Fighting the Botnet Ecosystem

Renaud BIDOU

Smart Network. Smart Business.
Bots, bots, bots
**Botnet classification**

1. **Monolithic**
   - Coherent, all features in one binary
   - Evolution may not be trivial
     - Kaiten, SDBot, Spybot

2. **Modular**
   - Evolution voluntarily made easy
   - Choice of appropriate language (C++)
     - AgoBot

3. **Barnum**
   - Set of heterogeneous scripts
   - Often relies on local interpreters
     - PHP bots, GTBot
Botnet classification

1. No control
   - Automated behavior
   - Less flexible, more resistant
     - Morris worm, CodeRed

2. Public infrastructure
   - Reliable and « anonymous »
   - Mostly IRC, P2P upcoming
     - 95% of botnets

3. Private CC Channel
   - Usually based on covert channels
   - Better stealth at short term
     - Sobig

Internal Structure
Command model
Propagation mechanism
Botnet classification

Internal Structure

Command model

Propagation mechanism

1. No
   - No propagation function
   - Relies on 3rd party
     - Kaiten

2. Single
   - Exploits one specific vulnerability
   - May need human action
     - CodeRed, Netsky, Mytob

3. Modular
   - Use of multiple exploits
   - Transported by different vectors
     - Morris worm, SDBot, MPack
1988 – *Morris Worm*

- Multiple vectors propagation
- « Unvoluntarily » blocked the internet
1988 – Morris Worm
1993 – EggDrop

- First « real » worm
- Propagated through IRC channels
1988 – Morris Worm
1993 – EggDrop
1998 – GTBot

- First bot based on IRC C&C Channel
- Competition with PrettyPark for the title
1988 – Morris Worm
1993 – EggDrop
1998 – GTBot
2000 – *Major DDoS*

- First visible DDoS for dummies
- Trin00, TFN, Stacheldraht
Short botnet history

1988 – Morris Worm
1993 – EggDrop
1998 – GTBot
2000 – Major DDoS
2001 – CodeRed

- First « large scale » worm
- Failed to DoS white house web site
Short botnet history

1988 – Morris Worm
Multiple vectors propagation
« Unvoluntarily » blocked the internet

1993 – EggDrop
First « real » worm
Propagated through IRC channels
First bot based on IRC C&C Channel
Competition with PrettyPark for the title

1998 – GTBot

2000 – Major DDoS
Trin00, TFN, Stacheldraht

2001 – CodeRed

2002 – Rise of the Giants

- AgoBot – Professional design
- SDBot – Still the most popular IRC bot
Short botnet history

1988 – Morris Worm
1993 – EggDrop
1998 – GTBot
2000 – Major DDoS
2001 – CodeRed
2002 – Rise of the Giants
2003 – Mass mailing worms

- PoC: Melissa, «I love you»
- Netsky, Mytob
Short botnet history

1988 – Morris Worm

1993 – EggDrop

1998 – GTBot

2000 – Major DDoS

2001 – CodeRed

2002 – Rise of the Giants

2003 – Mass mailing worms

2004 – Witty

- First « 0-day » worm
- Launched 36 hours after discovery
Short botnet history

1988 – Morris Worm
1993 – EggDrop
1998 – GTBot
2000 – Major DDoS
2001 – CodeRed
2002 – Rise of the Giants
2003 – Mass mailing worms
2004 – Witty

Since 2005 – The Botnet Ecosystem

- Turning technology into money
- A new actor on the field: organized crime
- No more « state of the art » research
- Evolution and variant of existing technologies
- Short-term exploits
Birth and growth of a botnet
Ecosystem actors

The Good
« Innocent » Systems

The Bad
Malicious Systems

The Ugly
0-day, botnet, malware « markets »
Birth of a botnet via spam

Markets

BUY

ATTACK

C&C

Relays

Botnet
Birth of a MPack-like botnet

Markets → BUY → C&C → SET → Relays → Botnet
**Basic propagation**

```
[urX]-700159 #foobar :.advscan lsass 200 5 0 -r -s
PRIVMSG #foobar :[lsass]: Exploiting IP: 200.124.175.XXX
PRIVMSG #foobar :[TFTP]: File transfer started
```
Advanced propagation

warez.cdkeys

AgoBot

WAREZ SITE
Making money with botnets

**Direct cash generation**

- **Spam**
  - Impacting stock values
  - Stealing credential (phishing)
  - « Nigerian scam »
  - Advertisement

