Botspy - Efficient Observation of Botnets

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

Hack.lu 2007
19th October 2007

Thanks

RWTH AACHEN
RHEINISCH-WESTFÄLISCHE TECHNISCHE HOCHSCHULE AACHEN

Pi1 - Laboratory for Dependable Distributed Systems

Prof. Dr.-Ing. Felix Freiling

Dipl.-Inform. Thorsten Holz

RedTeam Pentesting GmbH

many others...

"Pose as a Friend, Work as a Spy"

(Robert Greene)

```
DJFelipe]not[available!DJFelipe privmsg #secret :!login
    cocacola
DJFelipe]not[available!DJFelipe privmsg #secret :!keylog on
rBot|010404!~ufdj         privmsg #secret :[KEYLOG]: Already
    running.
rBot|015803!~tlknt        privmsg #secret :[KEYLOG]: Key
    logger active.
rBot|010343!~fwiap        privmsg #secret :[MAIN]: Password
    accepted.

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

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

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

Agenda

Motivation

- A Short Introduction to Botnets
- Observation of Botnets

The Technology - Botspy

- Features
- Botspy and its Environment

Results

- Performance
- Observations

Conclusion and the Future

Bots and Botnets

What is a bot/botnet?

- ★ Malware (malicious software)
- ★ Similar to viruses and worms
- ★ Can be controlled remotely by an attacker
- ★ Needs network infrastructure (C&C server)
- ★ Can be used for various purposes

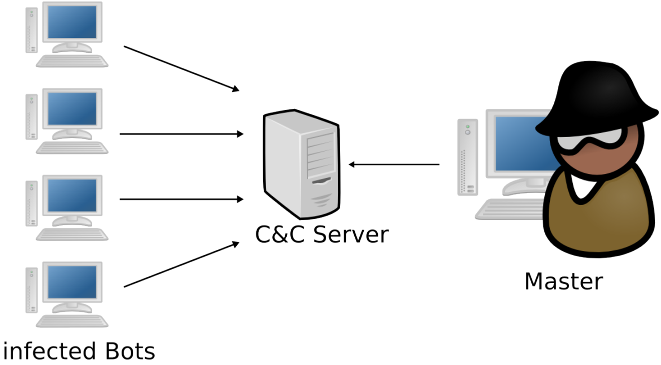
  See `http://www.angelfire.com/theforce/travon1120/RxBotCMDLIST.html`

  - ★ Spam, phishing
  - ★ DDoS
  - ★ Scanning, spreading
  - ★ Sniffing, keylogger
  - ★ Password collecting (e.g. online banking logins)
