

# Neutralizing Peer-to-Peer Botnets Deliberately Destroying Drones

Dennis Andriesse

VU University Amsterdam

May 14, 2013

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?

## 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

- 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



## 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
- . . .

# Man in the Browser Attacks

## 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

<p>Overschrijven naar bankrekening</p> <p>Nieuwe overschrijving      Overschrijven naar bankrekening <input type="button" value=""/></p> <p>Betalen met IBAN en BIC in Nederland. <input type="checkbox"/></p> <p>Bedrag (euro) * <input type="text" value="100 . 00"/></p> <p>Van Betaalrekening <input type="text" value="XXXXXXXXXX"/></p> <p>Naar rekening * <input type="text" value="1234567 t.n.v. J. Doe"/> <input type="button" value="Selecteer adres"/> <input type="checkbox"/> Opslaan in adresboek</p> <p>Datum * <input type="text" value="05-02-2013 (dd-mm-yy)"/></p> <p>Periodieke overschrijving <input type="radio"/> eenmalig <input type="radio"/> t/m <input type="text" value=" (dd-mm-yy)"/> Einddatum niet verplicht</p> <p>Betalingskenmerk Acceptgiro <input type="text" value=" - - - -"/></p> <p>Mededelingen <input type="text" value=""/></p> <p>* Verplicht veld</p> <p>Er staan geen opdrachten klaar om te worden verzonden.</p> <p><input type="button" value="Opslaan, nieuwe opdracht"/> <input type="button" value="Opslaan, naar verzendlijst"/> <input type="button" value="Wissen"/></p>	<p>Overschrijven naar bankrekening</p> <p>Nieuwe overschrijving      Overschrijven naar bankrekening <input type="button" value=""/></p> <p>Betalen met IBAN en BIC in Nederland. <input type="checkbox"/></p> <p>Bedrag (euro) * <input type="text" value="10000 . 00"/></p> <p>Van Betaalrekening <input type="text" value="XXXXXXXXXX"/></p> <p>Naar rekening * <input type="text" value="9999999 t.n.v. Mallory"/> <input type="button" value="Selecteer adres"/> <input type="checkbox"/> Opslaan in adresboek</p> <p>Datum * <input type="text" value="05-02-2013 (dd-mm-yy)"/></p> <p>Periodieke overschrijving <input type="radio"/> eenmalig <input type="radio"/> t/m <input type="text" value=" (dd-mm-yy)"/> Einddatum niet verplicht</p> <p>Betalingskenmerk Acceptgiro <input type="text" value=" - - - -"/></p> <p>Mededelingen <input type="text" value=""/></p> <p>* Verplicht veld</p> <p>Er staan geen opdrachten klaar om te worden verzonden.</p> <p><input type="button" value="Opslaan, nieuwe opdracht"/> <input type="button" value="Opslaan, naar verzendlijst"/> <input type="button" value="Wissen"/></p>
--	---

As seen by victim

As sent to bank

## 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

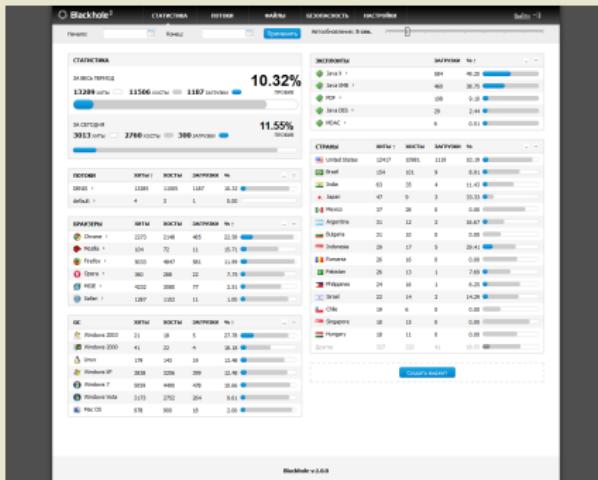
## Credential theft example: Call center employee

- 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

The screenshot shows the official website of the Miami Dolphins. At the top, there's a navigation bar with links for TICKETS, NEWS, TEAM, MEDIA, CHEERLEADERS, FAN ZONE, COMMUNITY, ESPAÑOL, FANTASY, and PRO SHOP. There are also social media icons for Facebook, Twitter, and YouTube, along with LOGIN | JOIN and NFL INTERNET NETWORK. A search bar is located at the top right.

