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

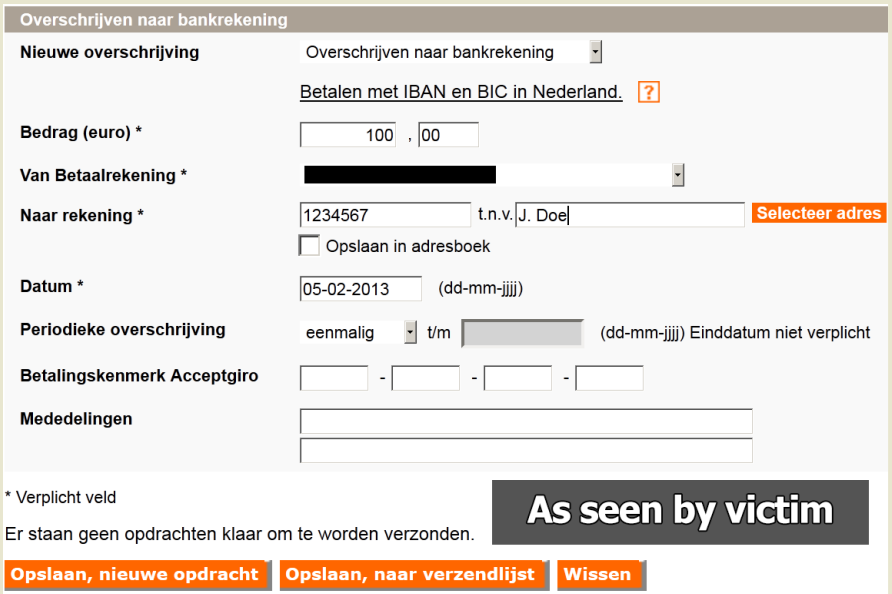
Damage caused by botnets

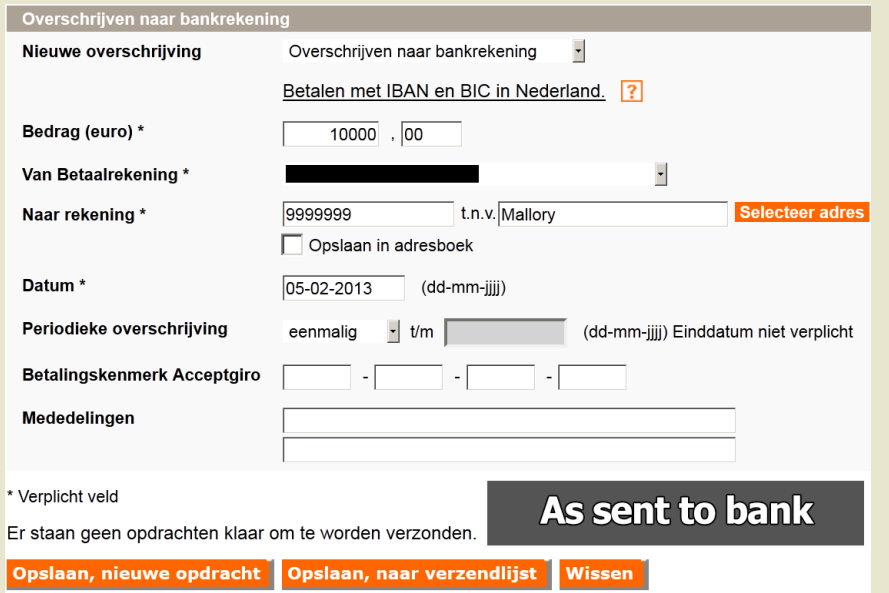
- Distributed Denial of Service (DDoS) attacks
- Man in the Browser (MitB) attacks
- Credential theft (banking credentials, facebook accounts, . . .)
- Spamming
- Installing more malware

  . . .

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

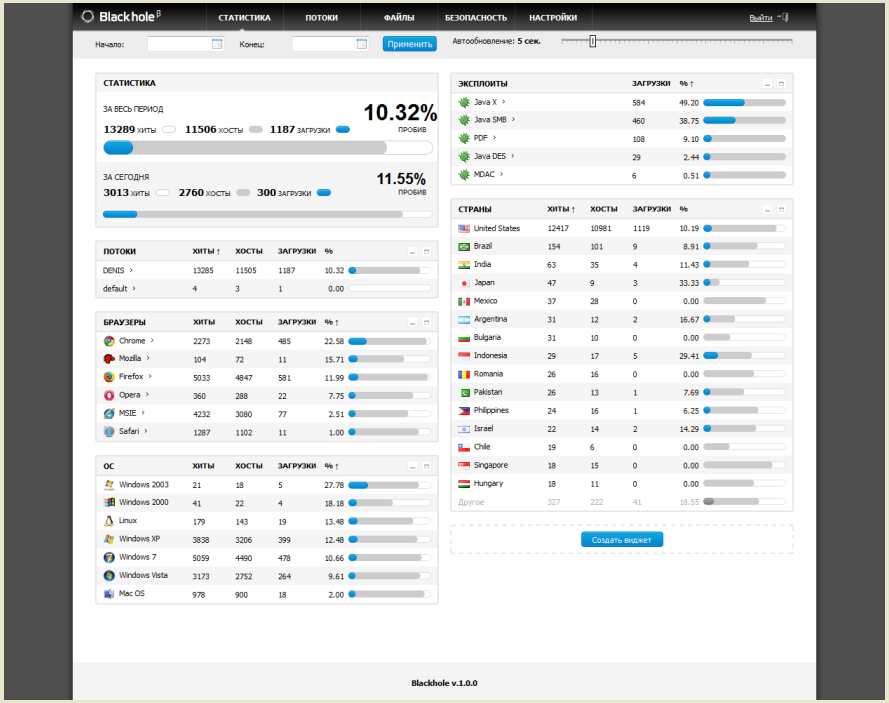
Credential theft example: Call center employee

