Neutralizing Peer-to-Peer Botnets Deliberately Destroying Drones

Dennis Andriesse

VU University Amsterdam

May 14, 2013

Cui Honorem, Honorem

Christian Rossow, VU University, The Netherlands

Tillmann Werner, CrowdStrike, USA

Brett Stone-Gross, Dell SecureWorks, USA

Daniel Plohmann, University of Bonn, Germany

Christian Dietrich, IFIS, Germany

Herbert Bos, VU University, The Netherlands

Acknowledgements

The ShadowServer Foundation

SURFnet

CERT.PL

Who am I?

- Ph.D. candidate, System and Network Security, VU Amsterdam
- Binary (de)obfuscation, reverse engineering and malware

The System and Network Security Group

- Security research group led by Herbert Bos
- Currently mostly focused on the Rosetta project
  - Developing reverse engineering techniques for complex / obfuscated / hard to reverse binaries

Further Reading

Further reading

- This is a public version of the talk; sensitive slides were cut :-(
- Will make all information public ASAP
- The following references provide more detailed information
- Will update the tech report as info becomes non-sensitive

C. Rossow, D. Andriesse, T.Werner, B. Stone-Gross, D. Plohmann, C. Dietrich, and H. Bos, *"P2PWNED: Modeling and Evaluating the Resilience of Peer-to-Peer Botnets"*, Proceedings of the 34th IEEE Symposium on Security and Privacy, (San Francisco, CA, USA), IEEE Computer Society, May 2013.
`http://tinyurl.com/p2pwned-2013`

D. Andriesse and H. Bos, *"An Analysis of the Zeus Peer-to-Peer Protocol"*, Technical Report IR-CS-74, VU University Amsterdam, May 2013.
`http://tinyurl.com/zeus-tech-report-2013`

Introduction to Botnets

Introduction to Botnets

What is a botnet?

- Network of malware–infected computers (*bots*)
- Controlled by *botmaster* to perform malicious actions
- Typically contains 100.000 - 1.000.000 bots

Introduction to Botnets

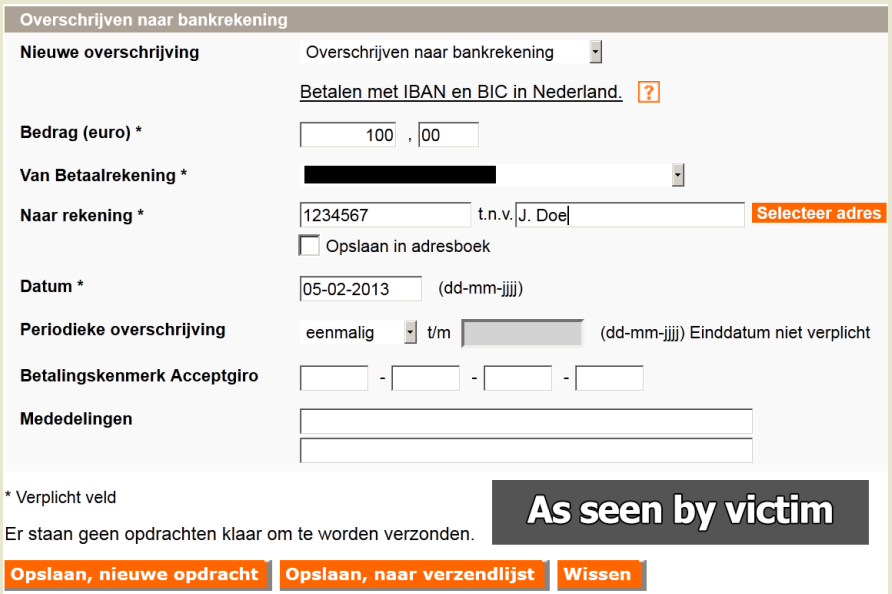
Damage caused by botnets

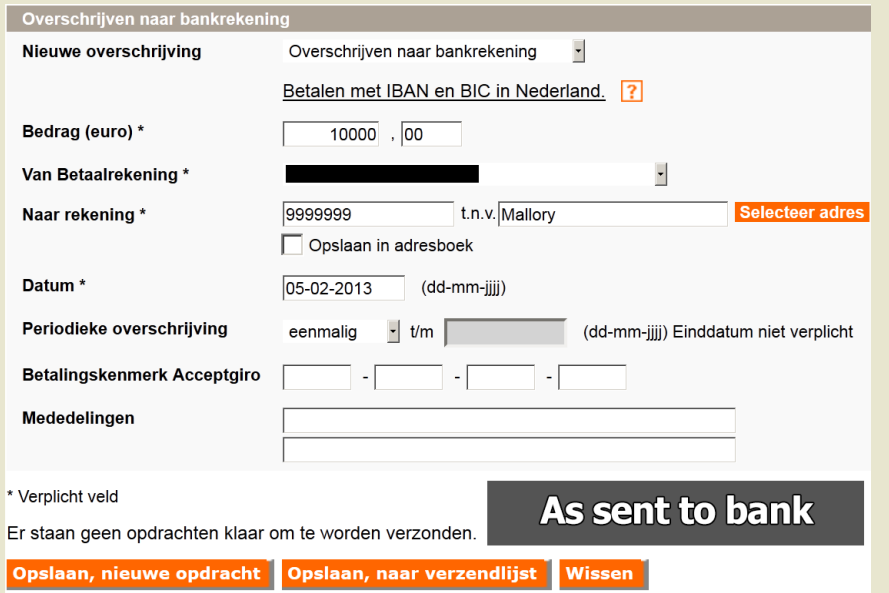
- Distributed Denial of Service (DDoS) attacks
- Man in the Browser (MitB) attacks
- Credential theft (banking credentials, facebook accounts, . . .)
- Spamming
- Installing more malware

  . . .

Stealing money with botnets

- Man in the Browser attacks are a popular way to steal money
- Bot hooks into your browser
- Steals money by altering web forms behind the scenes





Impact of Botnet Attacks

Financial damage in the Netherlands

- Dutch citizens are losing thousands to financial malware, as shown in "Kassa" in September 2012
- Largely due to botnets implementing MitB attacks

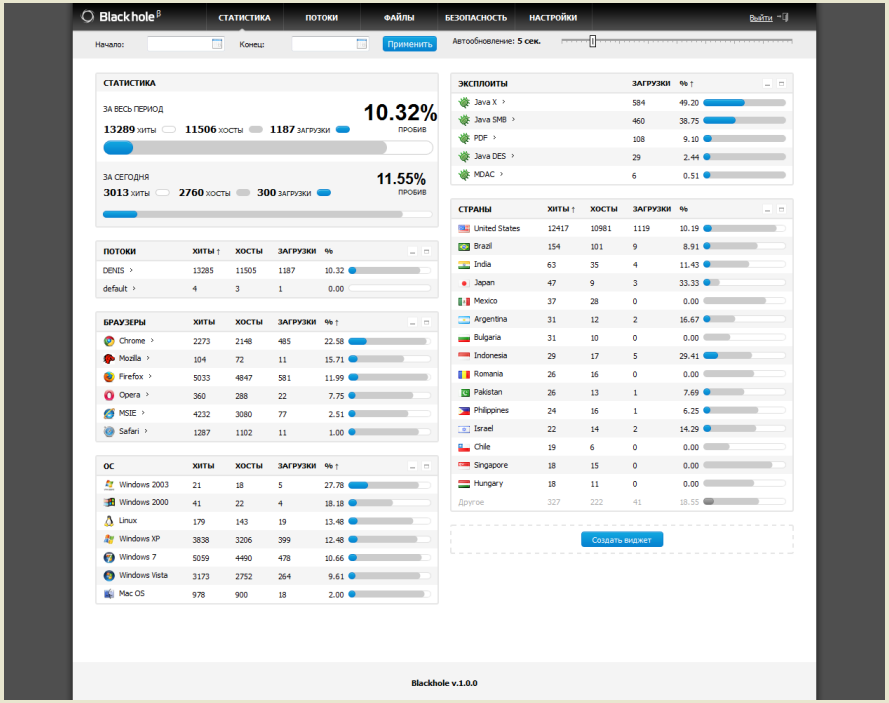
Credential theft example: Call center employee