  - ★ and lots more

Communication techniques

- Push:
  - Bot keeps a connection to the C&C server open
  - The attacker sends instructions over the server to the bots
  - e.g. IRC
- Pull:
  - Bot connects to the C&C server at regular intervals
  - Polls current instructions each time
  - e.g. HTTP
- Also: Decentralized networks - peer to peer - e.g. WASTE, eDonkey
  (not in this work)

Botnet



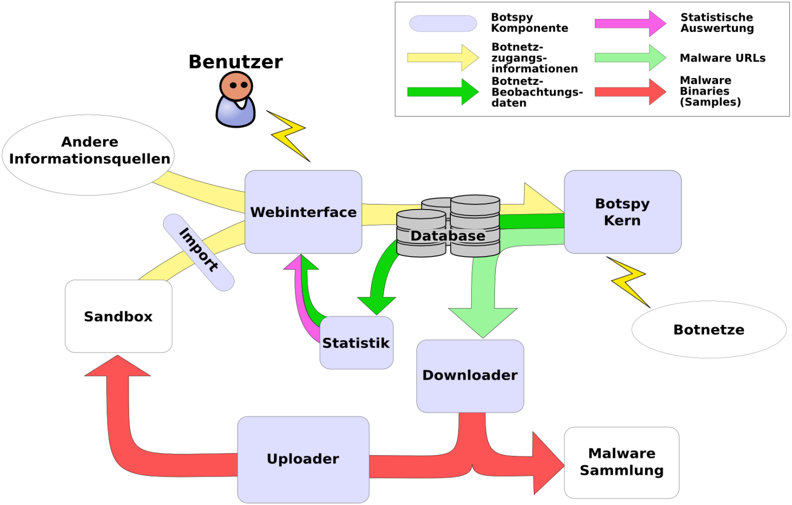
Prerequisites for an observation

- Information: How can we connect to the botnet?
  e.g.: Hostname, port, server password, channel, channel password, nickname, username
  - Collect malware: Honeypots, nepenthes
    `http://nepenthes.mwcollect.org/`
  - Analyze malware: CWSandbox
    `http://www.cwsandbox.org/`

Features/details

- Implemented in C++, uses Qt 4.1
- Multithreaded: Separate monitoring from logging
- Logging to SQL-DB
- Web interface in Ruby
  - Configure connections to botnets (also has a mass import)
  - Browsing of collected data
- Plugins: Simulate different types of bot behavior
- Use SOCKS5 proxies
- Monitoring of pull-connections

Botspy and its environment



Performance

Performance:

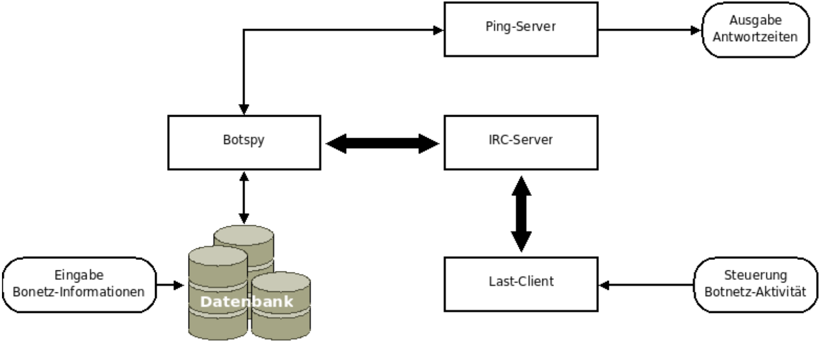
- ★ Accomplishing a task
- ★ Resources needed
- ★ Time needed

Here: Memory usage, response times, CPU load
Not: Database tuning, time needed for data analysis

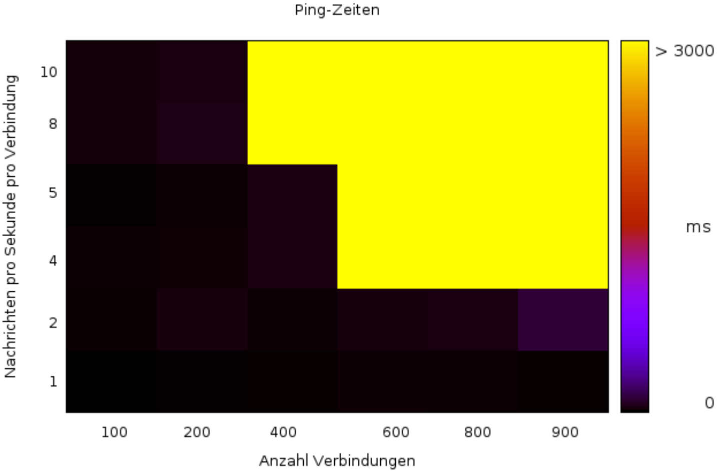
Memory usage

- ★ Without configured connections: 54 MB (32 MB being thread stacks, can be reduced)
- ★ 85KB per connection (increases almost linearly)
- ★ 250 byte per cached log message