- 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

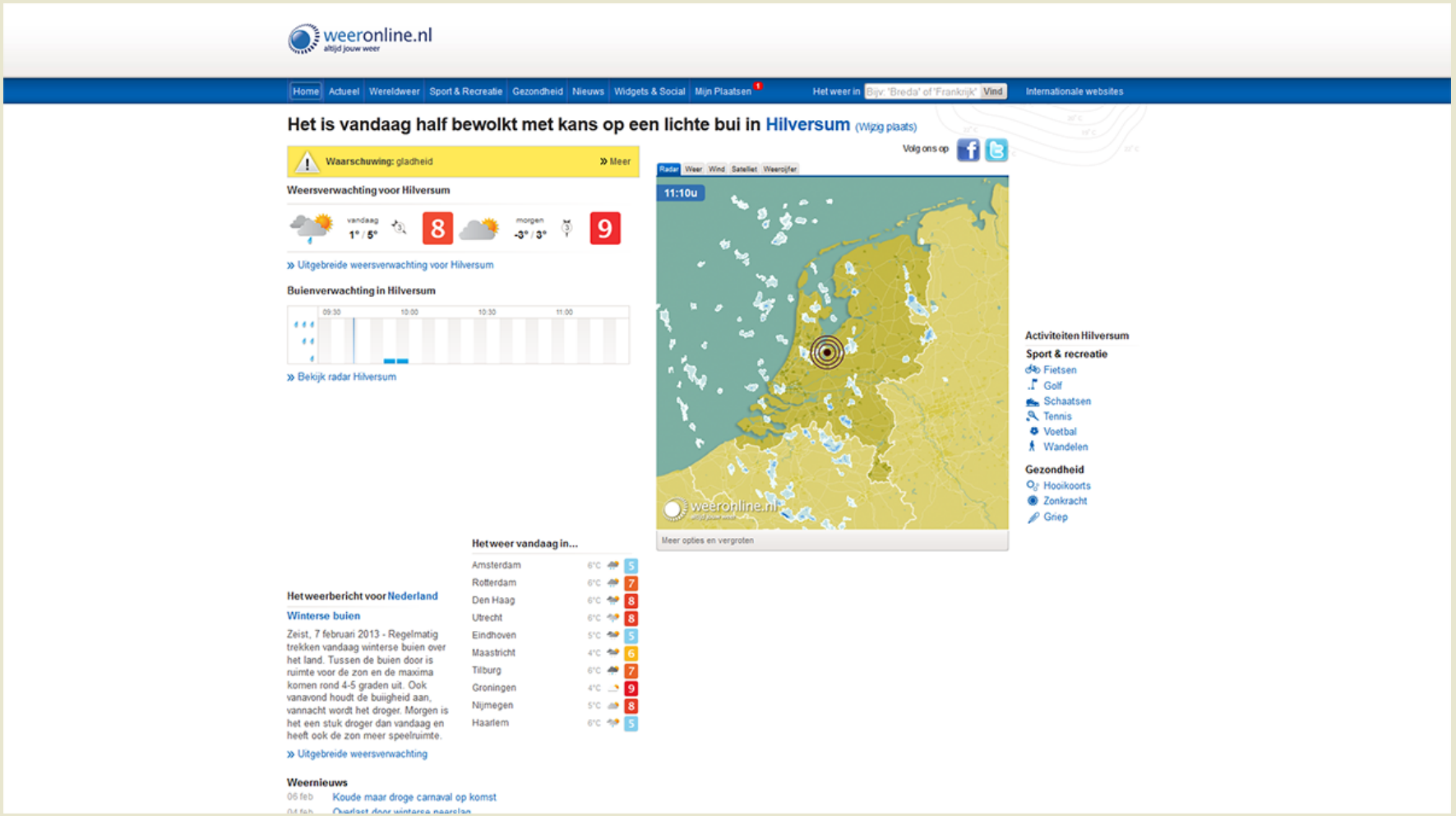
NU.nl

- 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

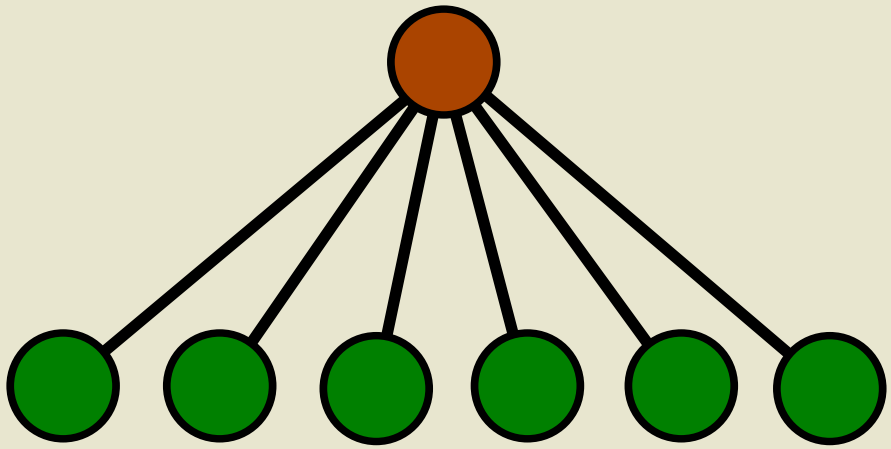
- Pay-per-install
  - Pay authors of existing malware to install ("drop") your malware
  - Very quick way to get lots of infections

Evolution of Botnets

Evolution of Botnets

Centralized botnets

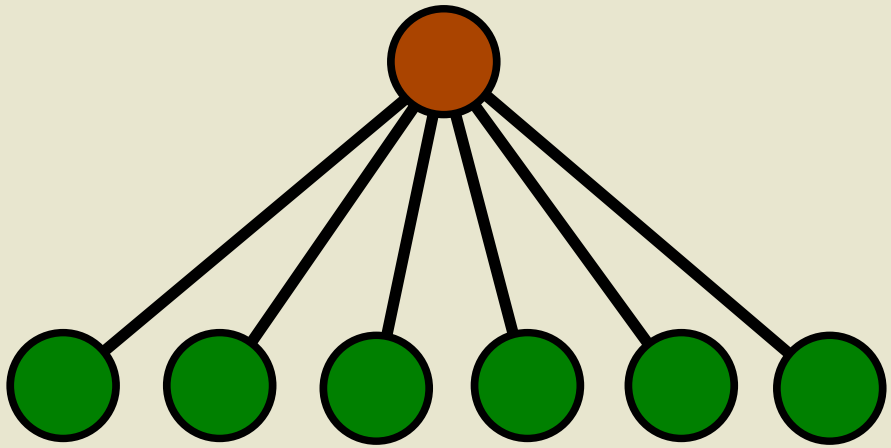
- Original botnets were centralized
- *Command and Control* (*C2*) server spreads commands to bots
- First botnets based on IRC (a chat protocol)
  - Bots enter the "chat room" and listen to commands
- Later botnets used HTTP
  - Bots fetch commands from a "web server"



Evolution of Botnets

Centralized botnets

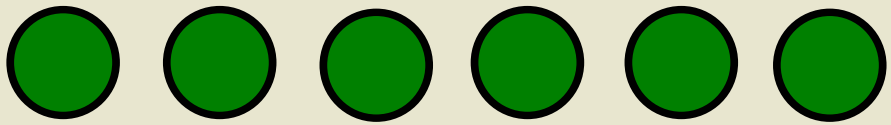
- Simple, easy to maintain for the bad guys
- Easy to disable for the good guys
  - Just take out the C2 server



Evolution of Botnets

Centralized botnets

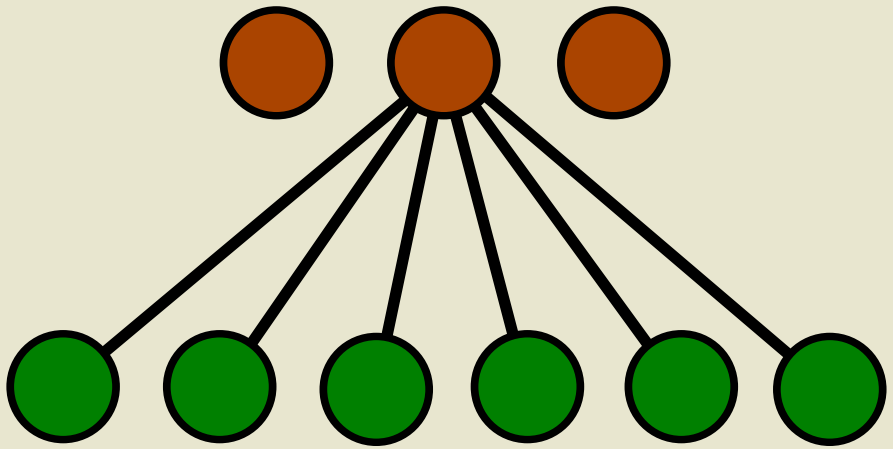
- Simple, easy to maintain for the bad guys
- Easy to disable for the good guys
  - Just take out the C2 server



Evolution of Botnets

Redundant infrastructure

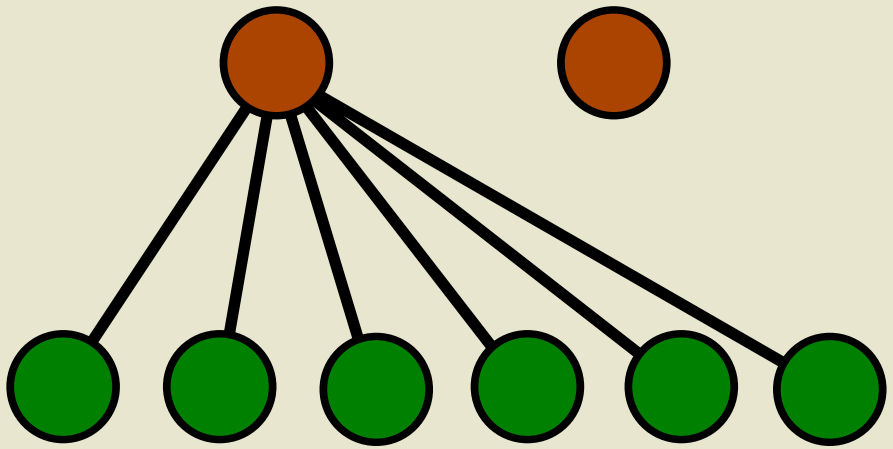
- Early way to strengthen centralized botnets: multiple C2 servers
- If one of the servers is disabled, bots just switch to another



Evolution of Botnets

Redundant infrastructure

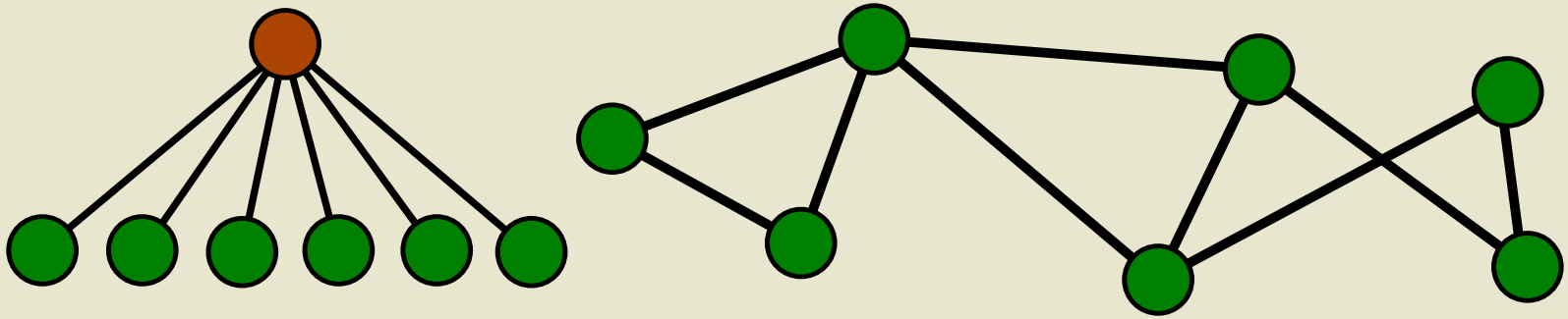
- Early way to strengthen centralized botnets: multiple C2 servers
- If one of the servers is disabled, bots just switch to another



