Botspy - Effiziente Beobachtung von Botnetzen

Claus R. F. Overbeck - RedTeam Pentesting GmbH
claus.overbeck@redteam-pentesting.de
http://www.redteam-pentesting.de

Felix Freiling, Thorsten Holz
Universität Mannheim

15. DFN-Cert Workshop – Sicherheit in vernetzten Systemen
13. Februar 2008, Hamburg

„Gib Dich wie ein Freund, aber handle wie ein Spion “

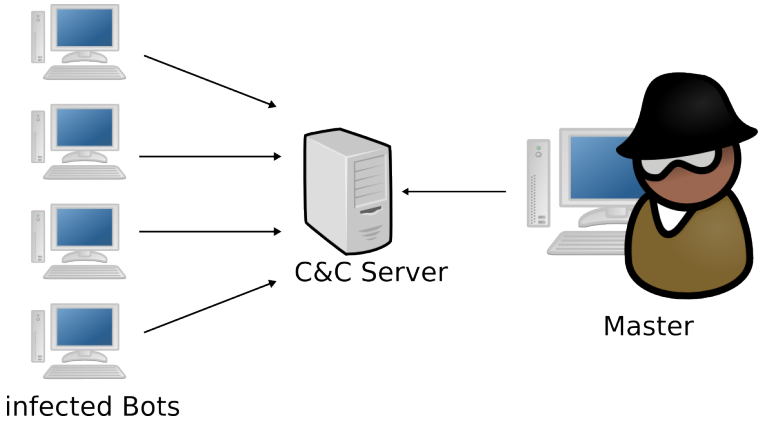
(Robert Greene)

```
DJFelipe                :!login cocacola
DJFelipe                :!keylog on

rBot|010404!~ufdj       :[KEYLOG]: Already running.
rBot|015803!~tlknt      :[KEYLOG]: Key logger active.
rBot|010343!~fwiap      :[MAIN]: Password accepted.

rBot|010211!~pntdgz     :[KEYLOG]: kotuntersuchung (Changed
                         Windows: easyVET)
rBot|010211!~pntdgz     :[KEYLOG]: frau mayer mit ekh mirko2[
                         LEFT]2[RGHT] - kastration (Changed
                         Windows: easyVET)
rBot|010536!~vwbvgv     :[KEYLOG]: termin 16.30 uhr, ;bergibt
                         sich st'ndig (Return) (Verwaltung)

rBot|010211!~pntdgz     :[KEYLOG]:  (Changed Windows: Microsoft
                          Word - Moorhuhn.dat)

rBot|010211!~pntdgz     :[KEYLOG]:  (Changed Windows: Microsoft
                          Word - Kuendigung Schneider.doc)
```

Bots and Botnets

Was ist ein Bot/Botnetz?

- ★ Malware (malicious software)
- ★ Vom Angreifer ferngesteuert
- ★ Benötigen Netwerkinfrastruktur (C&C Server)



- ★ Können für vielfältige Zwecke eingesetz werden.

  `http://www.angelfire.com/theforce/travon1120/RxBotCMDLIST.html`

  - ★ Spam, Phishing
  - ★ DDos
  - ★ Scanning, Spreading
  - ★ Sniffing, Keylogger
  - ★ Password collecting (z.B. Online-Banking-Zugänge)
  - ★ ... und vieles mehr

Kommunikationsmethoden

- Push:
  - Bot hält eine Verbindung zum C&C Server aufrecht
  - Angreifer postet neue Befehle
  - z.B. IRC
- Pull:
  - Bot verbindet sich regelmäßig zum C&C Server
  - Fragt jedesmal die aktuellen Instruktionen ab.
  - z.B. HTTP
- außerdem: Dezentrale Netze - peer to peer - z.B. WASTE, eDonkey
  (werden hier [noch] nicht betrachtet)

Voraussetzungen für eine Beobachtung

- Information: Wie kann ich mich zum Botnet verbinden?
  z.B.: Hostname, Port, Passwort, Channel, Channelpasswort, Nickname, Username
  - Malware sammeln: Honeypots, Nepenthes
    `http://nepenthes.mwcollect.org/`
  - Analysieren: CWSandbox
    `http://www.cwsandbox.org/`