The main header features the Miami Dolphins logo and the text "THE OFFICIAL WEBSITE OF THE MIAMI DOLPHINS". Below the header, a banner reads "UP NEXT: Finesters Final Drive 2/9/13 9AM - 10:30AM EST".

The central focus is the "TICKET CENTER" section, which includes buttons for "2013 SEASON TICKETS", "RENEW FOR 2013", "SINGLE GAME TICKETS", and "WIN 2013 SEASON TICKETS!". A phone number "1.888.FINS.TIX" is also displayed.

A large image of a Miami Dolphins player in action is prominently featured in the center of the page. Below this image, a headline reads "// Local Product Enjoys Rookie Year".

On the left side, there's a "FEATURED STORIES" section with several thumbnail images and titles. On the right side, there's a "Latest Headlines" section with a list of news items, each preceded by a small red triangle icon. At the bottom, there are sections for "Podcasts", "Top Videos", and "Top Photos", each with a grid of thumbnails.

# Drive-by Download Examples

NU.nl

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

The screenshot shows the NU.nl homepage from Tuesday, February 5, 2013. The page features a navigation bar at the top with links for Muziek, Sport, Hörgeld, Wijzig, Mijlpalen, Nieuws, and Meer. Below the navigation is the NU logo and a search bar. The main content area is divided into several sections:

- Voorpagina:** Headlines include "Ruimte voor demonstraties rond inhuldiging koning" (Space for demonstrations around the king's inauguration) and "Vervanger op Drents dieel A28 gevonden om boswachter te beschermen" (Replacement found on Drenthe section of A28 to protect forest ranger).
- Beurs:** Headline: "Meedor krijgt 15 jaar cel voor doden zoontjes Terwolde" (Meedor gets 15 years in prison for killing his son's children).
- Achterklep:** Headline: "Minister Oostendorp benadrukt dat gemeente niet snel zal kiezen voor verbod" (Minister Oostendorp emphasizes that the municipality will not quickly choose to ban).
- Opmereklap:** Headline: "Vuurwerk op Drents dieel A28 gevonden om boswachter te beschermen" (Explosives found on Drenthe section of A28 to protect forest ranger).
- Cultuur en Media:** Headline: "Goeden koekje gevonden op beeld in Hannover" (Good cookie found on a statue in Hannover).
- Wetenschap:** Headline: "Pantji Berlusconi op wint in pilingen Italie" (Pantji Berlusconi wins in Italian piles).
- Gezondheid:** Headline: "China richtte wapen op Japans schip" (China pointed its weapons at Japan's ship).
- Lifestyle:** Headline: "Grote politie inzet voor verzonnen overval" (Large police operation for a fabricated robbery).
- Auto:** Headline: "CDK en PvdA willen debat over matching" (CDK and PvdA want a debate about matching).
- Weer:** Headline: "Nederland plekt voor verdere politieke integratie Europa" (Netherlands selected for further political integration of Europe).
- Verkeer:** Headline: "Verkeer moet stoppen met hooizaden" (Traffic must stop with hay bales).
- NU-nieuws:** Headline: "Tiltberg moet stoppen met hooizaden" (Tiltberg must stop with hay bales).
- NU-blog:** Headline: "Zakenman voor verontschuldiging aan Europees parlementair" (Businessman for apology to European parliamentarian).
- NU-data:** Headline: "Zekkenberg: 'Wijgen geen gedrevenheid voor paardenkeringen'" (Zekkenberg: "We do not have a driving force for horse enclosures").
- NU-ni-apps:** Headline: "Funda experimenteert met woningprijs" (Funda experiments with housing price).
- Colofon:** Headline: "PVV stamt parlementaire enquête SNS" (PVV originates from parliamentary inquiry SNS).
- Economie:** Headline: "Recordaantal schepen naar zandstranden Azíz" (Record number of ships to sand beaches Azíz).
- Sport:** Headline: "Staking bij chemiebedrijf Sabic voorbij" (Strike at SABIC chemical company has ended).
- Mariano komende zomer weer in actie:** Headline: "Verondiepte atleet staat indoorseizoen over".
- Zware crash Venn tijdens WK skien:** Headline: "Sjiling naar tweede ronde ATP-toernooi Zagreb" (Sjiling to the second round of the ATP tournament in Zagreb).
- Fuentes laks bij transporteren bloedzuiken:** Headline: "Agen moet zelf hoofde van 'voedselkosten'" (Agent must be the head of 'food costs').