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

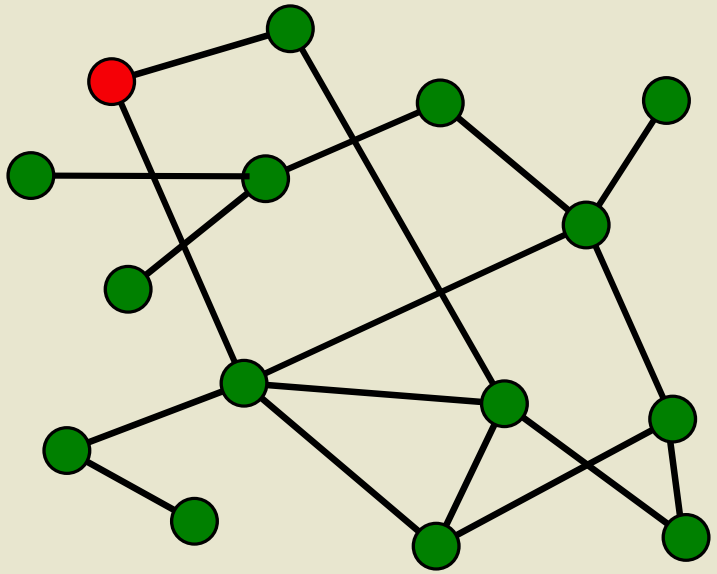
Commanding bots to uninstall

- 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

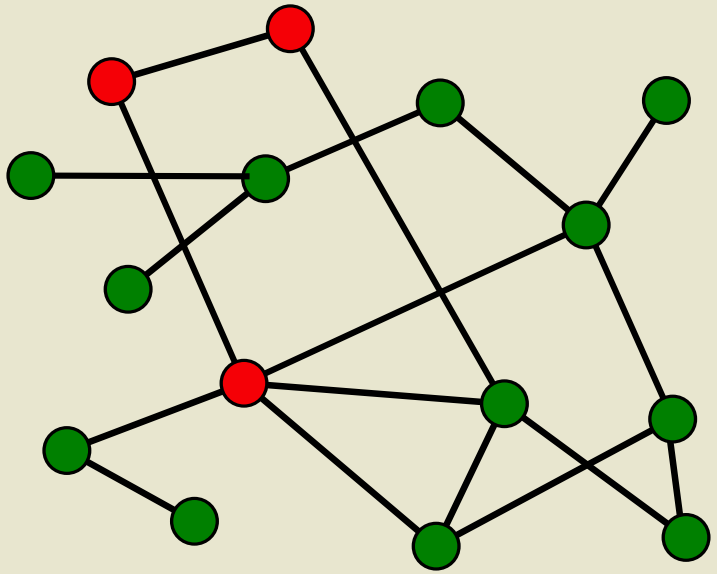
- Reconnaissance attacks try to find all the bots
  - Know how big the botnet is
  - Report bot addresses to Internet providers
- Abuse botnet's maintenance mechanism:
  1. Start with a few known bot addresses
  2. Ask these bots which other bots they know
  3. Repeat for newly found bots



Attacking P2P Botnets

Reconnaissance

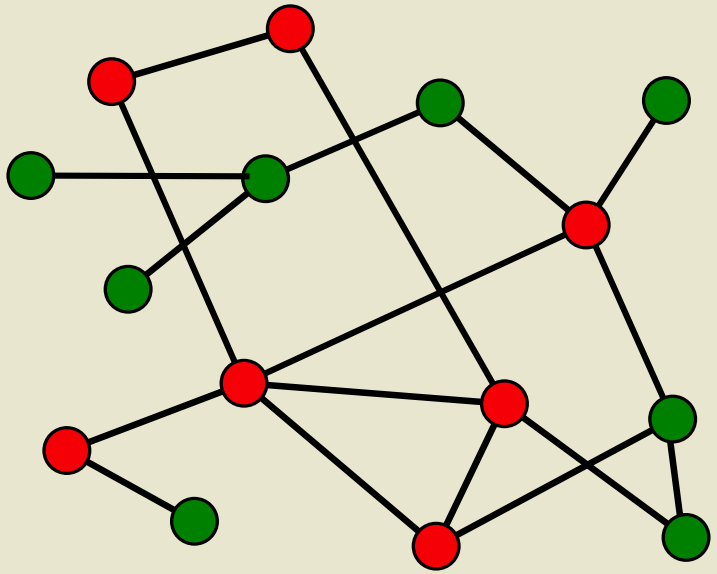
- Reconnaissance attacks try to find all the bots
  - Know how big the botnet is
  - Report bot addresses to Internet providers
- Abuse botnet's maintenance mechanism:
  1. Start with a few known bot addresses
  2. Ask these bots which other bots they know
  3. Repeat for newly found bots



Attacking P2P Botnets

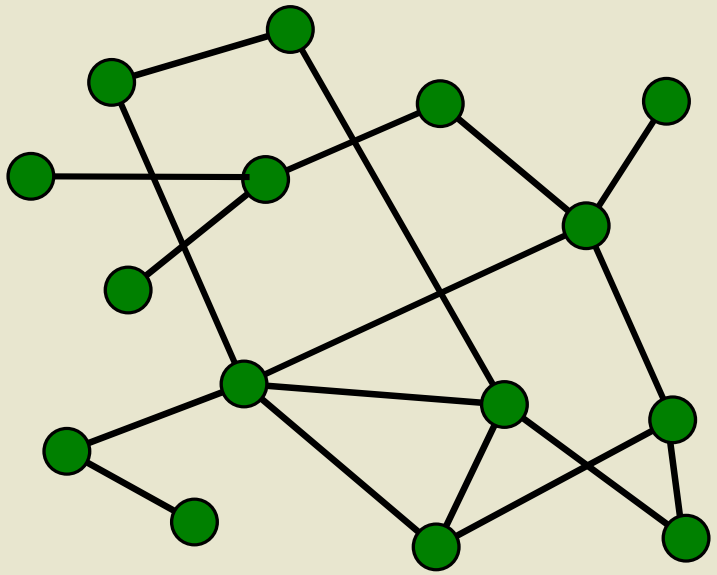
Reconnaissance

- 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



Sinkholing

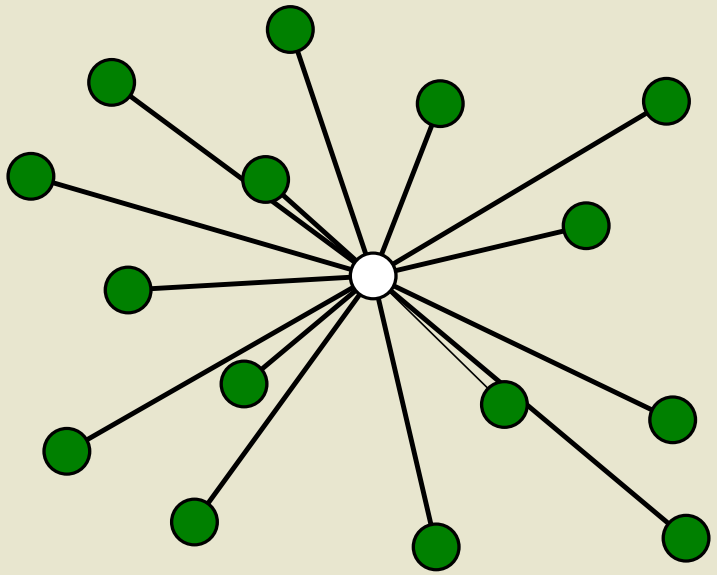
- Sinkholing attacks try to disconnect bots from each other
- Requires a way to modify bots' *peer lists*
- Try to redirect all bots to a benign *sinkhole* server