- Torpig stole thousands of credit card numbers
- Researchers found a single victim where 30 numbers were stolen
  - Call center employee working from home
  - Stolen credit card numbers belonged to customers

Infection Vectors

How to get infected

- Drive-by download
  1. Visit a malware-spreading website
  2. Website attempts to exploit your browser
  3. If your browser is vulnerable, the exploit installs malware
- Exploit kits can be bought in the underground community



Drive-by Download Examples

Miami Dolphins

- American Football team, hacked 3 days before Super Bowl

Drive-by Download Examples

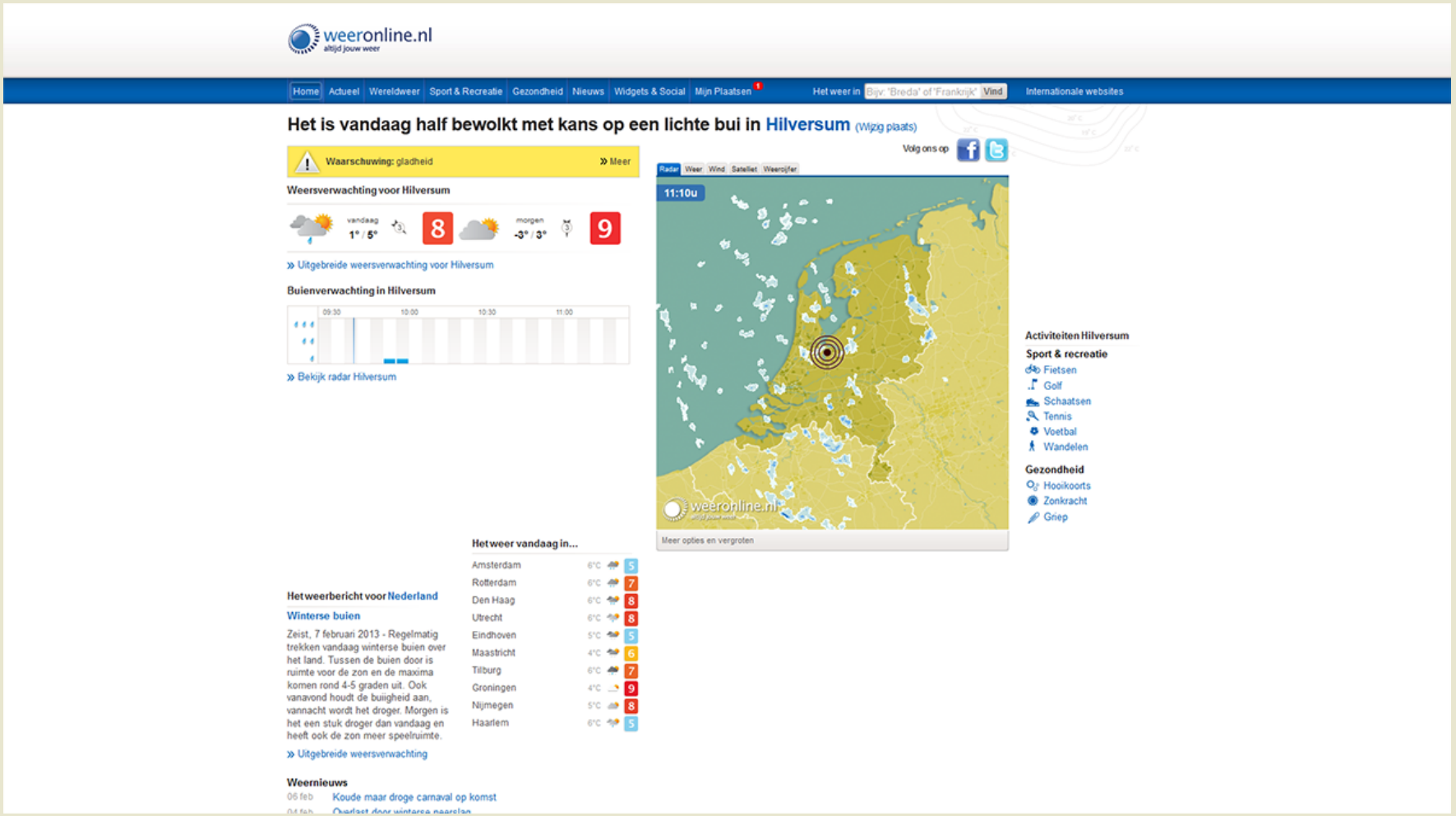
NU.nl

- Closer to home, NU.nl served malware via its advertising network

Drive-by Download Examples

Weeronline.nl

- Even checking the weather report could get you infected



Infection Vectors

How to get infected

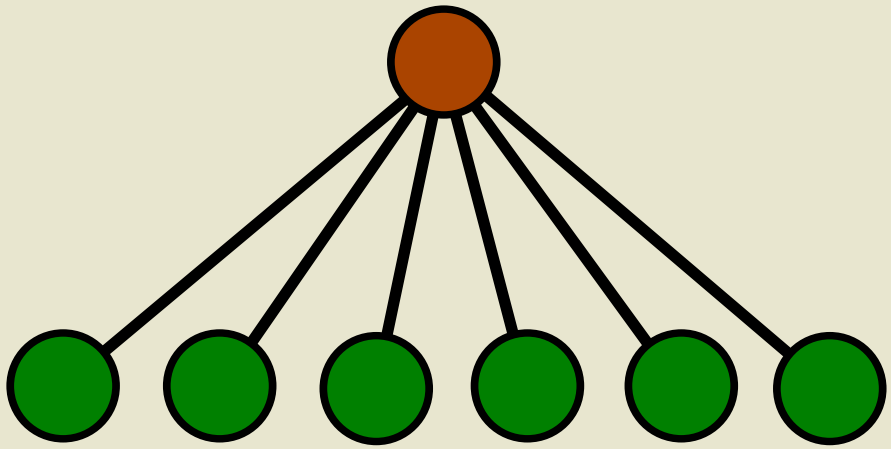
- Pay-per-install
  - Pay authors of existing malware to install ("drop") your malware
  - Very quick way to get lots of infections

Evolution of Botnets

Evolution of Botnets

Centralized botnets

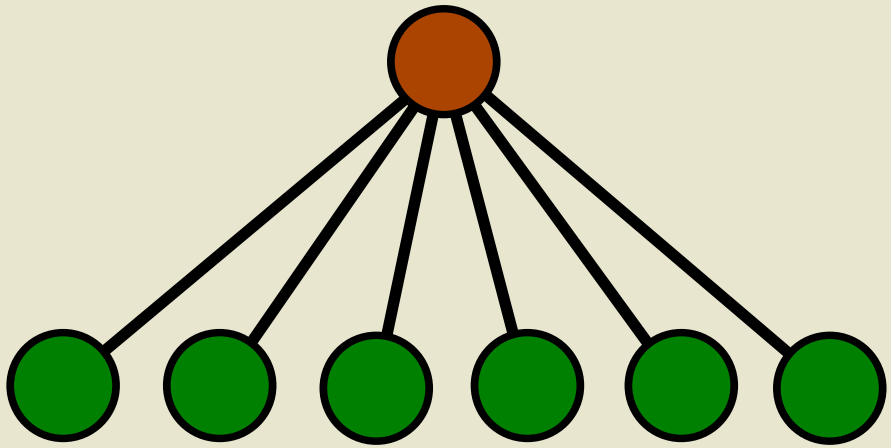
- Original botnets were centralized
- *Command and Control* (*C2*) server spreads commands to bots
- First botnets based on IRC (a chat protocol)
  - Bots enter the "chat room" and listen to commands
- Later botnets used HTTP
  - Bots fetch commands from a "web server"