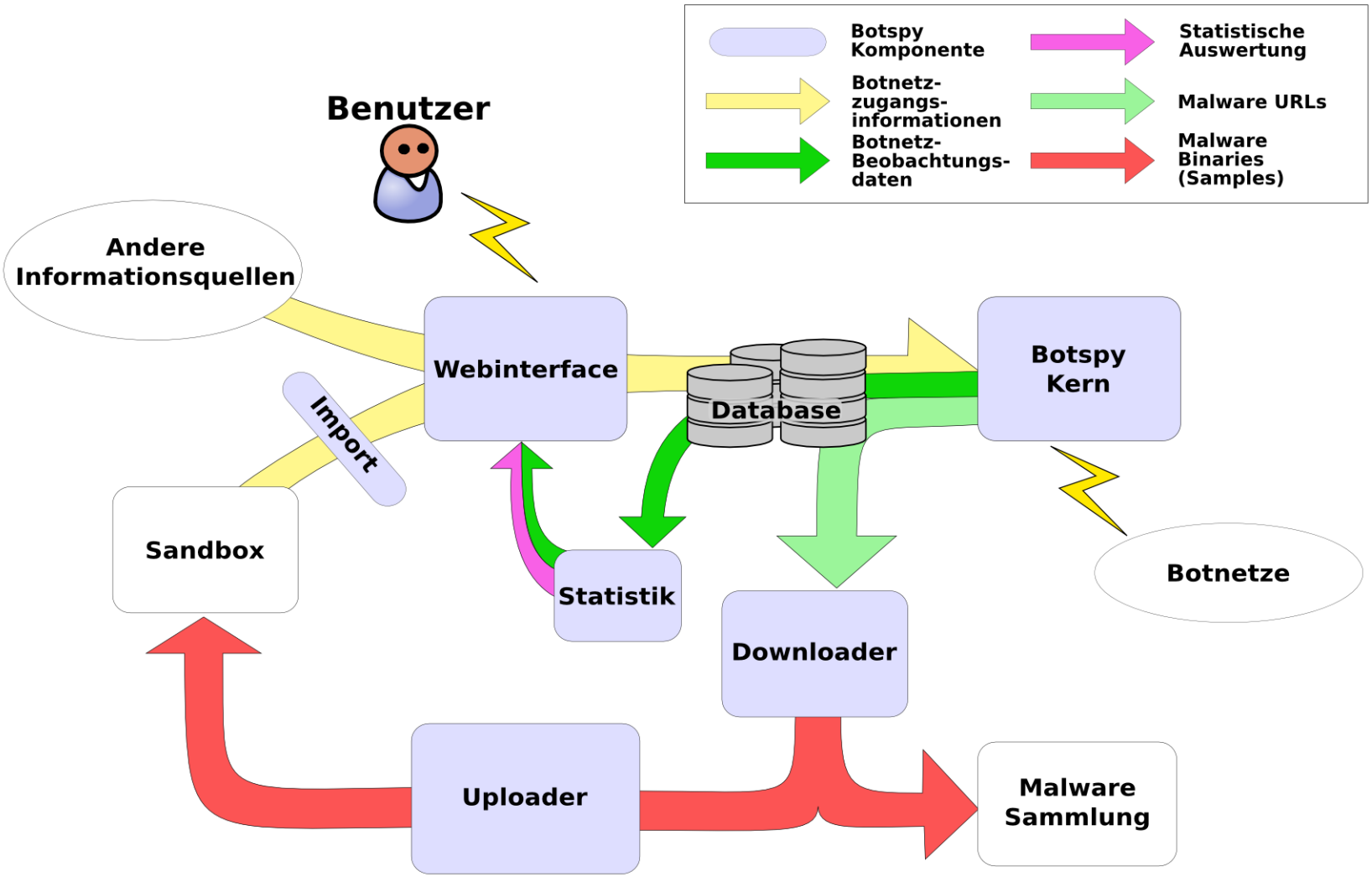
Features/Details - Botspy

- ★ Implementiert in C++, mit Qt 4.1
- ★ Multithreaded: Monitoring vom Logging trennen
- ★ Logging in SQL-DB
- ★ Webinterface in Ruby
  - ★ Konfigurieren der Verbindungen zu den Botnetzen (inkl. CSV-Import)
  - ★ Browsen der gesammelten Daten
- ★ Plugins: Unterschiedliche Botverhalten simulieren
- ★ Nutzt SOCKS5 Proxies
- ★ Beobachten von Pull-Verbindungen

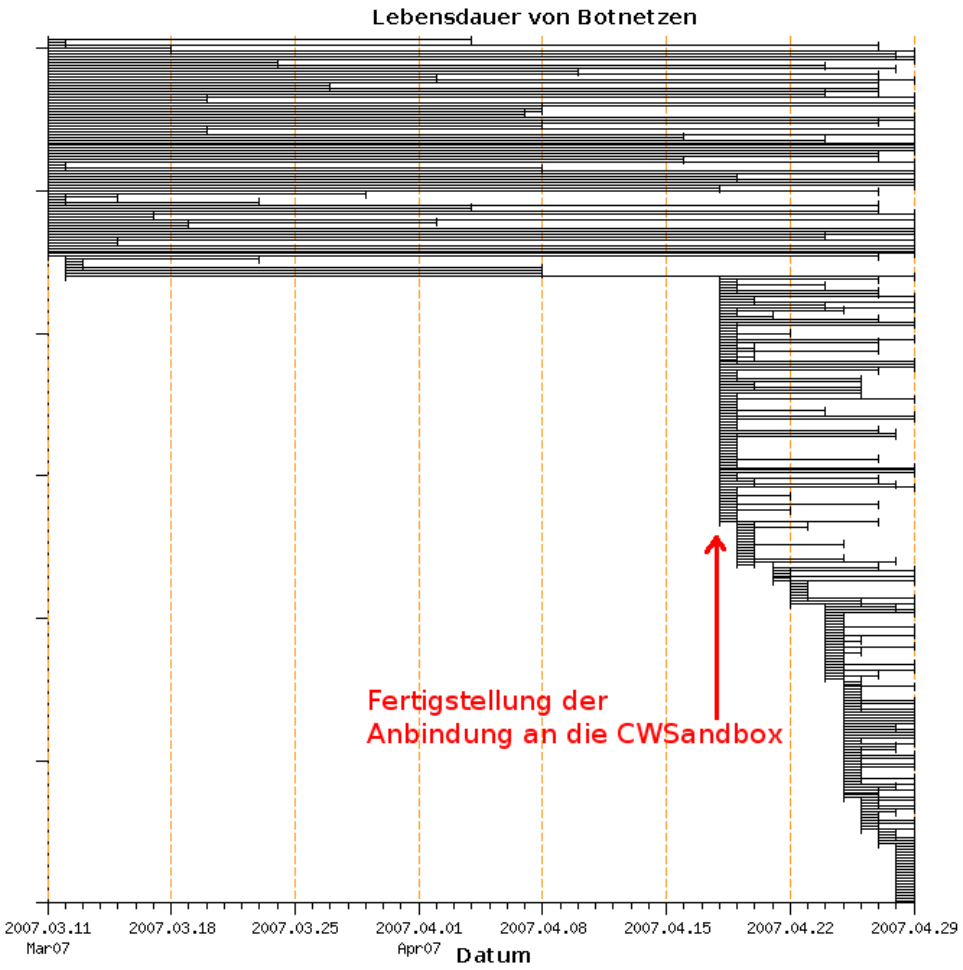
Performance:

- ★ CPU-Auslastung steigt linear mit der Anzahl der Nachrichten/Sekunde.

Botspys Umgebung

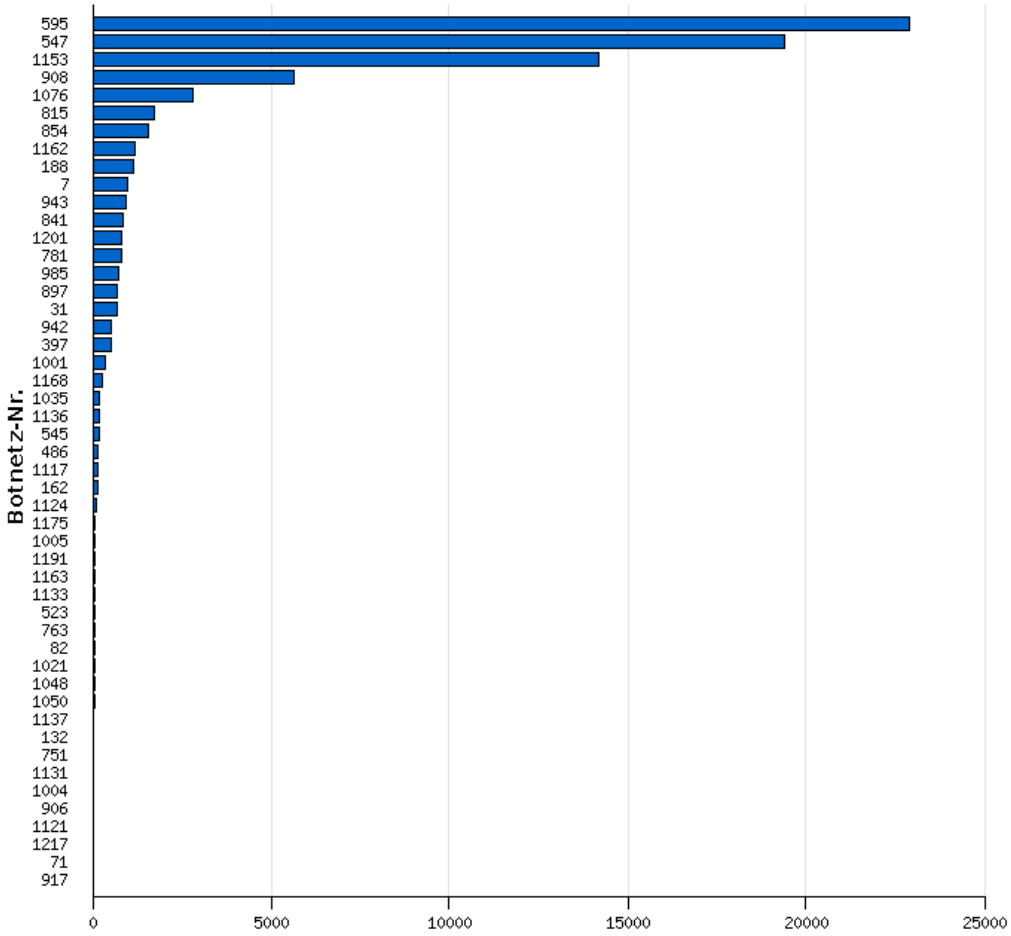


Lebensdauer von Botnetzen



- ★ Ein Botnetz war über 250 Tage aktiv
- ★ Ca. 15 - 20 neue Botnetze jeden Tag
- ★ Ca. 130 Botnetze gleichzeitig aktiv
- ★ Nur ca. 50% der Netze sind länger als zwei Tage aktiv
- ★ Problem: Einige Botnetze sind auf öffentlichen IRC-Servern aktiv.

