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

Prof. Dr.-Ing. Felix Freiling
Dipl.-Inform. Thorsten Holz
RedTeam Pentesting GmbH
many others...
“Pose as a Friend, Work as a Spy”

(Robert Greene)
DJFelipec not available! DJFelipec privmsg #secret :!login cocacola

DJFelipec not available! DJFelipec 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!~ vwbvvg 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
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

- Infected Bots
- C&C Server
- Master

Motivation
- The Technology - Botspy
- Results

Conclusion and the Future
- A Short Introduction to Botnets
- Observation of Botnets

Claus R. F. Overbeck, RedTeam Pentesting GmbH
Botspy - Efficient Observation of Botnets
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
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

Botspy - Efficient Observation of Botnets
Response times

Performance Observations

Ping-Zeiten

Anzahl Verbindungen

Nachrichten pro Sekunde pro Verbindung

0

> 3000

Claus R. F. Overbeck, RedTeam Pentesting GmbH

Botspy - Efficient Observation of Botnets
Motivation

The Technology - Botspy

Results

Conclusion and the Future

Performance

Observations

CPU load

Claustrum F. Overbeck, RedTeam Pentesting GmbH

Botspy - Efficient Observation of Botnets
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

<table>
<thead>
<tr>
<th>Criterion</th>
<th>Number</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitored botnets total</td>
<td>362</td>
<td>100,0%</td>
</tr>
<tr>
<td>Reachable via TCP</td>
<td>314</td>
<td>86,7%</td>
</tr>
<tr>
<td>Communication with botnet possible</td>
<td>216</td>
<td>59,7%</td>
</tr>
</tbody>
</table>
### Statistics

<table>
<thead>
<tr>
<th>Criterion</th>
<th>Number</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication with botnet possible</td>
<td>216</td>
<td>100,0%</td>
</tr>
<tr>
<td>Unique IP-addresses of C&amp;C-servers</td>
<td>135</td>
<td>62,5%</td>
</tr>
<tr>
<td>Providing a names list</td>
<td>192</td>
<td>88,9%</td>
</tr>
<tr>
<td>Providing a real names list</td>
<td>15</td>
<td>6,9%</td>
</tr>
<tr>
<td>Has set a topic</td>
<td>170</td>
<td>78,7%</td>
</tr>
<tr>
<td>Communicates with PRIVMSG</td>
<td>150</td>
<td>69,4%</td>
</tr>
<tr>
<td>Uses PRIVMSG and topic</td>
<td>104</td>
<td>48,1%</td>
</tr>
<tr>
<td>Uses encryption</td>
<td>44</td>
<td>20,4%</td>
</tr>
</tbody>
</table>
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
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-addresses could be resolved.