Evolution of Botnets

Centralized botnets

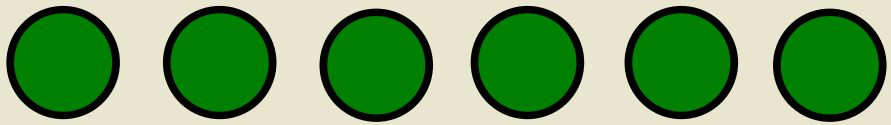
- Simple, easy to maintain for the bad guys
- Easy to disable for the good guys
  - Just take out the C2 server



Evolution of Botnets

Centralized botnets

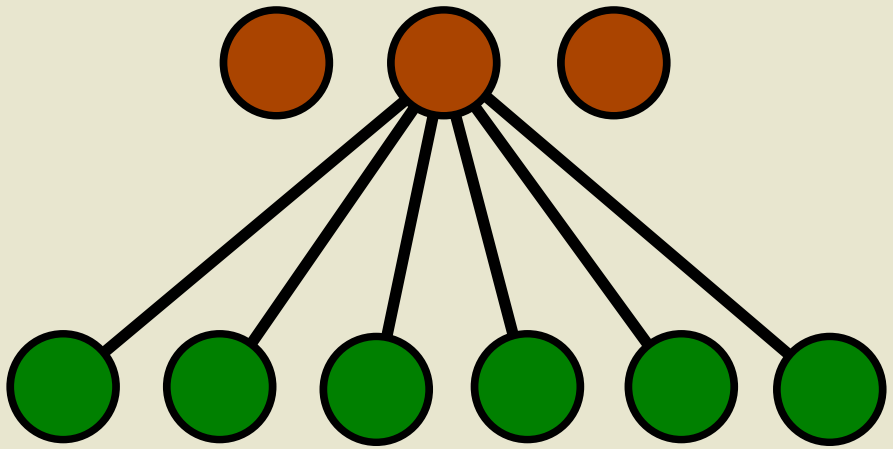
- Simple, easy to maintain for the bad guys
- Easy to disable for the good guys
  - Just take out the C2 server



Evolution of Botnets

Redundant infrastructure

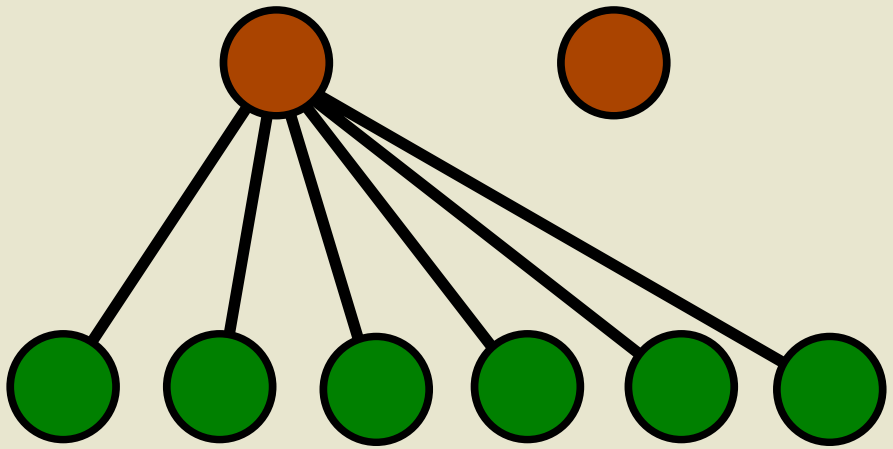
- Early way to strengthen centralized botnets: multiple C2 servers
- If one of the servers is disabled, bots just switch to another



Evolution of Botnets

Redundant infrastructure

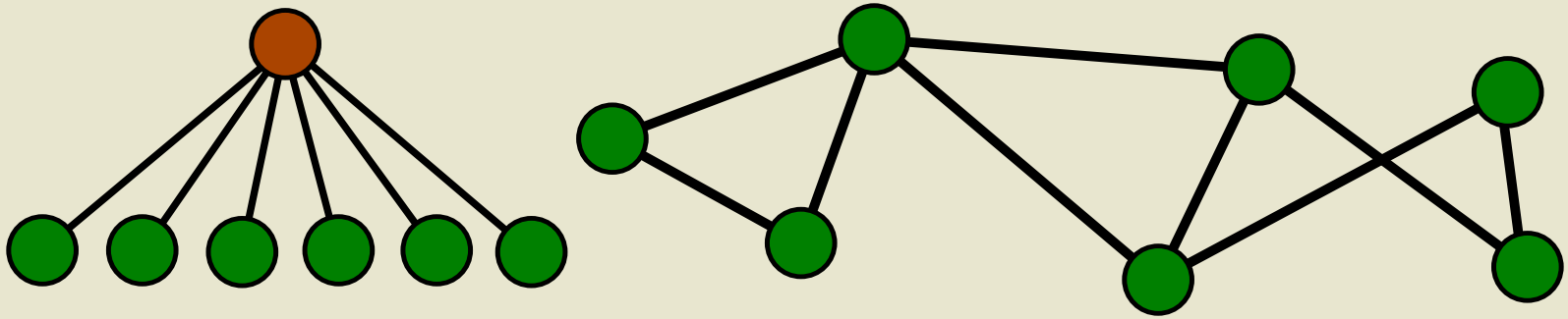
- Early way to strengthen centralized botnets: multiple C2 servers
- If one of the servers is disabled, bots just switch to another



Evolution of Botnets

Peer-to-Peer (P2P) botnets

- Centralized botnets are vulnerable because of their C2 servers
- P2P botnets have no centralized C2 servers
  - Every bot knows some of the other bots
  - Bots use P2P communication to spread commands
  - Much more resilient against takedowns



Peer-to-Peer Botnet Examples

Current P2P botnets

- Sality
  - January 2008
  - Pay-per-install
- ZeroAccess/Sirefef
  - May 2009
  - Pay-per-install
- **Zeus**
  - **October 2011**
  - **Credential theft**
- Kelihos/Hlux v4
  - March 2012
  - Spam

Attacking P2P Botnets

Attacking P2P Botnets

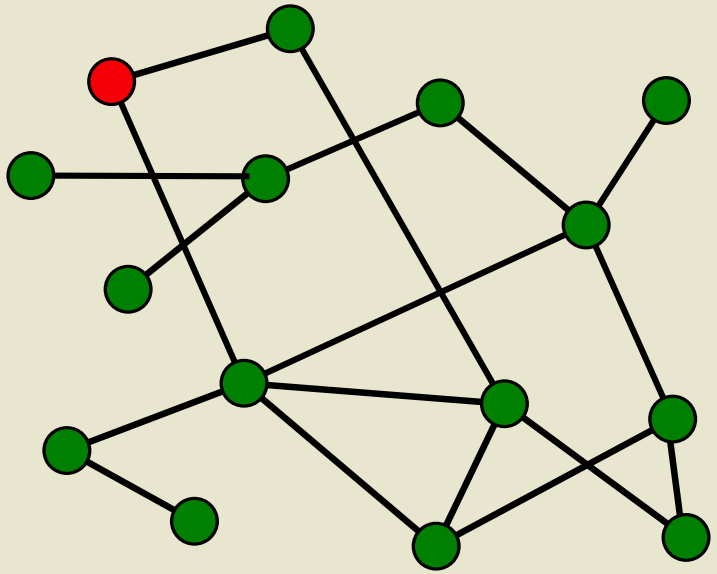
Commanding bots to uninstall

- Usually not possible because of command signing
- Bredolab (centralized) did not use command signing
- Team High Tech Crime performed a complete takeover in 2010
- They were rewarded with a Big Brother Award