On the right side of the page, there are several sidebar boxes:

- Volg NU.nl:** Links to Facebook, Twitter, and a weather forecast (3°C, 1 km, 1.401, 349.38, 0.09%).
- Wetenschap:** Headline: "Drooszuiker met 'opvoedwagen' opgereden" (Dried sugar with 'parenting car' driven over).
- NU in beeld:** Shows a photo of a person with a banner that says "VERWIJST HANNOVER".
- Bekijk fotoserie (100):** Link to a photo series.
- Meest gelezen:**
  1. Agent moet zelf hoofde van 'voedselkosten'
  2. Goeden koekje gevonden op beeld in Hannover
  3. Baumpinter ging sneller dan gedacht
  4. UEFA waarschuwt Manchester City en Paris Saint-Germain

# Drive-by Download Examples

## Weeronline.nl

- Even checking the weather report could get you infected

weeronline.nl  
alg je weer

Het is vandaag half bewolkt met kans op een lichte bui in Hilversum (Wijg pleats)

Waarschijnlijk gladheid

Wetterverwachting voor Hilversum

vandaag 8 morgen 9

Uitgebreide weerverwachting voor Hilversum

Buienverwachting in Hilversum

10:00 10:30 11:00

Bekijk radar Hilversum

11:10u

Activiteiten Hilversum

Sport & recreatie

- FietSEN
- Golf
- Schaatsen
- Tennis
- Voetbal
- Wandelen

Gezondheid

- Hokkies
- Zonracht
- Grip

Meer opties en vergroten

Met weer vandaag in...

Nederland	Amsterdam	Rotterdam	Den Haag	Utrecht	Eindhoven	Maastricht	Tilburg	Groningen	Nijmegen	Haarlem
Regelmatig	6°C ☁	6°C ☁	6°C ☁	6°C ☁	6°C ☁	6°C ☁	6°C ☁	6°C ☁	6°C ☁	6°C ☁
trekken vandaag winterse buien over het land. Tussen de buien door is ruims voor de zon en de maxima komen op 10°C. De wind is vanaf de noordwesten houdt de beschijf aan, vanavond wordt de droge. Morgen is het een stuk droger dan vandaag en heeft ook de zon meer speeltijd.	7 februari 2013									

Wetterbericht voor Nederland

Winterse buien

Zondag, 7 februari 2013 - Regelmatig trekken vandaag winterse buien over het land. Tussen de buien door is ruims voor de zon en de maxima komen op 10°C. De wind is vanaf de noordwesten houdt de beschijf aan, vanavond wordt de droge. Morgen is het een stuk droger dan vandaag en heeft ook de zon meer speeltijd.

Uitgebreide weerverwachting

Weerberichten

01 feb. Koude maar droge canaal op komst

02 feb. Oostwest door winterse nevelen

## 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

The screenshot shows the GoldInstall website interface. At the top, there's a banner featuring a woman in a bikini standing next to a white sports car. Below the banner is a navigation bar with links: Main, Sign up, Login, Rates, Contacts, Terms of service, and FAQ. A sub-header below the navigation bar reads "Goldinstall Rates for 1K Installs for each Country." Below this, there's a table listing rates for various countries:

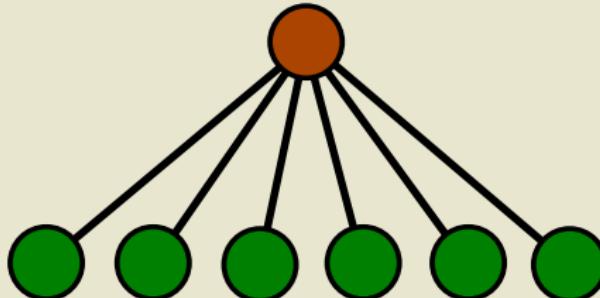
Country	Price
OTH	13\$
US	150\$
GB	110\$
CA	110\$
DE	30\$
BE	20\$
IT	65\$
CH	20\$
CZ	20\$

The screenshot shows the Gangsta Bucks website. The header features the "Gangsta Bucks" logo with a small American flag icon. Below the header is a main menu with links: Home, Conditions, Registrations, Tariffs, and Contacts. The background of the page has a stylized illustration of gangsters in suits and hats, along with playing cards and a city skyline silhouette. At the bottom, there's a row of smaller, semi-transparent gangster figures.

# Evolution of Botnets

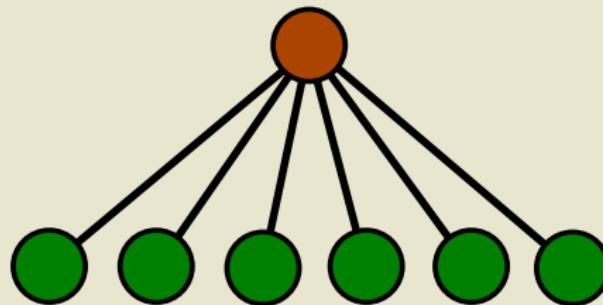
## Centralized botnets

- 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”