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

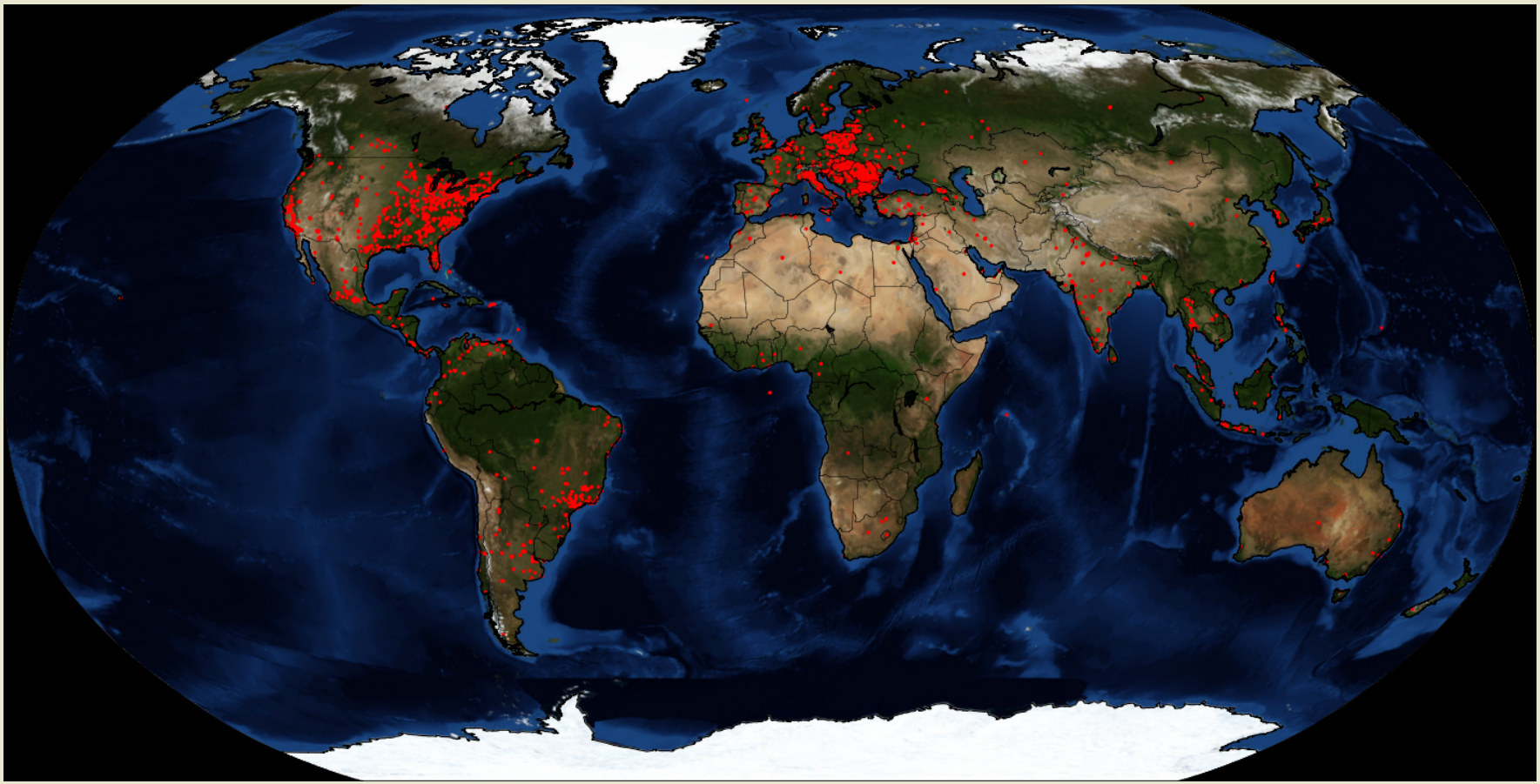
The Zeus Bot

- 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

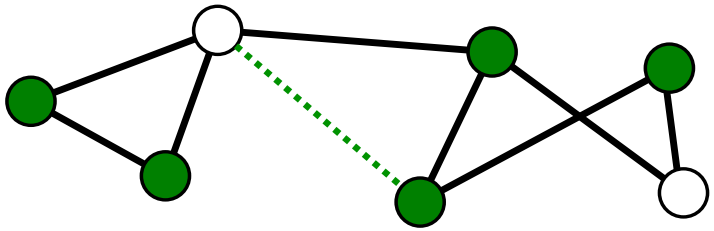
- Zeus evolved into a P2P variant around October 2011
- The P2P network currently contains 200.000 bots



Botnet Topology

P2P Layer

- Daily configuration updates
- Weekly binary updates



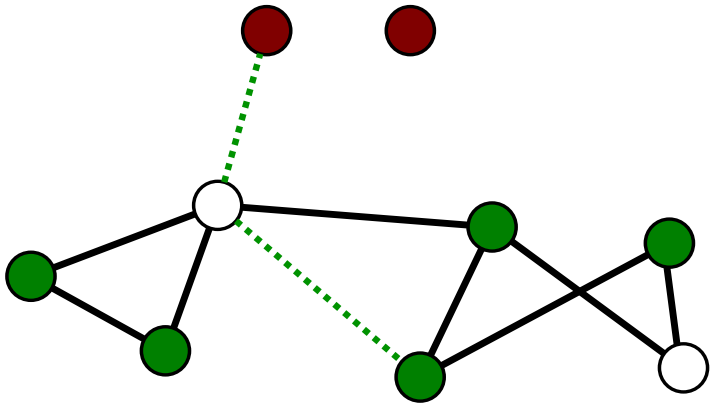
Botnet Topology

P2P Layer

- Daily configuration updates
- Weekly binary updates

Proxy Nodes

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



Botnet Topology

P2P Layer

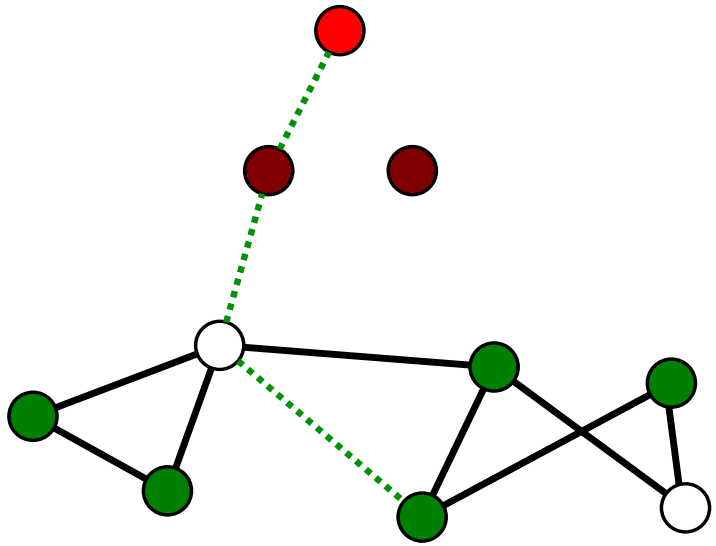
- Daily configuration updates
- Weekly binary updates

Proxy Nodes

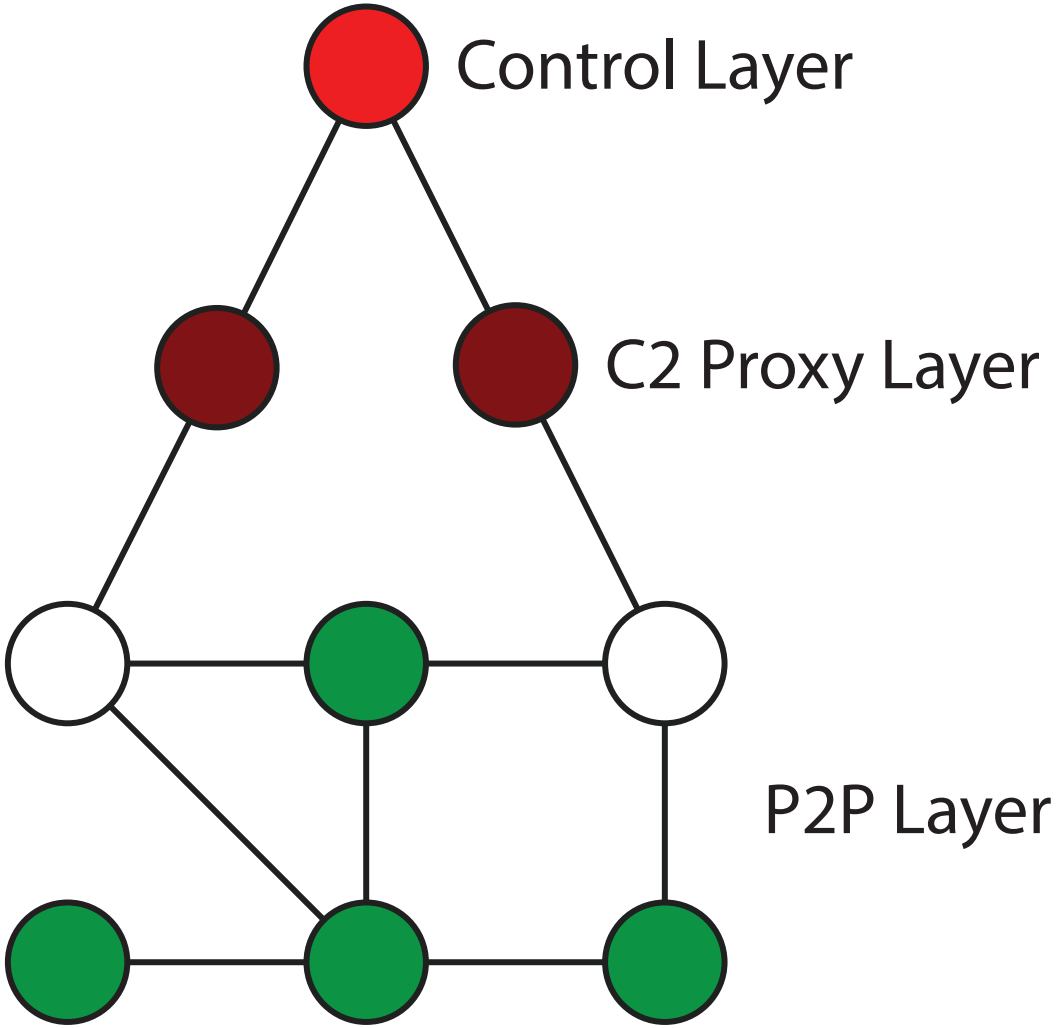
- Announced by special messages
- Route C2 communication
  - Stolen data
  - Commands