Attacking P2P Botnets

Reconnaissance

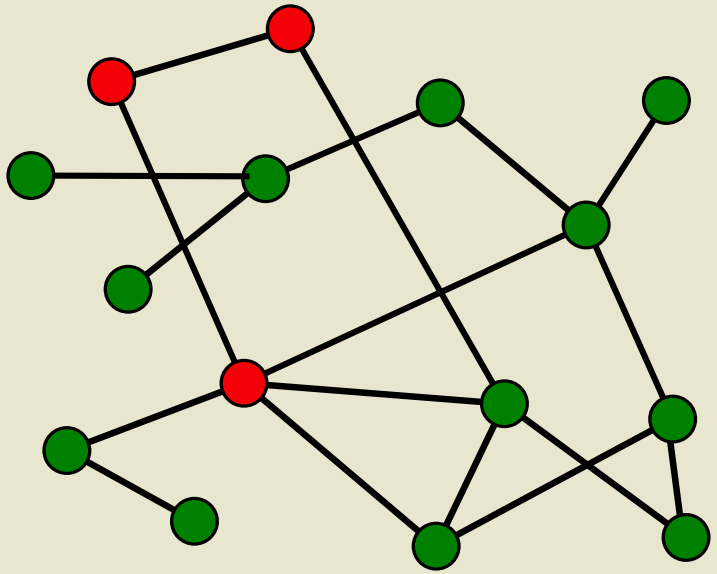
- Reconnaissance attacks try to find all the bots
  - Know how big the botnet is
  - Report bot addresses to Internet providers
- Abuse botnet's maintenance mechanism:
  1. Start with a few known bot addresses
  2. Ask these bots which other bots they know
  3. Repeat for newly found bots



Attacking P2P Botnets

Reconnaissance

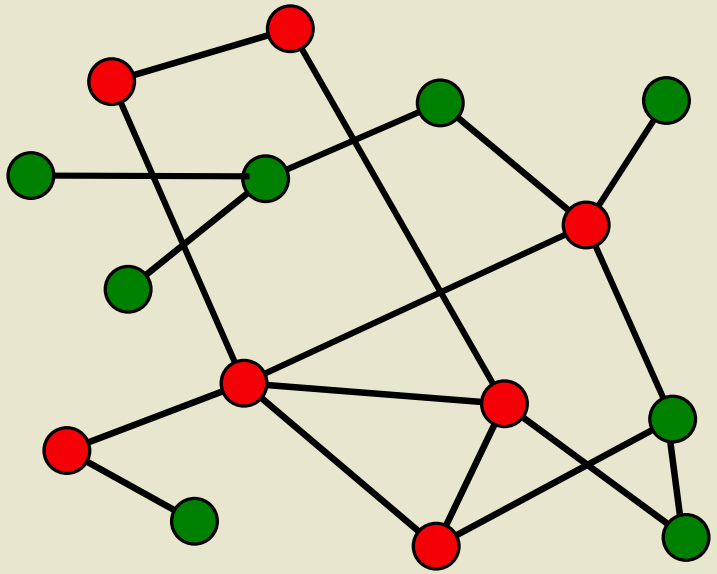
- Reconnaissance attacks try to find all the bots
  - Know how big the botnet is
  - Report bot addresses to Internet providers
- Abuse botnet's maintenance mechanism:
  1. Start with a few known bot addresses
  2. Ask these bots which other bots they know
  3. Repeat for newly found bots



Attacking P2P Botnets

Reconnaissance

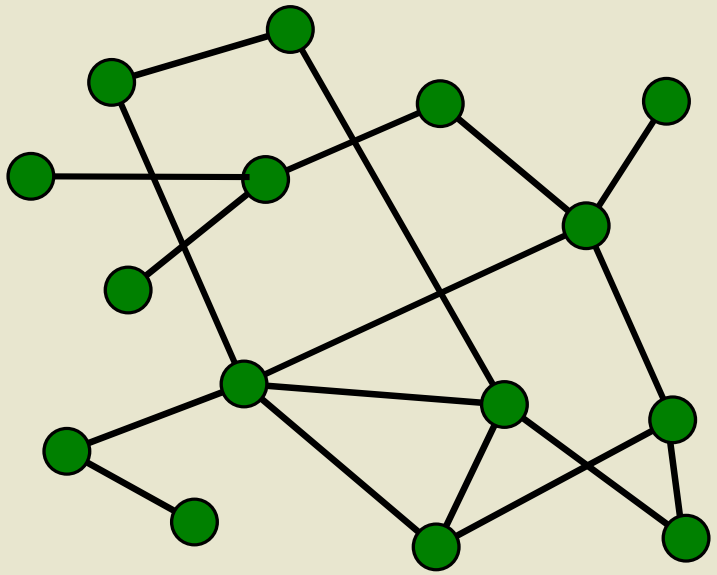
- Reconnaissance attacks try to find all the bots
  - Know how big the botnet is
  - Report bot addresses to Internet providers
- Abuse botnet's maintenance mechanism:
  1. Start with a few known bot addresses
  2. Ask these bots which other bots they know
  3. Repeat for newly found bots



Attacking P2P Botnets

Sinkholing

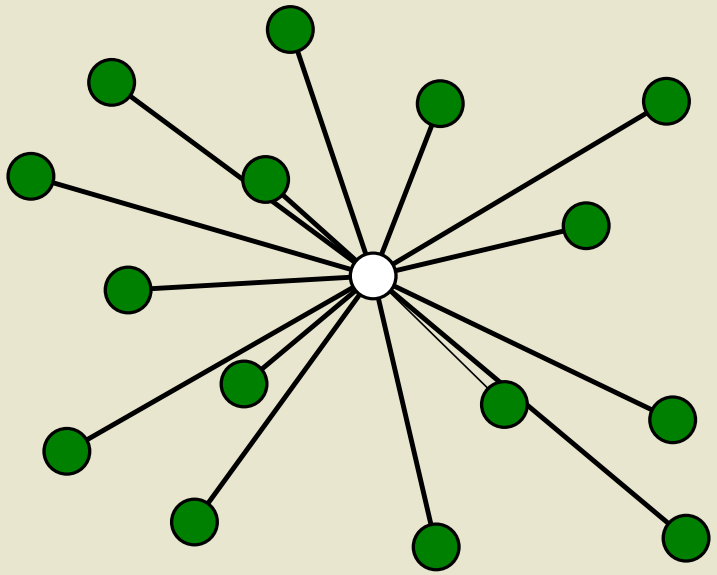
- Sinkholing attacks try to disconnect bots from each other
- Requires a way to modify bots' *peer lists*
- Try to redirect all bots to a benign *sinkhole* server



Attacking P2P Botnets

Sinkholing

- Sinkholing attacks try to disconnect bots from each other
- Requires a way to modify bots' *peer lists*
- Try to redirect all bots to a benign *sinkhole* server