Problem: Dynamic IP-addresses
TOP 20 autonomous systems with infected hosts

<table>
<thead>
<tr>
<th>Number</th>
<th>AS-No.</th>
<th>Country</th>
<th>Network name</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>10094</td>
<td>22927</td>
<td>AR</td>
<td>Telefonica de Argentina</td>
<td>21,00%</td>
</tr>
<tr>
<td>4007</td>
<td>7738</td>
<td>BR</td>
<td>Telecomunicacoes da Bahia S.A.</td>
<td>8,34%</td>
</tr>
<tr>
<td>3284</td>
<td>3320</td>
<td>DE</td>
<td>DTAG Deutsche Telekom AG</td>
<td>6,83%</td>
</tr>
<tr>
<td>2787</td>
<td>5617</td>
<td>PL</td>
<td>TPNET Polish Telecom_s commercial IP network</td>
<td>5,80%</td>
</tr>
<tr>
<td>2336</td>
<td>8167</td>
<td>BR</td>
<td>TELESC - Telecomunicacoes de Santa Catarina SA</td>
<td>4,86%</td>
</tr>
<tr>
<td>1286</td>
<td>8151</td>
<td>MX</td>
<td>Uninet S.A. de C.V.</td>
<td>2,68%</td>
</tr>
<tr>
<td>982</td>
<td>3209</td>
<td>DE</td>
<td>Arcor IP-Network</td>
<td>2,04%</td>
</tr>
<tr>
<td>923</td>
<td>12741</td>
<td>PL</td>
<td>INTERNETIA-AS Netia SA</td>
<td>1,92%</td>
</tr>
<tr>
<td>801</td>
<td>8422</td>
<td>DE</td>
<td>NETCOLOGNE NETCOLOGNE AS</td>
<td>1,67%</td>
</tr>
<tr>
<td>634</td>
<td>8447</td>
<td>AT</td>
<td>TELEKOM-AT Telekom Austria AutonomousSystem</td>
<td>1,32%</td>
</tr>
<tr>
<td>627</td>
<td>7303</td>
<td>AR</td>
<td>Telecom Argentina S.A.</td>
<td>1,30%</td>
</tr>
<tr>
<td>493</td>
<td>9269</td>
<td>HK</td>
<td>CTIHK-AS-AP City Telecom (H.K.) Ltd.</td>
<td>1,03%</td>
</tr>
<tr>
<td>435</td>
<td>5462</td>
<td>GB</td>
<td>CABLEINET Telewest Broadband</td>
<td>0,91%</td>
</tr>
<tr>
<td>425</td>
<td>8404</td>
<td>CH</td>
<td>CABLECOM Cablecom GmbH</td>
<td>0,88%</td>
</tr>
<tr>
<td>402</td>
<td>3352</td>
<td>ES</td>
<td>TELEFONICA-DATA-ESPAÑA Internet Access Network of TDE</td>
<td>0,84%</td>
</tr>
<tr>
<td>364</td>
<td>5413</td>
<td>GB</td>
<td>AS5413 PIPEX Communications</td>
<td>0,76%</td>
</tr>
<tr>
<td>357</td>
<td>12353</td>
<td>PT</td>
<td>VODAFONE-PT Vodafone Portugal</td>
<td>0,74%</td>
</tr>
<tr>
<td>343</td>
<td>25019</td>
<td>SA</td>
<td>SAUDINETSTC-AS Autonomus System Number for SaudiNet</td>
<td>0,71%</td>
</tr>
<tr>
<td>339</td>
<td>18881</td>
<td>BR</td>
<td>Global Village Telecom</td>
<td>0,71%</td>
</tr>
<tr>
<td>337</td>
<td>3269</td>
<td>IT</td>
<td>ASN-IBSNAZ TELECOM ITALIA</td>
<td>0,70%</td>
</tr>
<tr>
<td>16805</td>
<td></td>
<td>Other</td>
<td></td>
<td>34,97%</td>
</tr>
</tbody>
</table>
Communication patterns in botnets
Communication patterns in botnets

Botnet 371 has the same pattern as botnet 366

12 groups with 52 botnets

⇒ only 176 unique botnets
Growth of botnets

![Graph 1: Anzahl bestimmter Kommandos](image1)

- PRIVMSG
- TOPIC
- JOIN
- PART/QUIT

![Graph 2: Anzahl Bots in Botnetz](image2)
Communication patterns in botnets (locality)

Botnet 547:

![Graphs showing communication patterns in botnets](image-url)
Distributed Denial of Service

- IT: 127 (40.7%)
- US: 35 (11.2%)
- DE: 35 (11.2%)
- AT: 24 (7.7%)
- SE: 13 (4.2%)
- SA: 9 (2.9%)
- PK: 8 (2.6%)
- HU: 8 (2.6%)
- GB: 8 (2.6%)
- Others: 45 (14.4%)
Distributed Denial of Service

- HTTP-Servers: 131 (32.4%)
- SSH-Servers: 55 (13.6%)
- FTP-Servers: 48 (11.9%)
- Random-TCP: 30 (7.4%)
- ICMP: 29 (7.2%)
- Telnet-Servers: 25 (6.2%)
- IRC-Servers: 21 (5.2%)
- Identd/Auth-Servers: 14 (3.5%)
- HTTPS-Servers: 10 (2.5%)
- Others: 41 (10.1%)
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-to-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...)