C2 Proxies

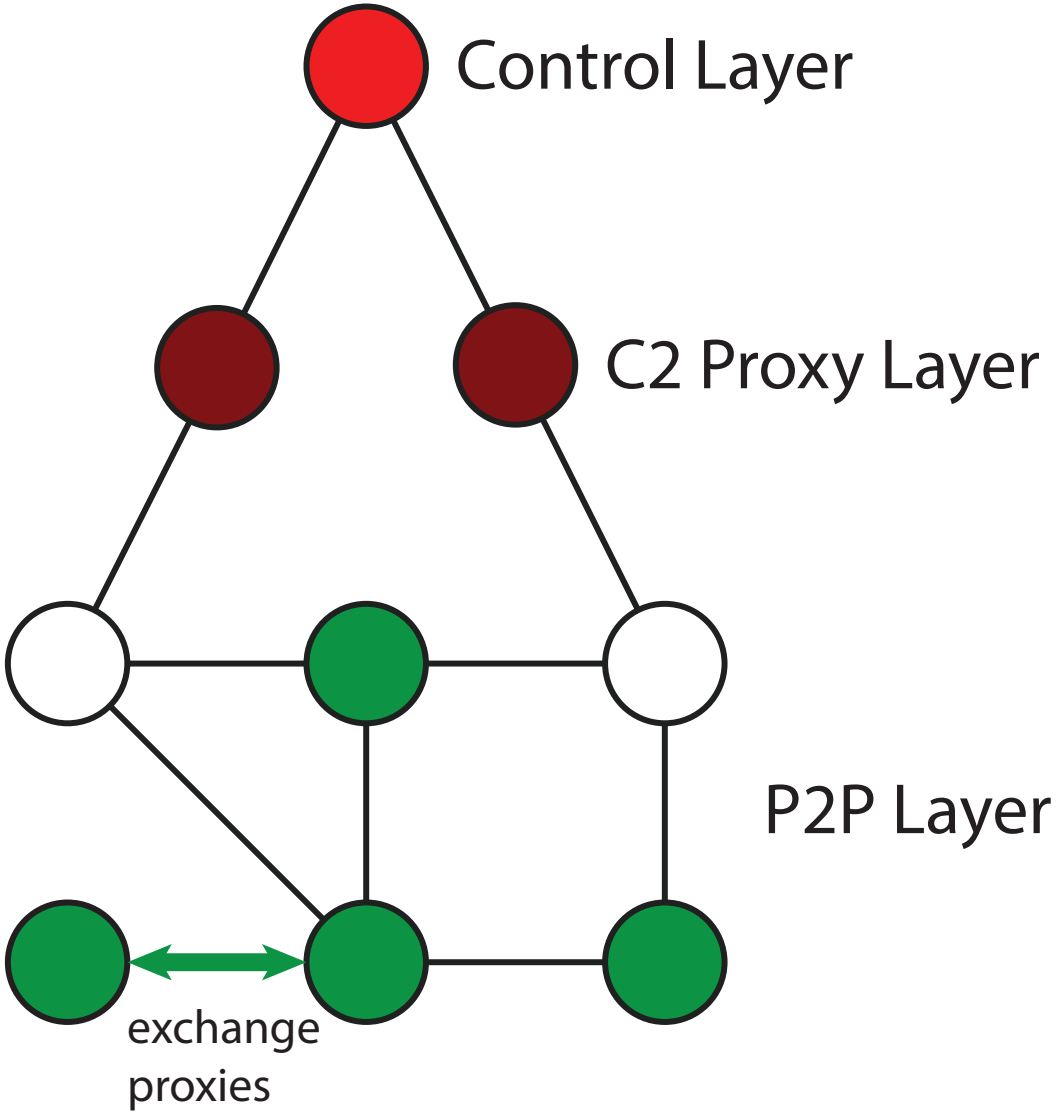
- Plain HTTP proxies
- Additional layer between botnet and backend