Introduction to P2P Zeus

Introduction to P2P Zeus

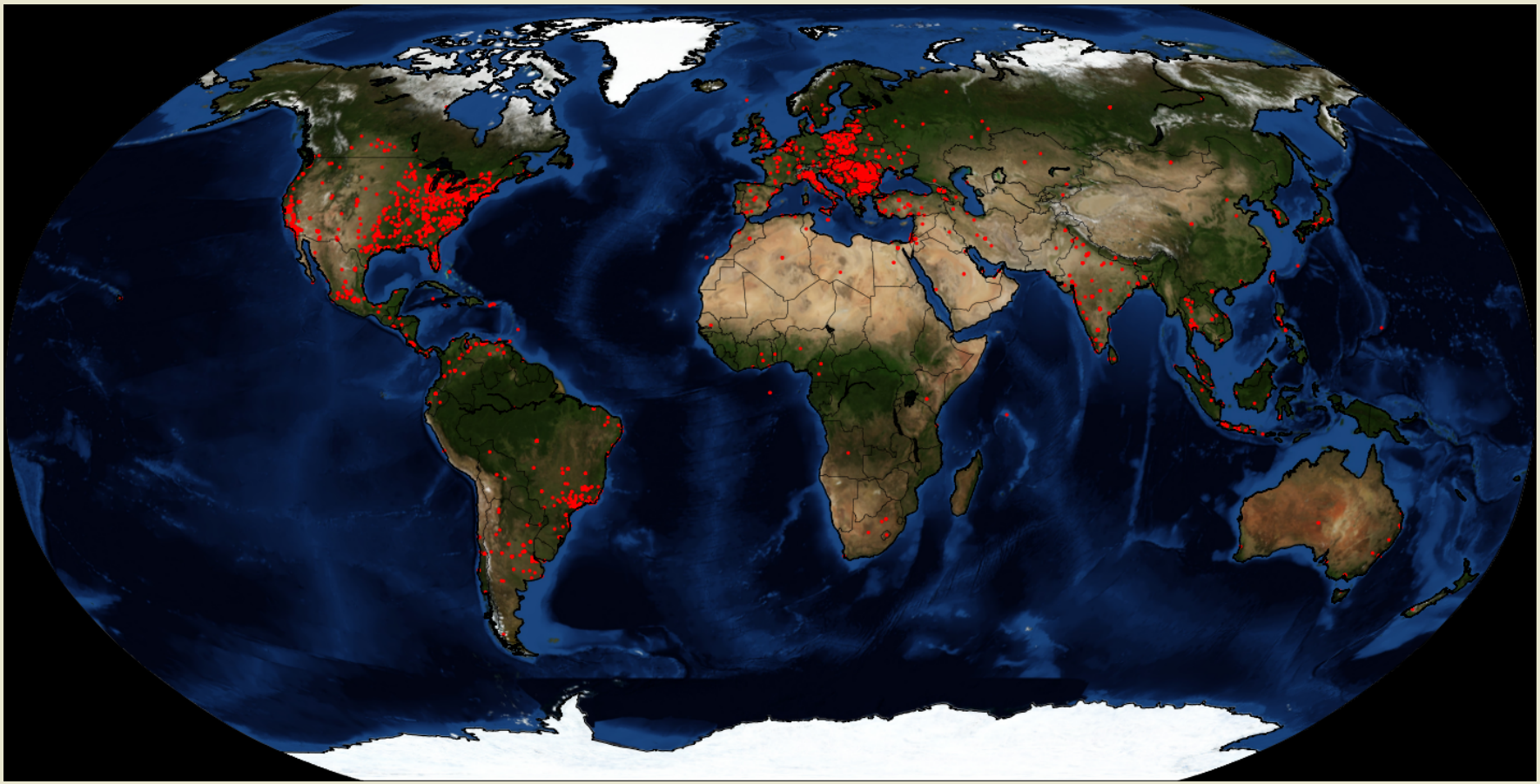
The Zeus Bot

- Banking trojan, information stealer
- Centralized version around since 2007
- Sold as DIY toolkit for $4000
- FBI tracked a group in 2010 which stole over $70m with it

Introduction to P2P Zeus

P2P Zeus/Gameover

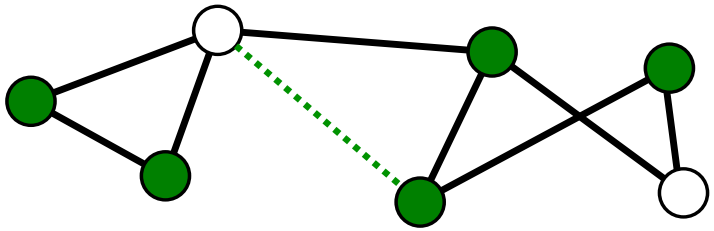
- Zeus evolved into a P2P variant around October 2011
- The P2P network currently contains 200.000 bots



Botnet Topology

P2P Layer

- Daily configuration updates
- Weekly binary updates



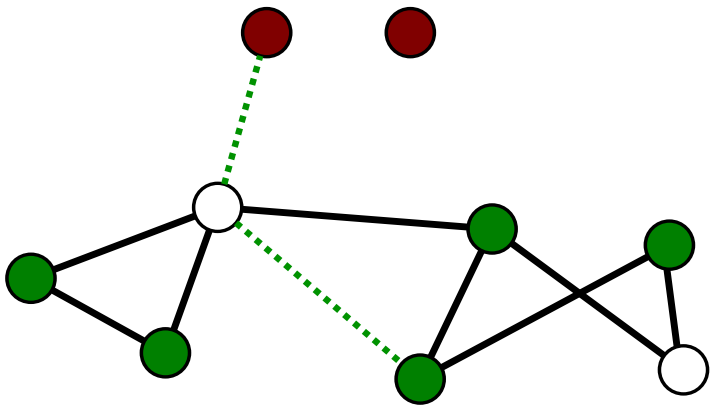
Botnet Topology

P2P Layer

- Daily configuration updates
- Weekly binary updates

Proxy Nodes

- Announced by special messages
- Route C2 communication
  - Stolen data
  - Commands



Botnet Topology

P2P Layer

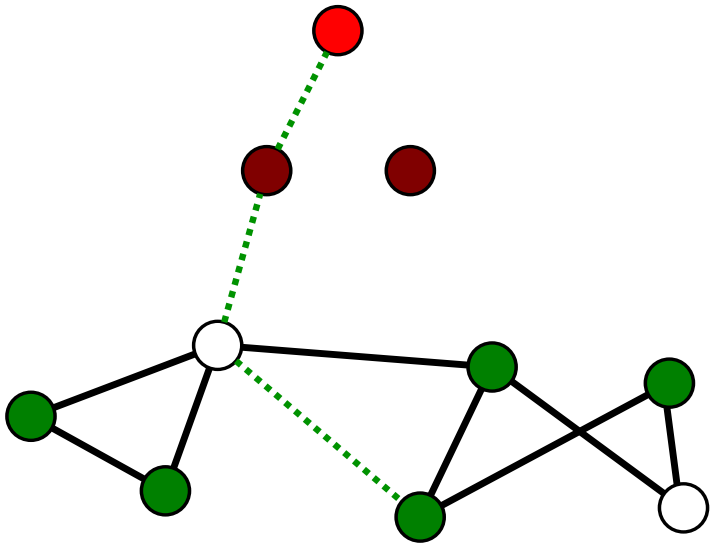
- Daily configuration updates
- Weekly binary updates