- ★ With 900 connections and 100 messages cached per connection approx. 153 MB used

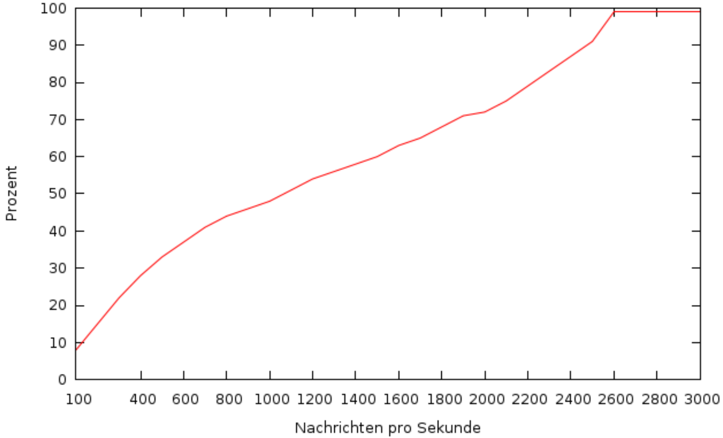
Measuring response times



Response times



CPU load


100
90
80
70
60
50
40
30
20
10
0
Prozent
100
400
600
800
1000
1200
1400
1600
1800
2000
2200
2400
2600
2800
3000
Nachrichten pro Sekunde

Statistics

Core observation time: March 17th 2007, 17:30 to April 25th 2007, 18:30 (39 days), only for the statistics, total observation was much longer.

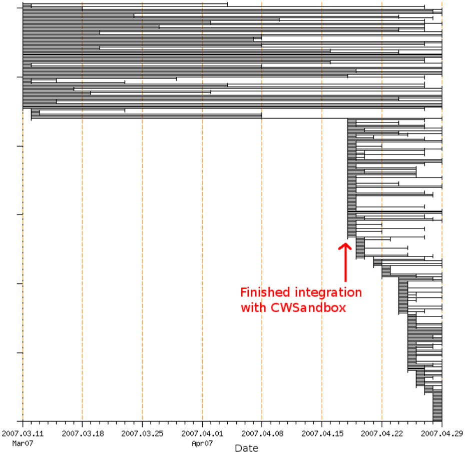
Only IRC style botnets

Criterion	**Number**	**Percent**
Monitored botnets total	362	100,0%
Reachable via TCP	314	86,7%
Communication with botnet possible	216	59,7%

Statistics

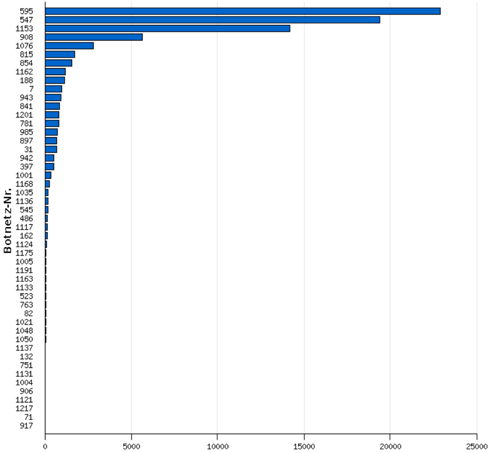
Criterion	Number	Percent
Communication with botnet possible	216	100,0%
Unique IP-addresses of C&C-servers	135	62,5%
Providing a names list	192	88,9%
Providing a real names list	15	6,9%
Has set a topic	170	78,7%
Communicates with PRIVMSG	150	69,4%
Uses PRIVMSG and topic	104	48,1%
Uses encryption	44	20,4%

Lifetime of botnets



- ★ One botnet was active for more than 250 days
- ★ Approx. 15 - 20 new botnets every day
- ★ Approx. 130 botnets at the same time
- ★ Only about 50% are active for more than two days
- ★ Problem: Some botnets run on public IRC servers

Size of botnets, top 50 botnets

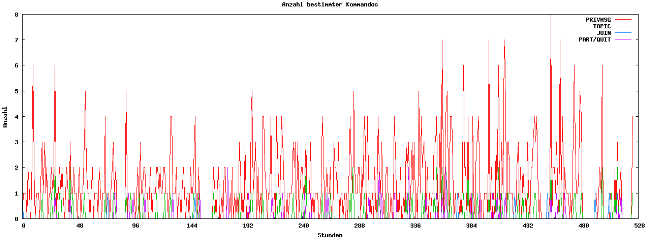


- ★ A total of 60.919 different host names have been seen
- ★ Only few botnets with more than 1000 host names
- ★ Problem: Fake host names: 2C307E3F.D97B7C4C. 85187735.IP
- ★ 48.061 unique IP-adresses could be resolved
- ★ Problem: Dynamic IP-addresses