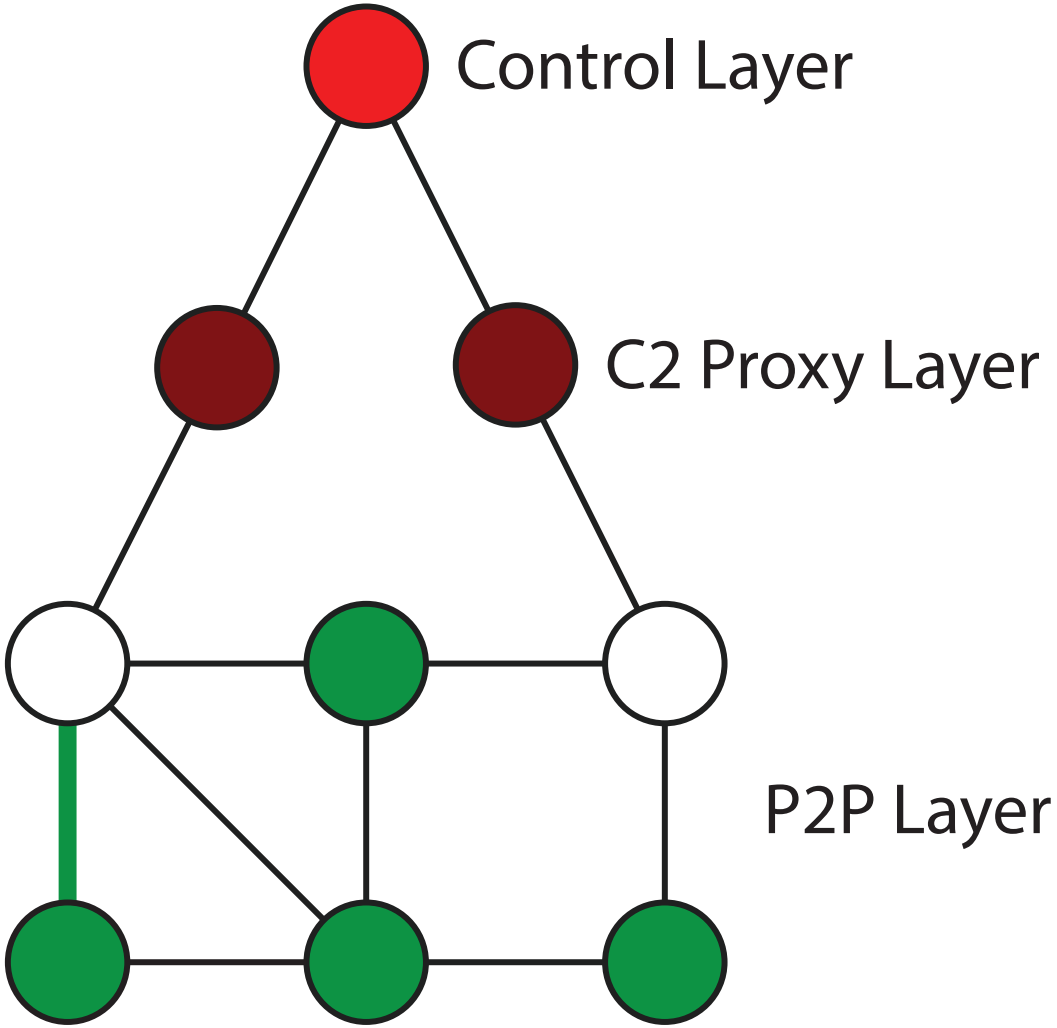
C2 Communication



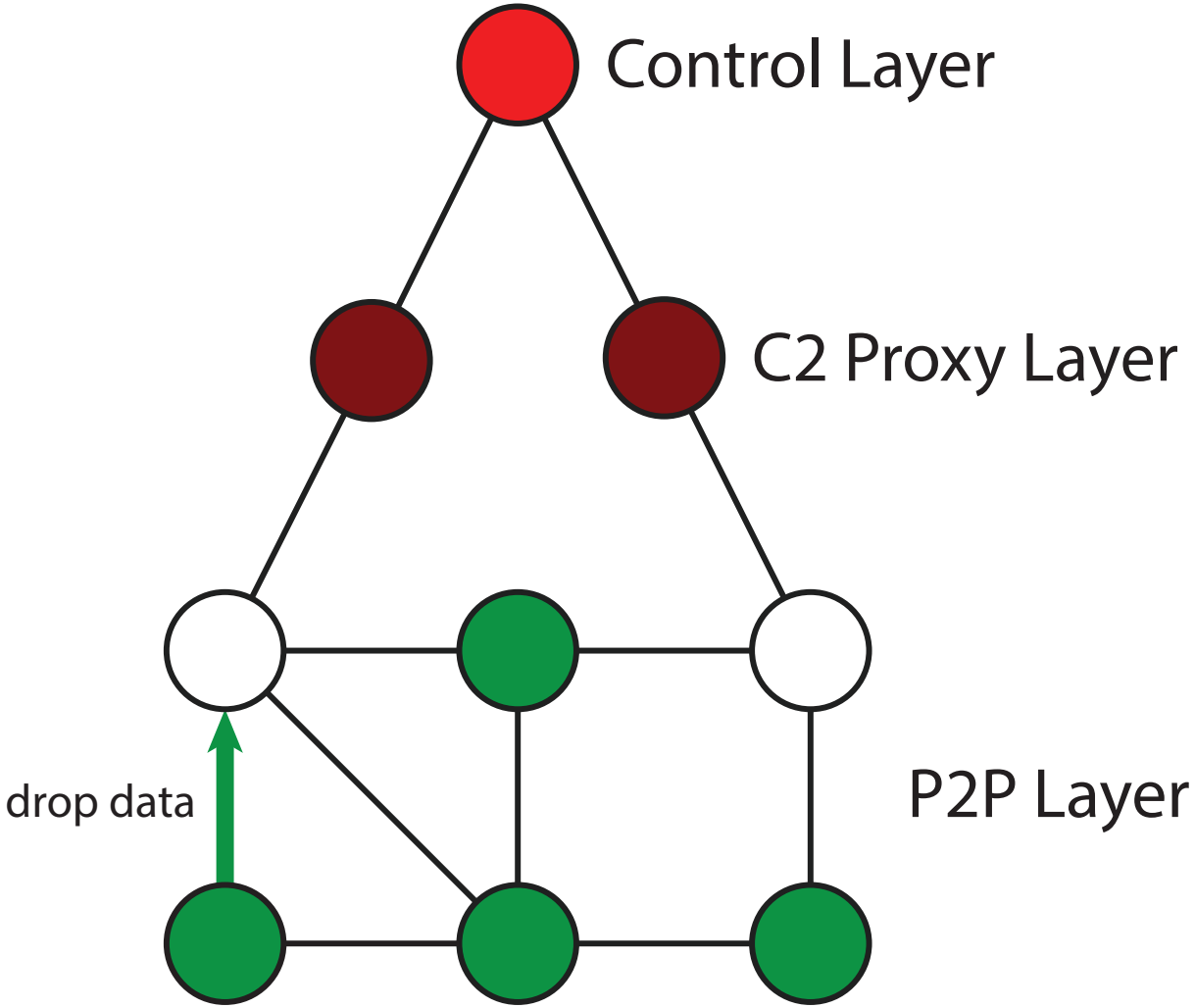
C2 Communication



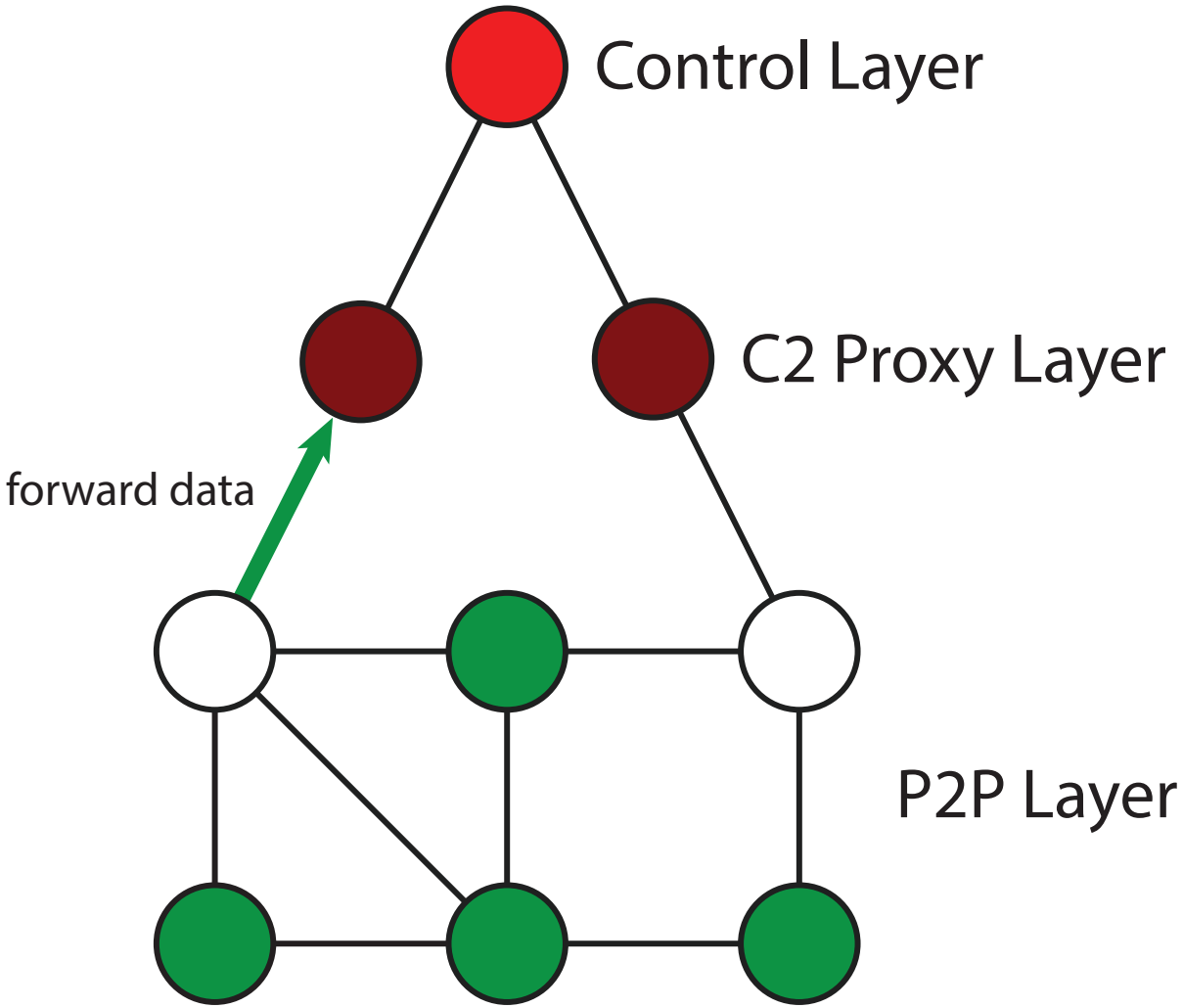
C2 Communication



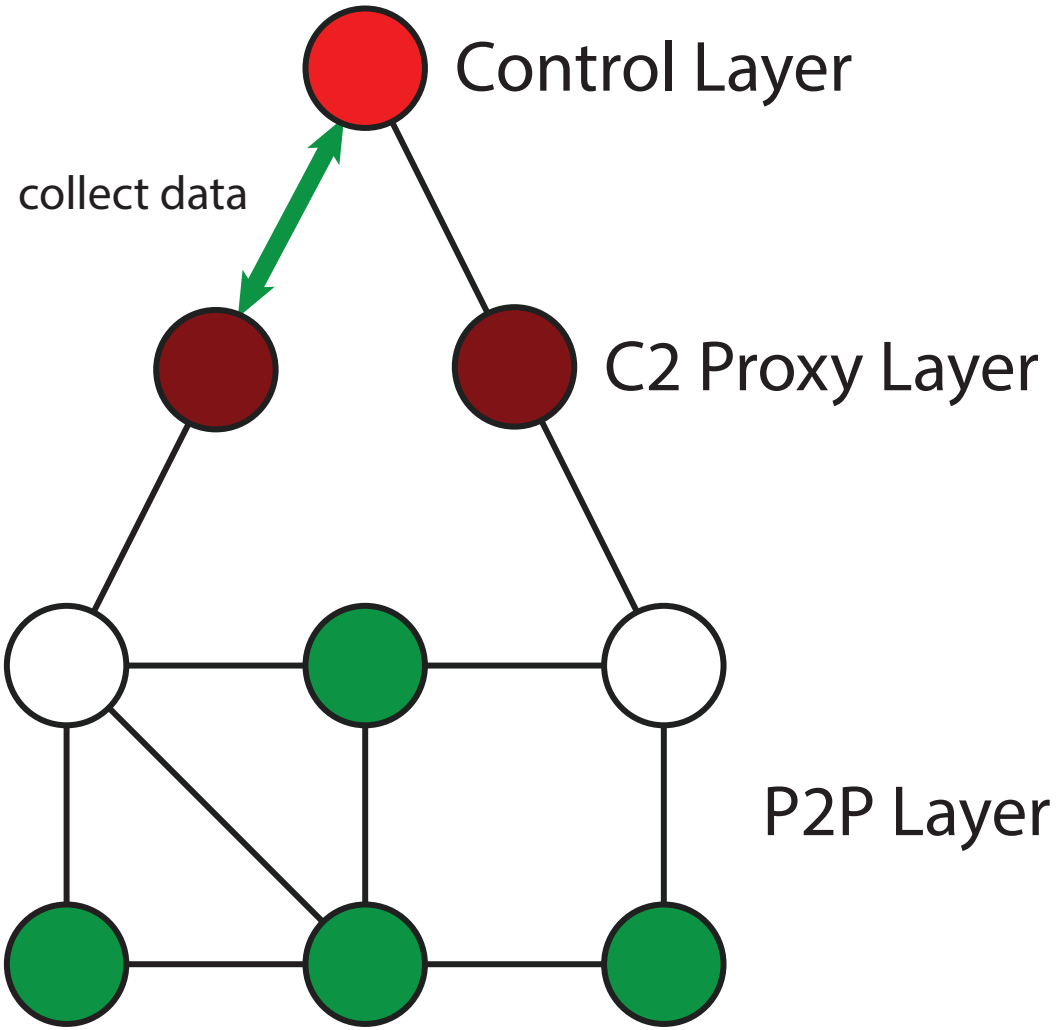
C2 Communication



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
...