Größe der Botnetze - Top 50



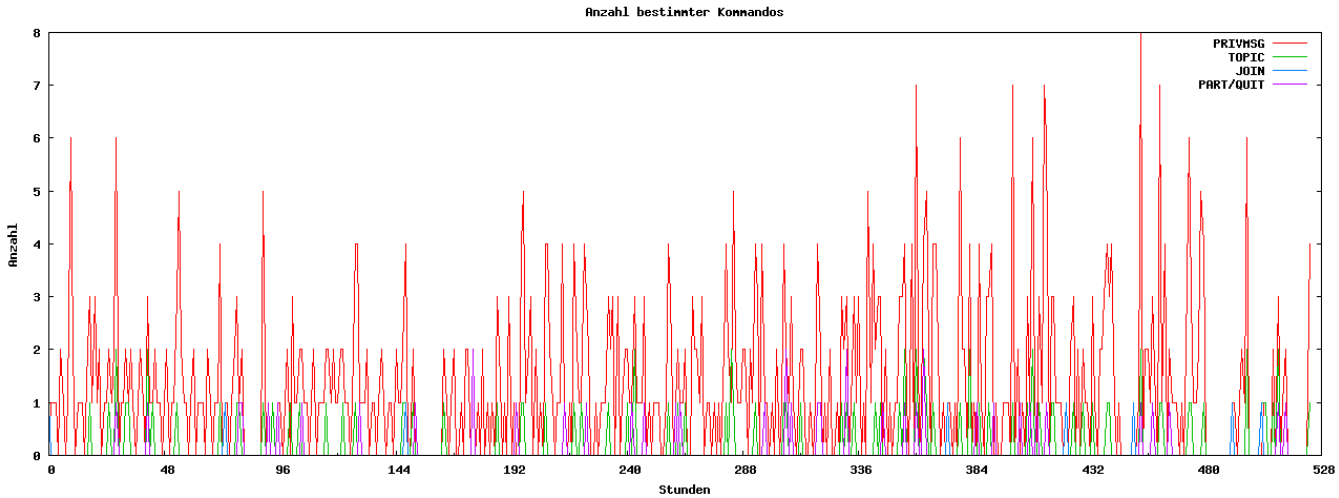
- ★ Insgesamt 60.919 verschiedene Hostnamen beobachtet
- ★ Nur wenige Botnetze mit mehr als 1000 Hostnamen
- ★ Problem: Fake-Hostnamen: 2C307E3F.D97B7C4C.85187735.IP
- ★ Es konnten 48.061 unterschiedliche IP-Adressen aufgelöst werden.
- ★ Problem: DHCP

Beobachtungszeit: 17. März 2007 17:30 Uhr bis 25. April 2007 18:30 (39 Tage)

TOP 20 Autonome Systeme mit infizierten Rechnern

Nummer	AS-Nr.	Land	Netzwerkname	Prozent
10094	22927	AR	Telefonica de Argentina	21,00%
4007	7738	BR	Telecomunicacoes da Bahia S.A.	8,34%
3284	3320	DE	DTAG Deutsche Telekom AG	6,83%
2787	5617	PL	TPNET Polish Telecom_s commercial IP network	5,80%
2336	8167	BR	TELESC - Telecomunicacoes de Santa Catarina SA	4,86%
1286	8151	MX	Uninet S.A. de C.V.	2,68%
982	3209	DE	Arcor IP-Network	2,04%
923	12741	PL	INTERNETIA-AS Netia SA	1,92%
801	8422	DE	NETCOLOGNE NETCOLOGNE AS	1,67%
634	8447	AT	TELEKOM-AT Telekom Austria AutonomousSystem	1,32%
627	7303	AR	Telecom Argentina S.A.	1,30%
493	9269	HK	CTIHK-AS-AP City Telecom (H.K.) Ltd.	1,03%
435	5462	GB	CABLEINET Telewest Broadband	0,91%
425	8404	CH	CABLECOM Cablecom GmbH	0,88%
402	3352	ES	TELEFONICA-DATA-ESPANA Internet Access Network of TDE	0,84%
364	5413	GB	AS5413 PIPEX Communications	0,76%
357	12353	PT	VODAFONE-PT Vodafone Portugal	0,74%
343	25019	SA	SAUDINETSTC-AS Autonomus System Number for SaudiNet	0,71%
339	18881	BR	Global Village Telecom	0,71%
337	3269	IT	ASN-IBSNAZ TELECOM ITALIA	0,70%
16805			Other	34,97%