TOP 20 autonomous systems with infected hosts

Number	AS-No.	Country	Network name	Percent
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%

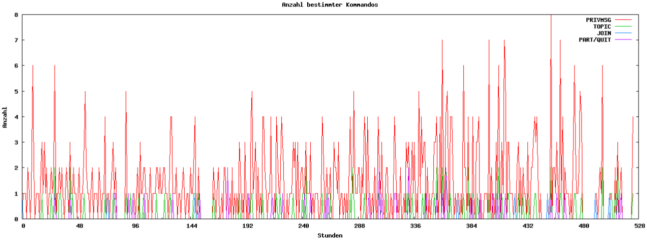
Communication patterns in botnets

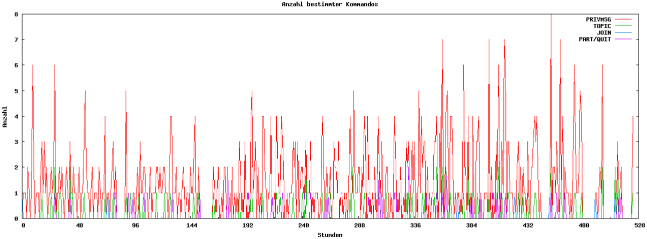


PRIVMSG 🟥
TOPIC 🟩
JOIN 🟦
PART/QUIT 🟪

← Botnet 366

Communication patterns in botnets





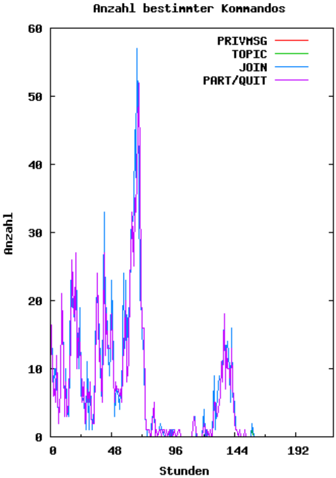
← Botnet 366

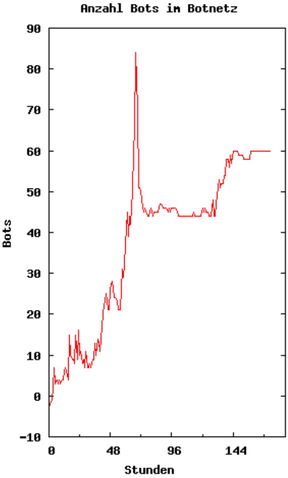
Botnet 371 has the same pattern as botnet 366

12 groups with 52 botnets

⇒ only 176 unique botnets

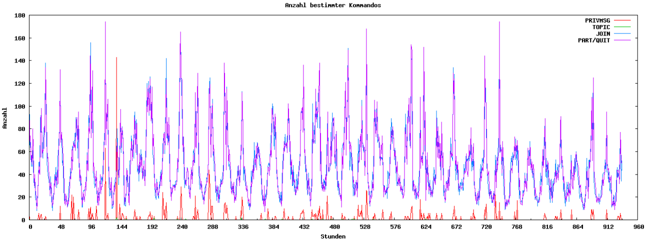
Growth of botnets

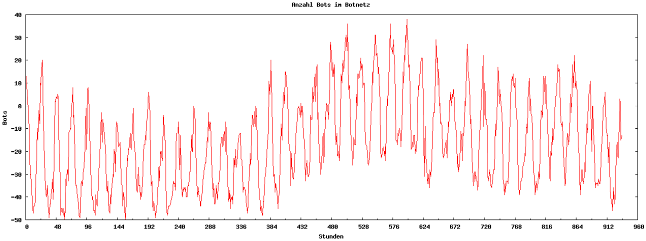




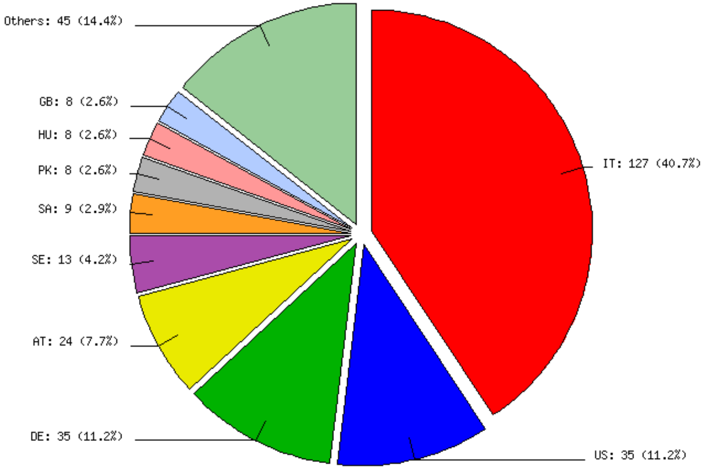
Communication patterns in botnets (locality)

Botnet 547:

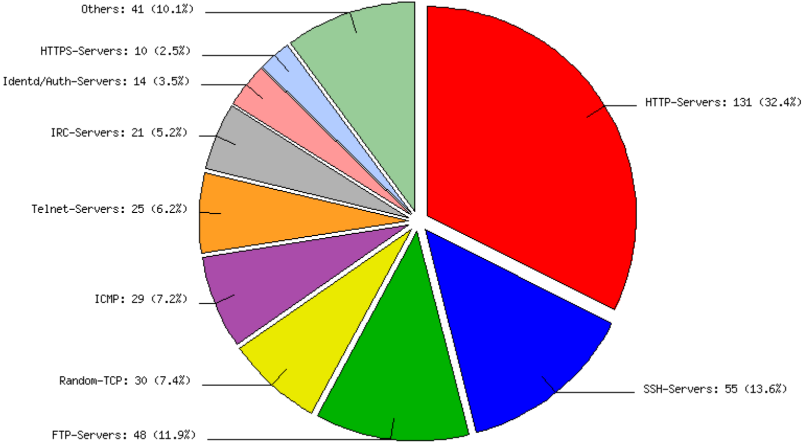




Distributed Denial of Service



Distributed Denial of Service



Distributed Denial of Service

DDoS targets:

- Targets are often dedicated servers or hosting providers
- The real target can only be guessed
- Reverse lookup often gives host names like:

  ```
  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
  ```
- In the end, only a war of the script-kiddies?

Conclusion and the future

- Much of our knowledge on botnets is based on guesswork
- We need more data

Botspy was developed to be easily extensible and adaptable. Tasks for the future:

- Collect and analyze more data
- Monitor peer-2-peer networks
- Monitor encrypted networks
- Automate analysis and integrate in web interface
- Integration with other systems, e.g. real-time notification about infected hosts

Questions?

(If there is still time left...)