Zeus Sinkholing War Stories

Weaknesses in the P2P Protocol

Peer list poisoning

- Possible to push a peer list update to a node
  - Bots store sender if $|peerlist| < 50$
  - If remote peer known but different IP address: Update entry
- Can "poison" a bot by claiming to be a known bot with new IP

Weaknesses in the P2P Protocol

Peer list poisoning

- Possible to push a peer list update to a node
  - Bots store sender if $|peerlist| < 50$
  - If remote peer known but different IP address: Update entry
- Can "poison" a bot by claiming to be a known bot with new IP

186.88.196.115
142.163.184.154
208.41.173.138
95.104.110.191

Peer List Request
ID: 4; IP: 192.168.0.1

Weaknesses in the P2P Protocol

Peer list poisoning

- Possible to push a peer list update to a node
  - Bots store sender if $|peerlist| < 50$
  - If remote peer known but different IP address: Update entry
- Can "poison" a bot by claiming to be a known bot with new IP

186.88.196.115
142.163.184.154
208.41.173.138
192.168.0.1

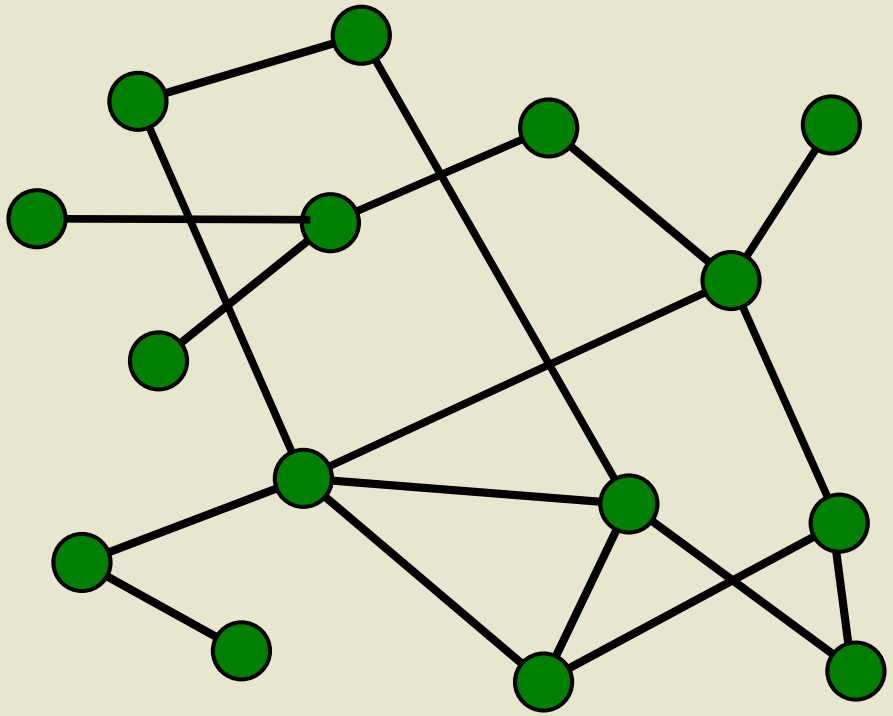
Peer List Response

First Sinkholing Attack

First Sinkholing Attack

Attack Plan

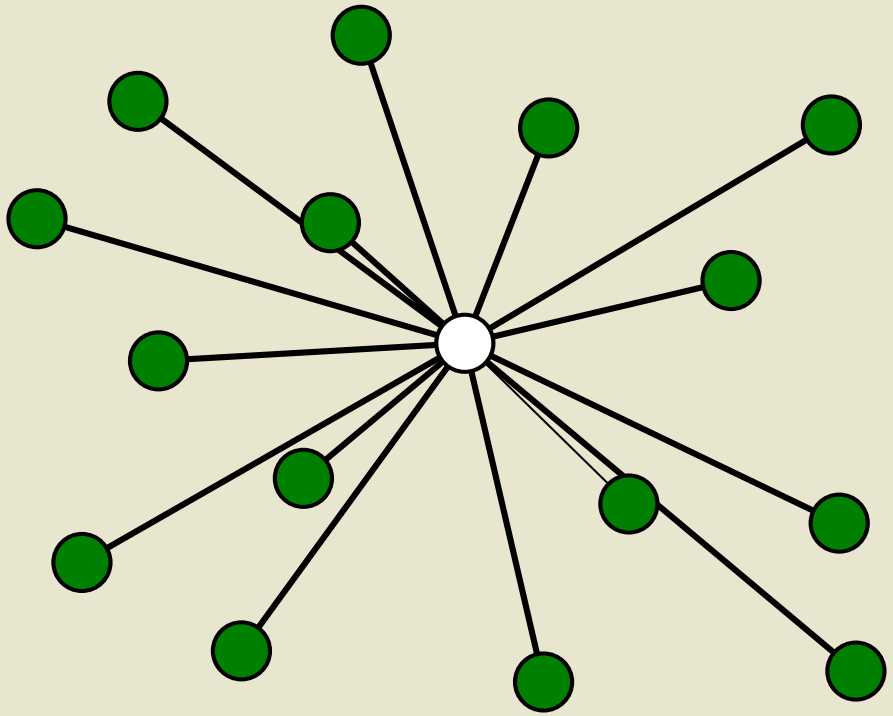
- Goal: Redirect bots to sinkholes, prevent normal operation
- Method: Replace peer list entries with our sinkholes
- Bonus: Log bots as they check in at the sinkholes, report them



First Sinkholing Attack

Attack Plan

- Goal: Redirect bots to sinkholes, prevent normal operation
- Method: Replace peer list entries with our sinkholes
- Bonus: Log bots as they check in at the sinkholes, report them



Poisoning Example

- Bot peer list before the attack:

Bot ID	IP address	Port
c2ad2c7621e8cc9057e8ee0fe678acdf216f8d0f	186.88.196.115	10355
c28df459e506e3fbaf0fe4e09c3e8a1fcc697f39	142.163.184.154	12631
3e6684b8016ad93410bc94803d1da9502239f582	208.41.173.138	13850
c19aff3ecf6a2e0443640baad118ee528ccd43ce	95.104.110.191	15550
3d0445ac21017cf284191485fc045e23a4d65dba	75.38.136.56	10169
5b68273785dc1a0e19d1461ccb5688e150528697	98.203.40.174	21918
e10fa5a555f3653837ceef2380da034dc7190261	174.134.88.28	19433
c1ff72dda4362153a43079ed35301537aaf56634	74.234.107.231	25975
93b2028482d876a9dd4a3b01b2265956f189aed4	190.206.20.161	29346
c3575bcd52b97c1484bee81dfa1bfcf5d3fd1343	79.113.161.10	16824

Poisoning Example

- Bot peer list *after* the attack:

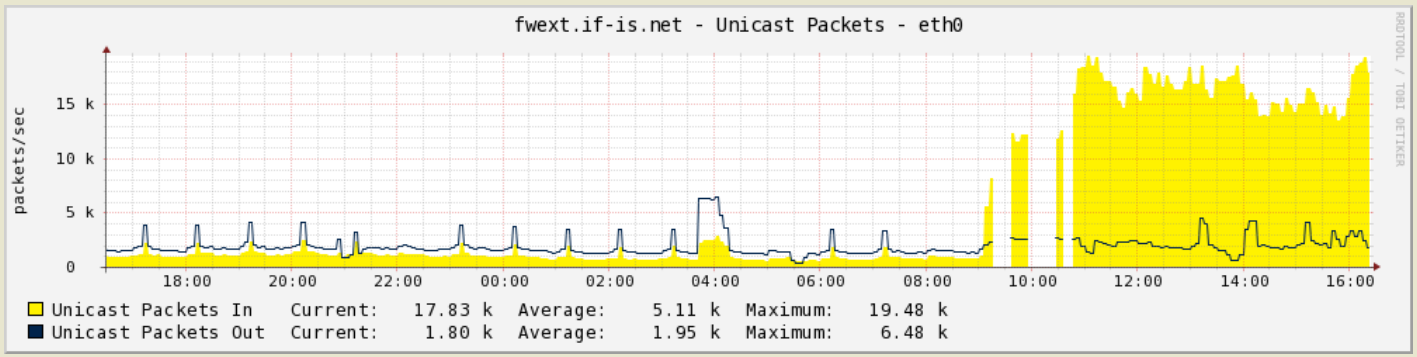
Bot ID	IP address	Port
c2ad2c7621e8cc9057e8ee0fe678acdf216f8d0f	192.168.1.1	13337
c28df459e506e3fbaf0fe4e09c3e8a1fcc697f39	192.168.1.2	13337
3e6684b8016ad93410bc94803d1da9502239f582	192.168.1.3	13337
c19aff3ecf6a2e0443640baad118ee528ccd43ce	192.168.1.4	13337
3d0445ac21017cf284191485fc045e23a4d65dba	192.168.1.5	13337
5b68273785dc1a0e19d1461ccb5688e150528697	192.168.1.6	13337
e10fa5a555f3653837ceef2380da034dc7190261	192.168.1.7	13337
c1ff72dda4362153a43079ed35301537aaf56634	192.168.1.8	13337
93b2028482d876a9dd4a3b01b2265956f189aed4	192.168.1.9	13337
c3575bcd52b97c1484bee81dfa1bfcf5d3fd1343	192.168.1.10	13337