- **Extortion**
  - DDoS
  - Private data stealth

- **On-demand Hacking**

---

*Graph showing data related to spam activity.*
Botnet market

- Renting the botnet & services
  - Time limited DoS generator
  - Mail relays & spam campaigns
  - Proxy chains to provide anonymity
  - Advertisement via pop-ups
  - Malware distribution

Technology markets

- 0-day markets
  - Corporate vs. Underground
  - « Promoted » by security laws
  - IE vulnerability ~ 50,000 $

- Tools / malware market
  - « Hacking for dummies »
  - MPack ~ 500 $
Most of current security concerns are involved in the ecosystem
Hurting the ecosystem

**Laws**

- **Financial**
  - Common laws against crime money
  - Increase risks ad reduce interest for criminals
  - Falls into organized crime prevention methods
  - Efficient for « big » business not for 10.000$ exploits

- **IT specific**
  - Illegal behaviors repression
    - spam, intrusion etc.
    - more or less effective
  - Prevention of research
    - Adopted by many countries
    - Forbid security research and publication
    - Leads to opposite effects, searchers going underground
Hurting the ecosystem

Laws impact

No impact on operations
**Education**

- Computer security basics
  - Anti-virus update
  - Apply vendors security updates
  - Relatively efficient

- Good usage of IT
  - Do not click on everything!
  - Avoid suspicious sites
  - Only use legal software and licenses
  - No illegal download of MP3, DivX
  - Stop believing everybody wants to give you money!
  - Merely useless: humans will be humans
Education impact

Mostly limited by lack of application ⇒ kill users
Technologies

- Host-based technologies
  - Local hygiene
    - Patches, user accounts not admin, data encryption etc.
  - Security technologies
    - Anti-viruses, anti-spyware, HIPS, personal firewall
  - Good efficiency but relies on end-user system

- Network-based technologies
  - Traffic control
    - Firewalls, NAC, Proxys
  - Security enforcement
    - Anti-Spam, IPS, URL filtering
  - Efficient but very heterogeneous
Hurting the ecosystem

Technology impact

Expensive and heterogeneous ⇒ efficiency limited
All Together

Hurting the ecosystem

The fight can be won ⇒ Theoretically
Reasons for a disaster

- Unlimited scope
  - World-wide phenomenon
    - reduces local laws impact
    - International prosecution maybe impossible
  - Everybody can be a victim
    - enterprise, home users, universities etc.
    - different level of education, security technologies etc.

- Global security impossible to provide
  - Cost
  - Management
    - No one as a all-in-one solution
    - Even if some claim they do …
  - Lack of knowledge
The command & control channel
Targeting the C&C Channel

Strike to the heart

C&C channel is single point of failure
Communication Protocols

- IRC
  - 80% of current botnets
  - Distributed and Reliable
  - Clear text, most command known

- P2P
  - Some experiments
    - PhatBot (AgoBot variant) uses the WASTE network
  - Probable future of IRC network

- Proprietary channels
  - Usually based on Covert Channels and/or encryption
  - Needs a « private » infrastructure
  - Efficient at short-term but quickly blocked
    - TOR to change this status …
**Prevention technologies**

- **Filtering**
  - ✓ Efficient against basic channels, who needs IRC anyway?
  - ✗ Useless in all other cases

- **Signatures**
  - ✓ Efficient against common commands issued through cleartext channels
  - ✓ Efficient against major botnet variants
  - ✓ Efficient to **block** most P2P communications
  - ✗ Useless for encrypted and « home-made » channels
## Prevention technologies

- **Protocol anomalies**
  - Comes together with stateful analysis
  - Efficient against covert channels
  - Useless for other C&C channels

- **Behavioral analysis**
  - Efficient in detecting abnormal use of legitimate traffic
  - Relatively efficient against encrypted channels
  - Useless against « low volume » C&C channels
**Autonomous Botnets**
- Few but famous: Morris Worm, CodeRed
- Definitely a pain
- AI to make them more and more dangerous

**Everybody’s concern**
- Channels to be blocked wherever computers are
- Unmanaged systems & networks will remain active

**One step behind anyway**
- Prevention techniques are known
- Channels are designed to bypass
- Development takes time
Conclusion
Another never-ending story?

Complete security is not realistic

Prevention scope should be global

Legal impact is long-term

Secure behavior is becoming usual

Most effects can be mitigated

Botnet resources can be exhausted