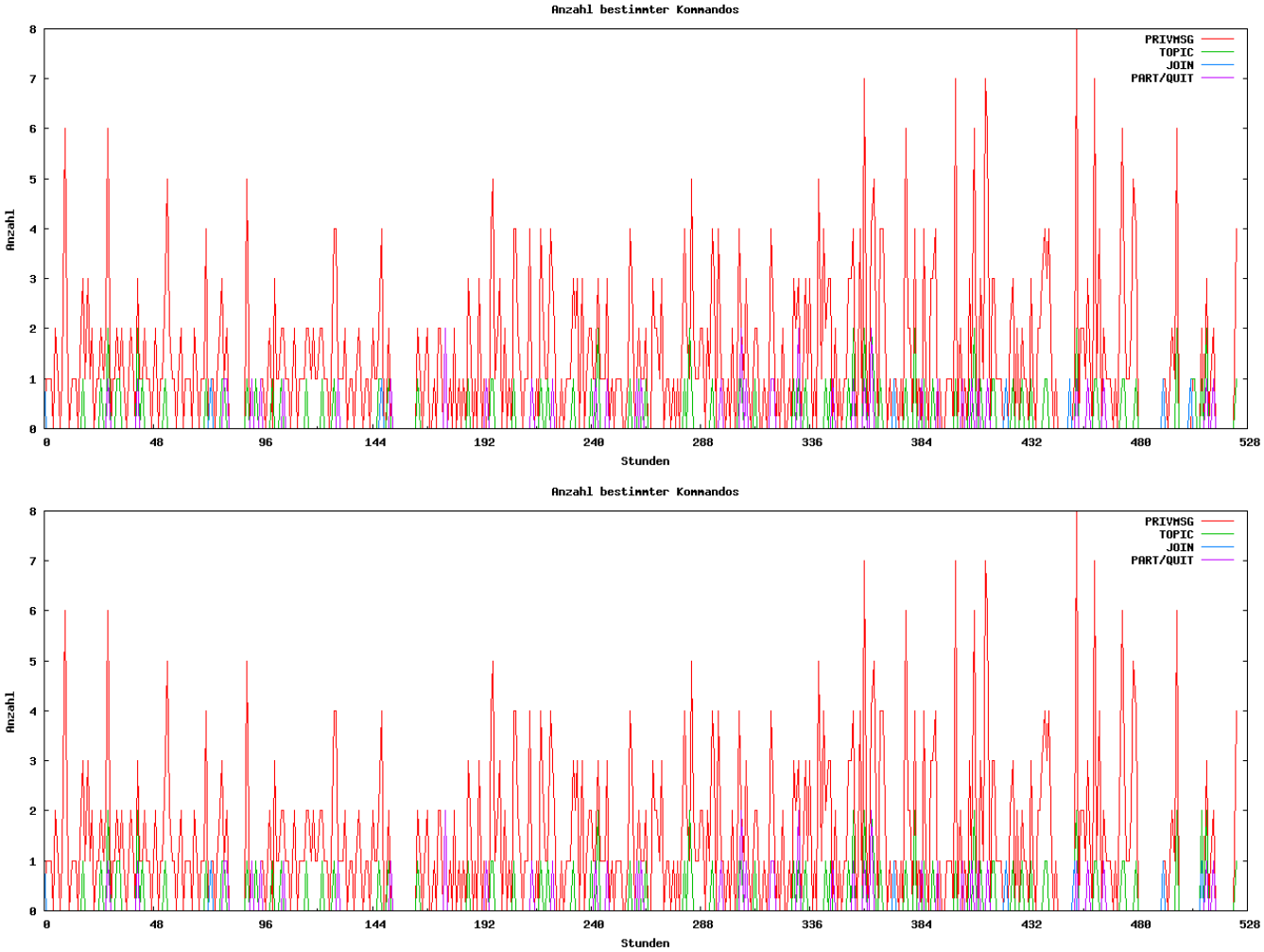
Kommunikationsmuster in Botnetzen



PRIVMSG
TOPIC
JOIN
PART/QUIT

← Botnet 366

Kommunikationsmuster in Botnetzen



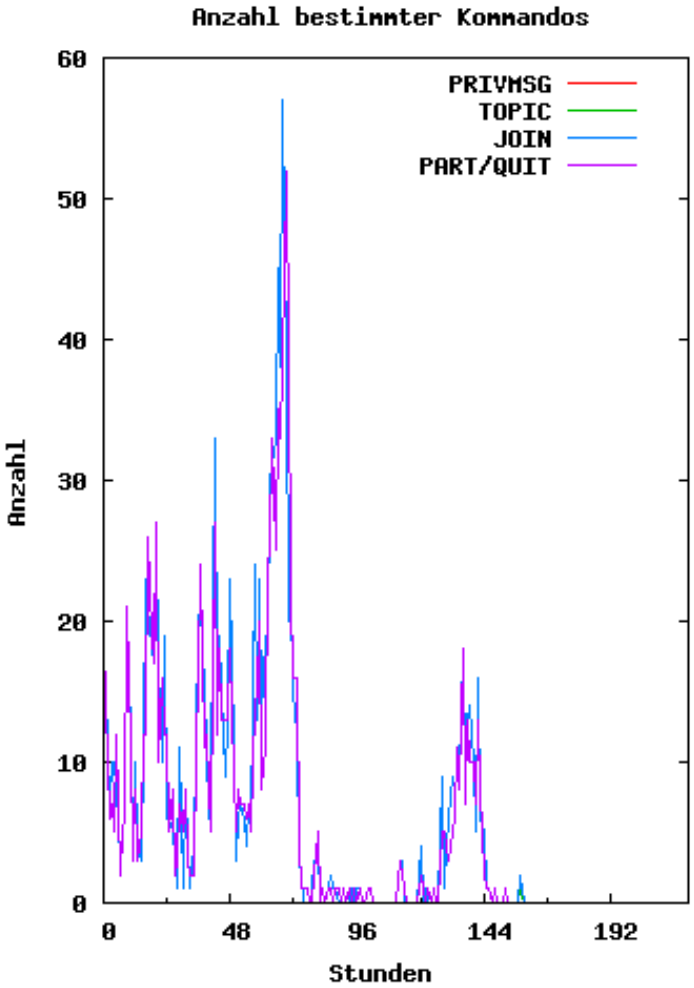
← Botnet 366

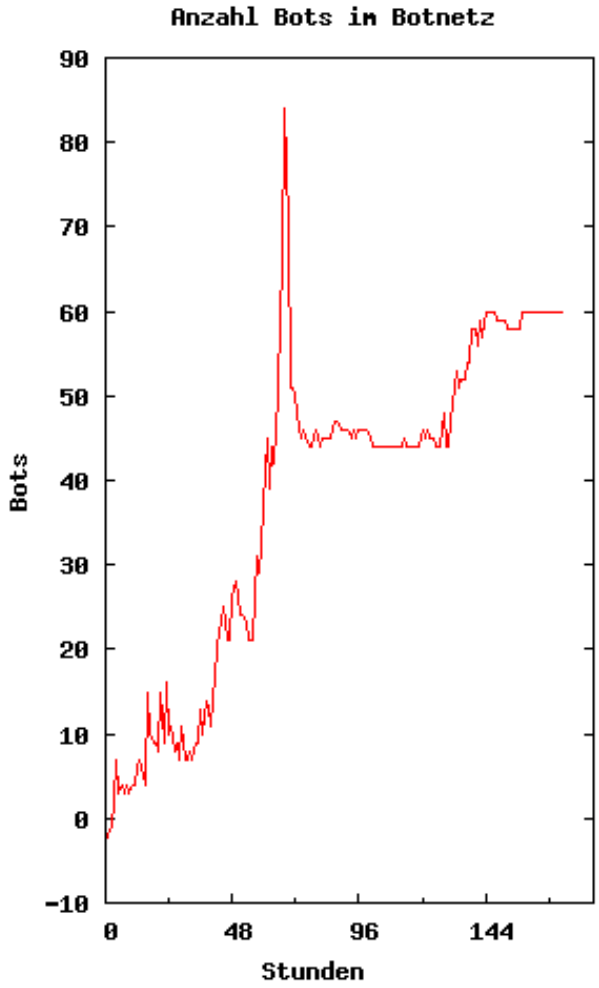
Botnet 371 hat das gleiche Muster wie Botnet 366