Counteractions by the Botmasters

Attacks Against the Sinkholes

- On May 10th 2012, the botmasters launched a counterattack
  - DDoS attack against our sinkholes
  - Hardcoded blacklist filters several IP ranges
  - IP address /20 Filter

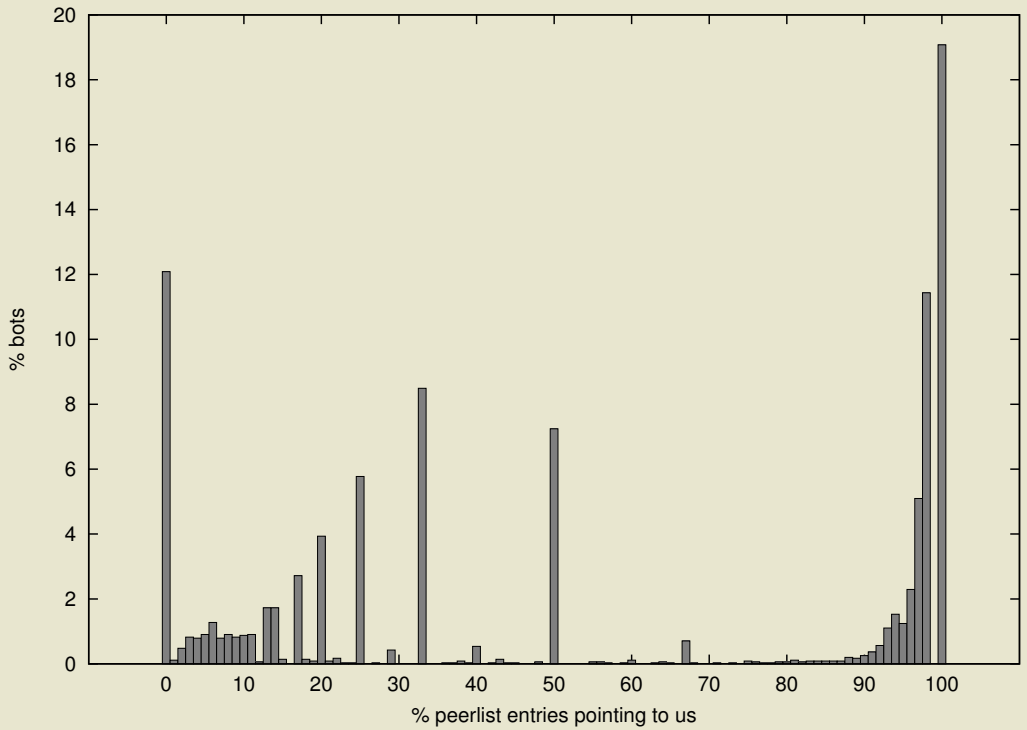
```
64.233.160.0/19    91.212.136.0/24    195.168.53.48/16
64.88.164.160/27   91.213.143.0/24     195.74.76.0/24
   65.52.0.0/14    128.130.0.0/15     207.46.130.0/16
  66.148.64.0/18    131.107.0.0/16     208.118.60.0/20
   84.74.14.0/24     150.26.0.0/24      212.5.80.0/26
 85.222.116.0/22   193.175.86.0/24     212.67.88.64/19
  91.103.64.0/22    193.71.68.0/24     91.199.104.0/24
  195.164.0.0/16
```



Effect of the First Attack

Assessment Results

- We lost some bots, but retained contact with ∼20%
  - Fully poisoned NATed nodes are unable to recover
  - They did not receive the May 10^{th} update
- Poisoned peers are still continuously contacting our sinkholes



Second Sinkholing Attack

Improving the Attack Strategy

Tweaks

- New strategy: Shrink peer lists
  - Gain access to the whole list
  - Less sinkhole IP addresses needed
  - Reduce load on the sinkholes
- Overwrite a few peer list entries with sinkhole addresses
- Invalidate the rest
  - Probe bot for peer list
  - Overwrite received entries, *only change ports*
  - Set some of the entries to sinkhole IPs
- Much more difficult for botmasters to notice

Improving the Attack Strategy

Tweaks

- Lots of technical improvements
- Details after presentation if there is time :-)

Poisoning Example

- Bot peer list before the attack:

Bot ID	IP address	Port
c2ad2c7621e8cc9057e8ee0fe678acdf216f8d0f	186.88.196.115	10355
c28df459e506e3fbaf0fe4e09c3e8a1fcc697f39	142.163.184.154	12631
3e6684b8016ad93410bc94803d1da9502239f582	208.41.173.138	13850
c19aff3ecf6a2e0443640baad118ee528ccd43ce	95.104.110.191	15550
3d0445ac21017cf284191485fc045e23a4d65dba	75.38.136.56	10169
5b68273785dc1a0e19d1461ccb5688e150528697	98.203.40.174	21918
e10fa5a555f3653837ceef2380da034dc7190261	174.134.88.28	19433
c1ff72dda4362153a43079ed35301537aaf56634	74.234.107.231	25975
93b2028482d876a9dd4a3b01b2265956f189aed4	190.206.20.161	29346
c3575bcd52b97c1484bee81dfa1bfcf5d3fd1343	79.113.161.10	16824

Poisoning Example

- Bot peer list *after* the attack:

Bot ID	IP address	Port
c2ad2c7621e8cc9057e8ee0fe678acdf216f8d0f	186.88.196.115	22945
c28df459e506e3fbaf0fe4e09c3e8a1fcc697f39	142.163.184.154	10361
3e6684b8016ad93410bc94803d1da9502239f582	192.168.1.1	14521
c19aff3ecf6a2e0443640baad118ee528ccd43ce	95.104.110.191	24540
3d0445ac21017cf284191485fc045e23a4d65dba	75.38.136.56	12954
5b68273785dc1a0e19d1461ccb5688e150528697	98.203.40.174	13953
e10fa5a555f3653837ceef2380da034dc7190261	10.0.0.1	25486
c1ff72dda4362153a43079ed35301537aaf56634	74.234.107.231	21953
93b2028482d876a9dd4a3b01b2265956f189aed4	190.206.20.161	17435
c3575bcd52b97c1484bee81dfa1bfcf5d3fd1343	79.113.161.10	12653

Poisoning Example

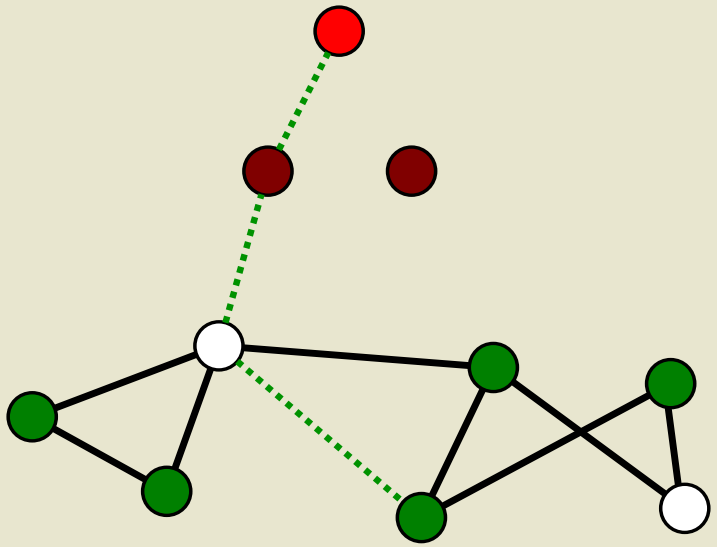
- Bot peer list after three validation rounds:

Bot ID	IP address	Port
3e6684b8016ad93410bc94803d1da9502239f582	192.168.1.1	14521
e10fa5a555f3653837ceef2380da034dc7190261	10.0.0.1	25486

Effect of the Second Sinkholing Attack

Assessment Results

- About 97% sinkholed
- DGA prevents a lasting effect
- C2 communication still possible
- Data dropping still possible



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