Proxy Nodes

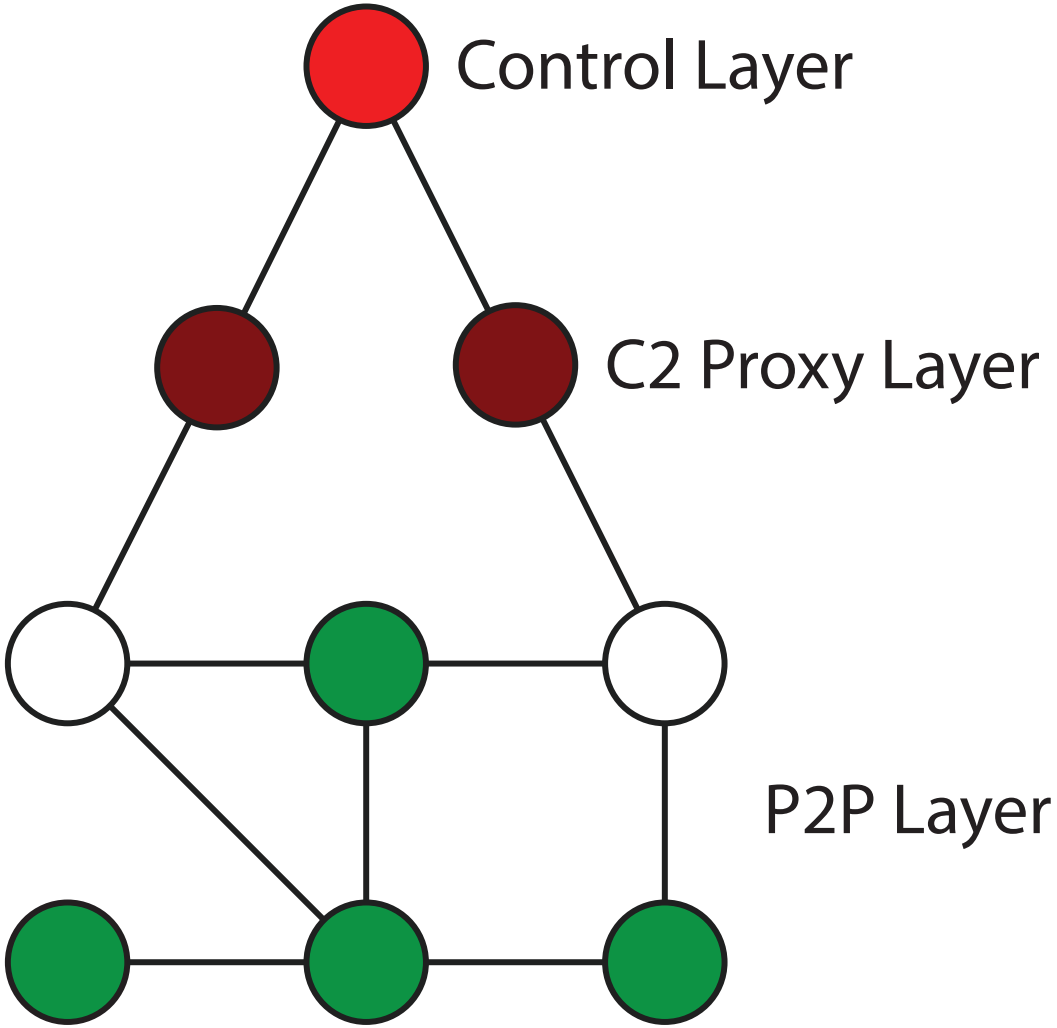
- Announced by special messages
- Route C2 communication
  - Stolen data
  - Commands

C2 Proxies

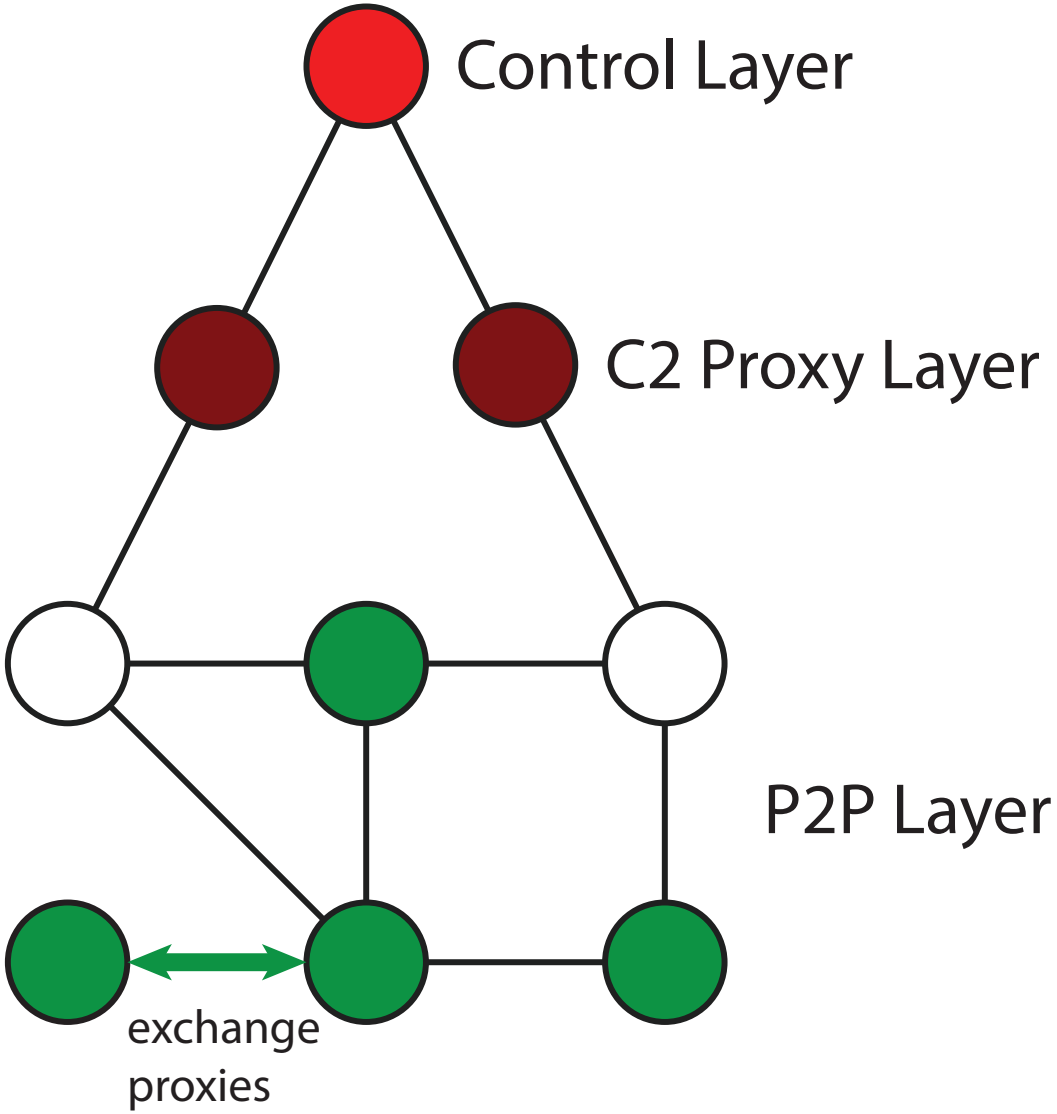
- Plain HTTP proxies
- Additional layer between botnet and backend