In 216 Botnetzen 12 Gruppen mit 52 Netzen

⇒ nur 176 unterschiedliche Netze

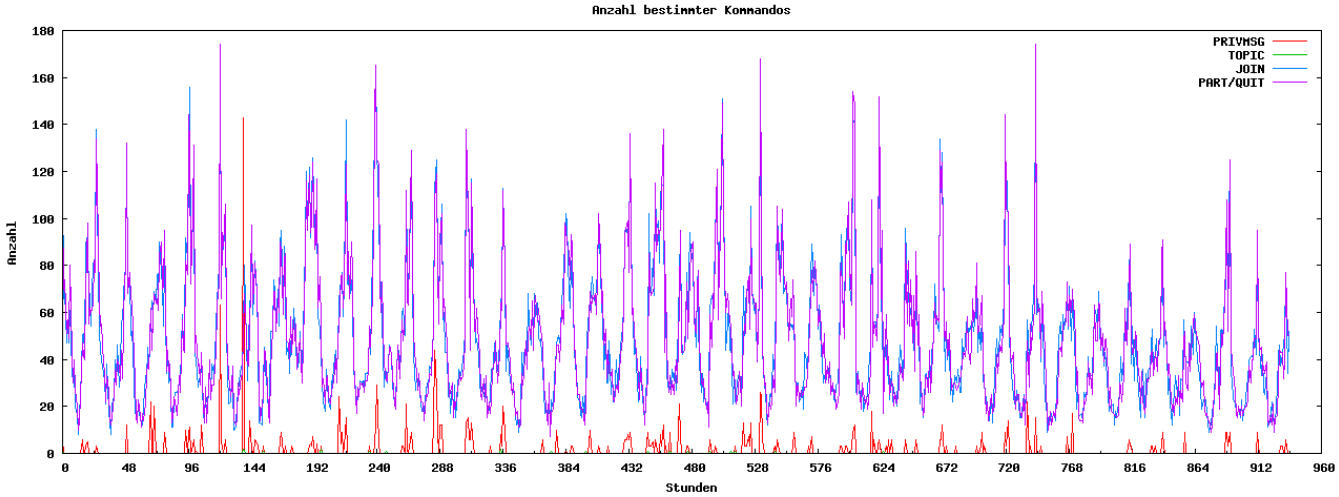
Wachstum von Botnetzen

