → weitere Beobachtung notwendig
- Untersuchung des Templatesystems
  - z.B. Generieren von E-Mails zum Training von Spamfiltern
- Angriff auf das Botnetz

UNIVERSITÄT MANNHEIM

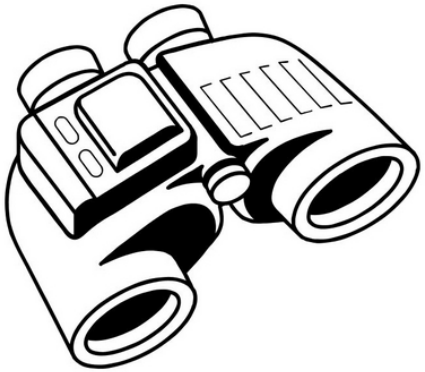
Ausblick



- in den letzten Wochen gab es fast 10 neue Versionen
  - → weitere Beobachtung notwendig
- Untersuchung des Templatesystems
  - z.B. Generieren von E-Mails zum Training von Spamfiltern
- Angriff auf das Botnetz

UNIVERSITÄT MANNHEIM

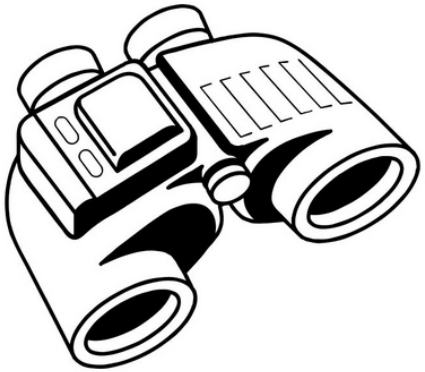
Ausblick



- in den letzten Wochen gab es fast 10 neue Versionen
  - $\longrightarrow$ weitere Beobachtung notwendig
- Untersuchung des Templatesystems
  - z.B. Generieren von E-Mails zum Training von Spamfiltern
- Angriff auf das Botnetz

UNIVERSITÄT MANNHEIM

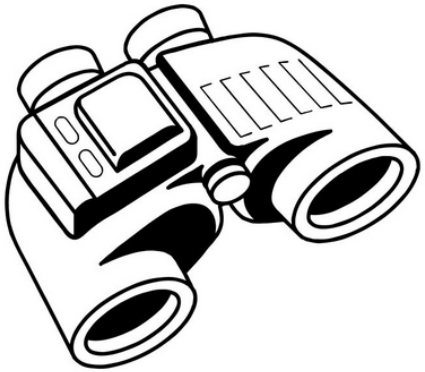
Ausblick



- in den letzten Wochen gab es fast 10 neue Versionen
  - $\rightarrow$ weitere Beobachtung notwendig
- Untersuchung des Templatesystems
  - z.B. Generieren von E-Mails zum Training von Spamfiltern
- Angriff auf das Botnetz

UNIVERSITÄT MANNHEIM

Ausblick



- in den letzten Wochen gab es fast 10 neue Versionen
  - $\rightarrow$ weitere Beobachtung notwendig
- Untersuchung des Templatesystems
  - z.B. Generieren von E-Mails zum Training von Spamfiltern
- Angriff auf das Botnetz

UNIVERSITÄT MANNHEIM

Fragen?

UNIVERSITÄT MANNHEIM

Danke für die Aufmerksamkeit

UNIVERSITÄT MANNHEIM