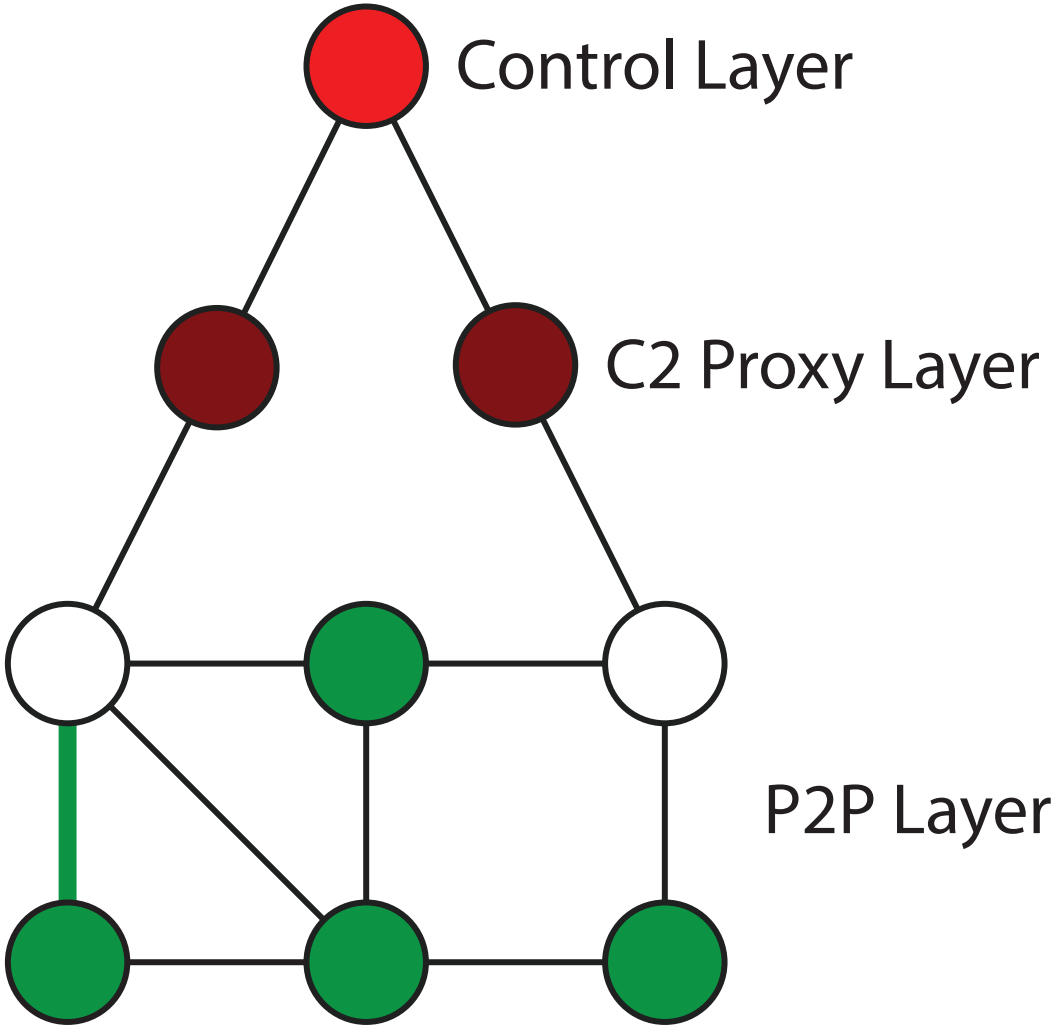
C2 Communication



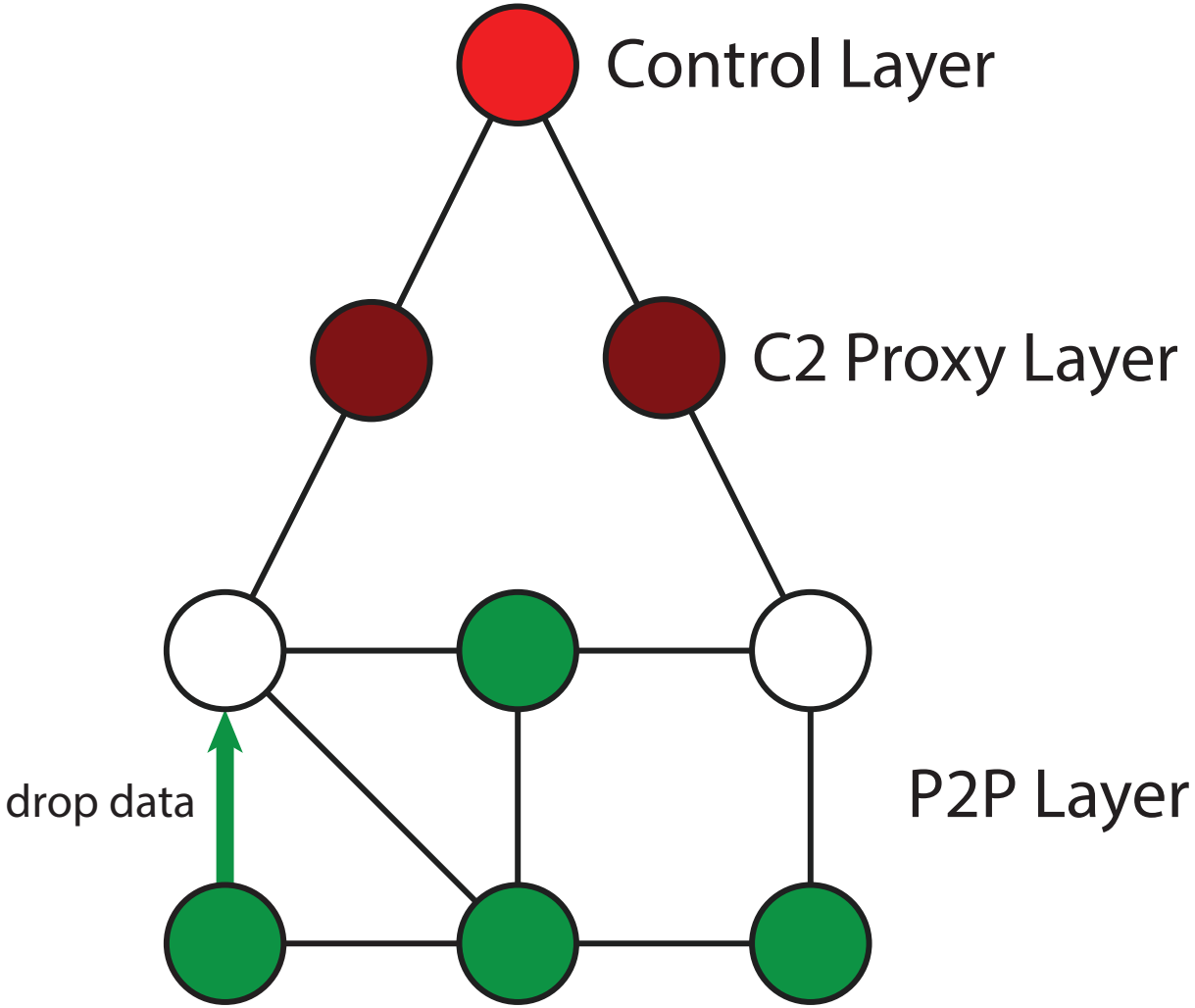
C2 Communication



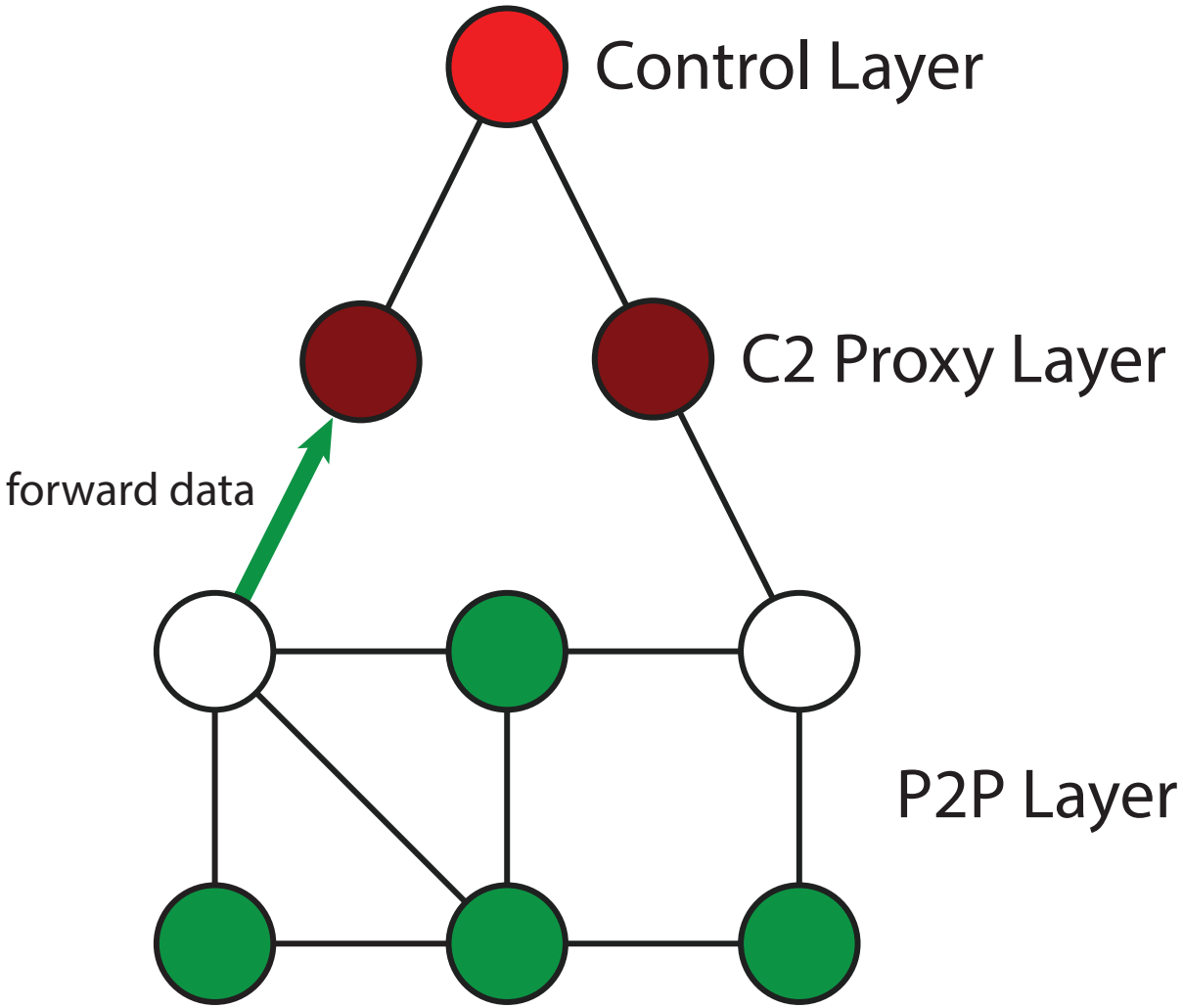
C2 Communication



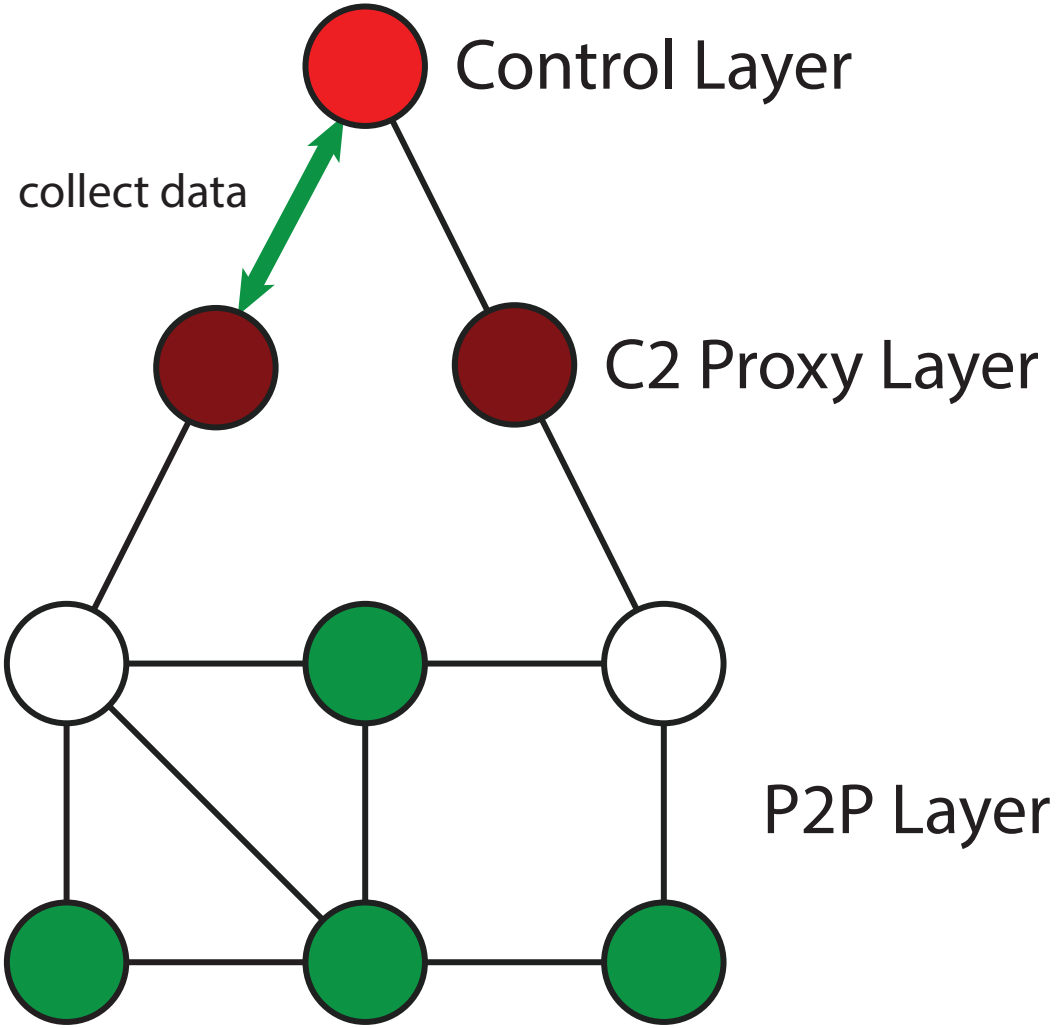
C2 Communication



C2 Communication



C2 Communication



A Backup Channel

Domain Name Generation

- Bots that cannot connect to the botnet launch a DGA
- Generates 1000 domain names per week
  - Starts trying from random initial domain
  - Downloads new seed peer list

```
$ ./zeus_dga.py -d 23.01.2013 -o zeus-dga-domains.txt

Generated 1000 domain names:
   .biz: 166
   .com: 266
  .info: 133
   .net: 134
   .org: 134
    .ru: 167
```

zxqcmbamypfmtuwqoibuoy.ru
xthzltayhiusmbdiblrrgukvts.com
fqgyssobrgtopmftxslbqeqy.net
nvqmjsfzdcmxsmdsgofeil.org
...

Conclusion

Take away message

- Botnets are becoming increasingly advanced
- Some P2P botnets already quite nasty to disable
  - All kinds of resilience measures
  - Ethical problems with remote cleanups
- Must decide when the cure becomes worse than the disease