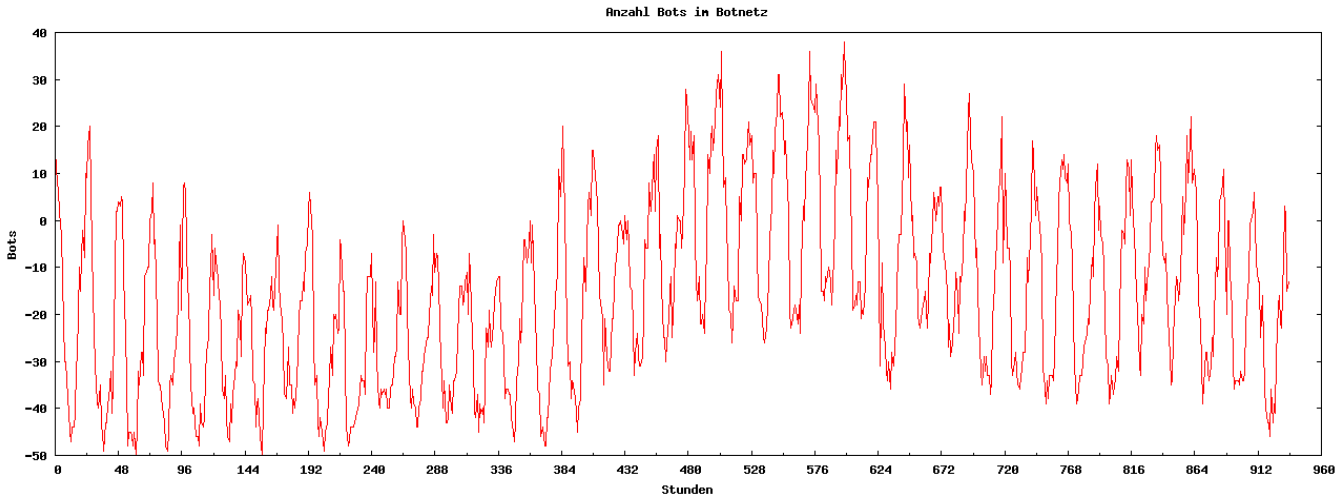




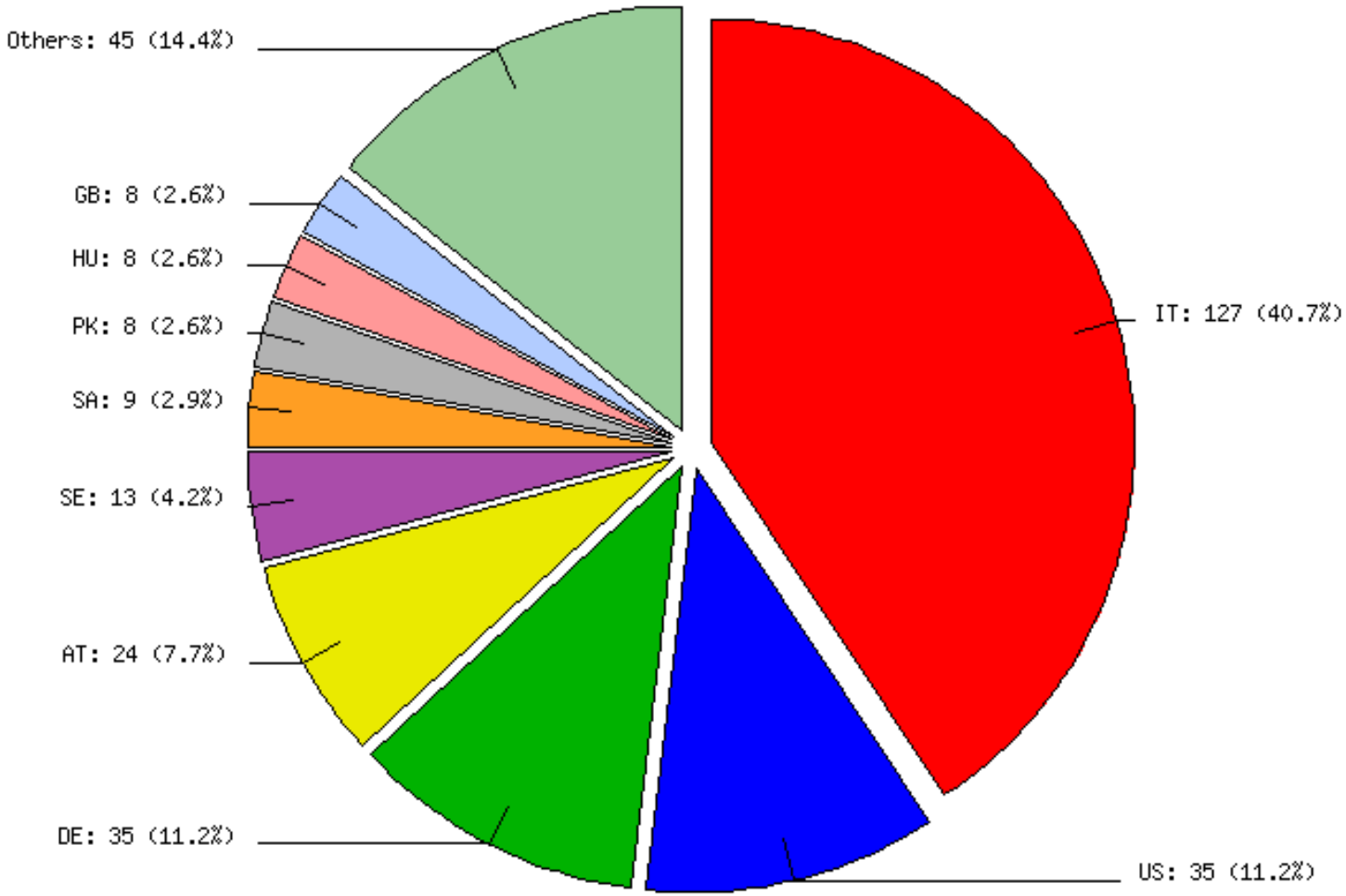
Kommunikationsmuster in Botnetzen - Tagesrhythmus

Botnetz 547:

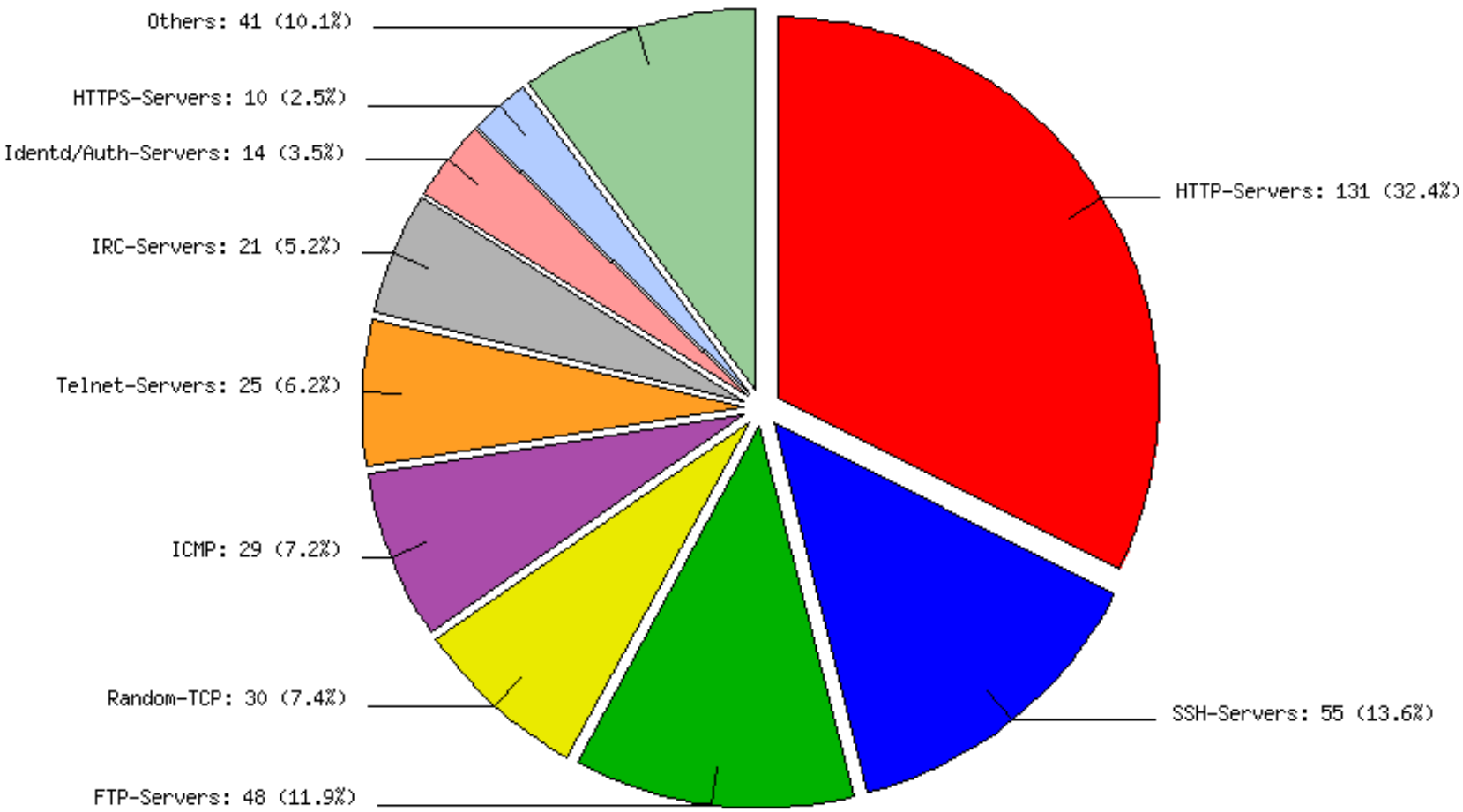




Distributed Denial of Service - Ziele/Land



Distributed Denial of Service - Ziele/Dienst



Distributed Denial of Service

DDoS Ziele:

- ★ Oft gegen Dedicated Server oder Hosting-Provider
- ★ Eigentliches Ziel bleibt meist unklar
- ★ Reverse Lookup liefert häufig Hostnamen wie:

  `if.you.whois.me.i.ddos.you.with.1GB.us`
  `lets.play.war.script.until.excess.flood-flood.info`
  `used.a.hacked.cc.and.bought.a.hacked.name`
  `since.1872.massrooting.by.darksoul.biz`
  `Do.NOT.Play.With.Fire.Cuz.I.Am.attackers.biz`
- ★ Doch nur Krieg der Skript-Kids?

Zusammenfassung und Ausblick

- ★ Ein großer Teil unseres Wissens über Botnetze basiert auf Vermutungen.
- ★ Wir brauchen mehr Daten/Beobachtungen.

Botspy wurde so entwickelt, dass eine Erweiterung leicht möglich sein soll. Aufgaben für die Zukunft:

- ★ Weiter Daten sammeln und analysieren
- ★ Beobachten von Peer-2-Peer Netzen
- ★ Beobachtung verschlüsselter Netze
- ★ Integrieren weiterer Analysen in das Webinterface
- ★ Integration mit anderen Systemen, z.B. Echtzeitbenachrichtigung über infizierte Rechner

Ihre Fragen?

(Falls wir noch etwas Zeit haben...)