## Centralized botnets

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



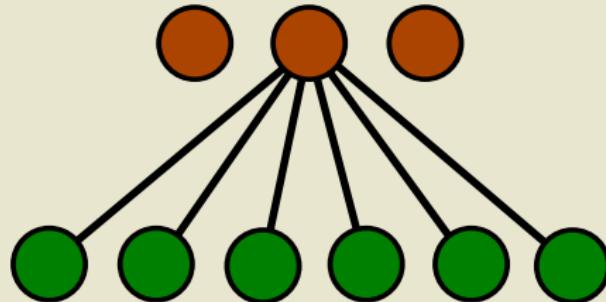
## Centralized botnets

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



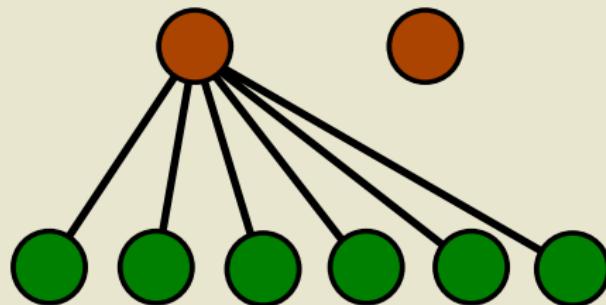
## Redundant infrastructure

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



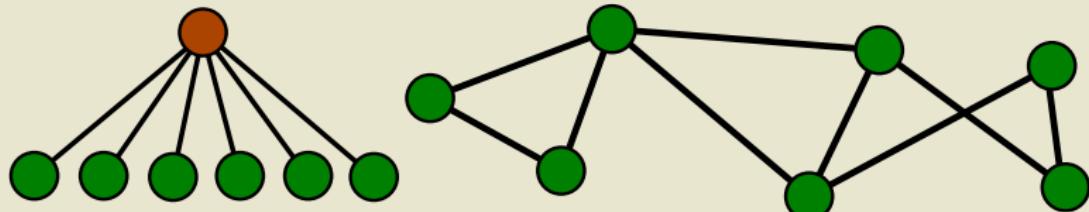
## Redundant infrastructure

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



## 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



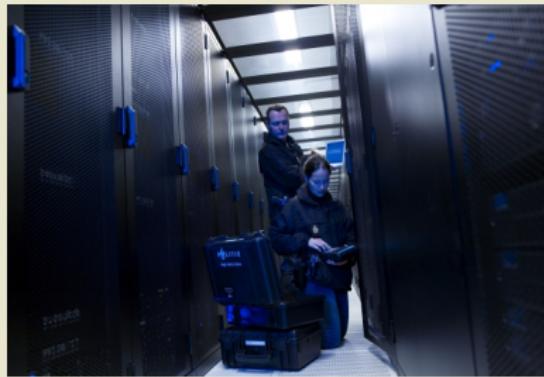
## Current P2P botnets

- 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

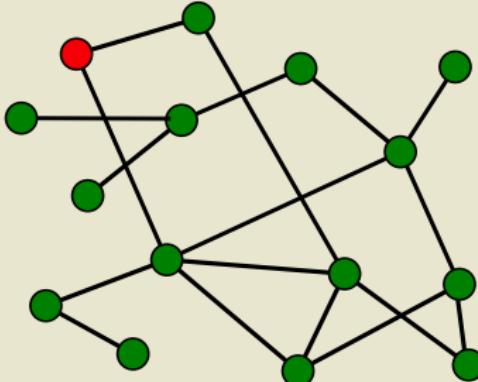
## Commanding bots to uninstall

- 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



## Reconnaissance

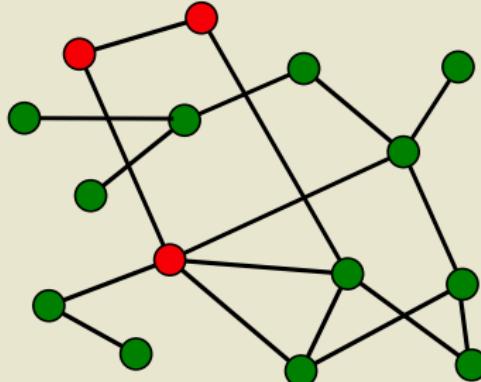
- Reconnaissance attacks try to find all the bots
  - Know how big the botnet is
  - Report bot addresses to Internet providers
- Abuse botnet's maintenance mechanism:
  - ① Start with a few known bot addresses
  - ② Ask these bots which other bots they know
  - ③ Repeat for newly found bots



## Attacking P2P Botnets

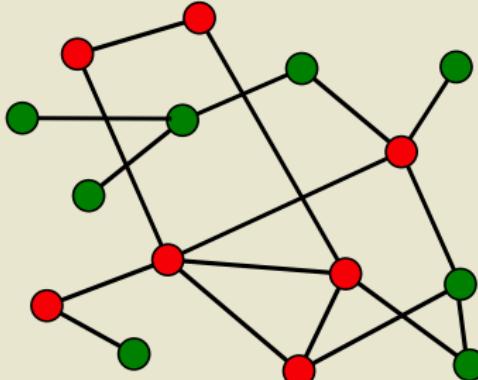
## Reconnaissance

- 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



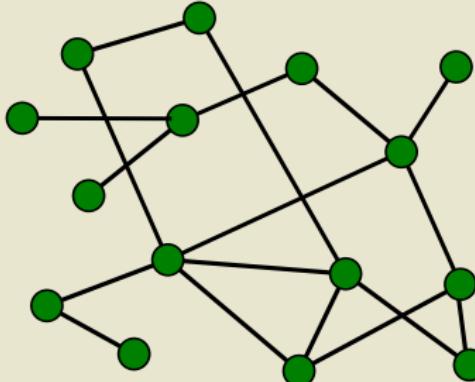
## Reconnaissance

- 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



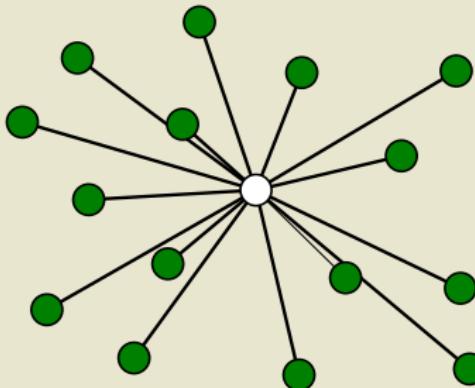
## Sinkholing

- 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



## 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

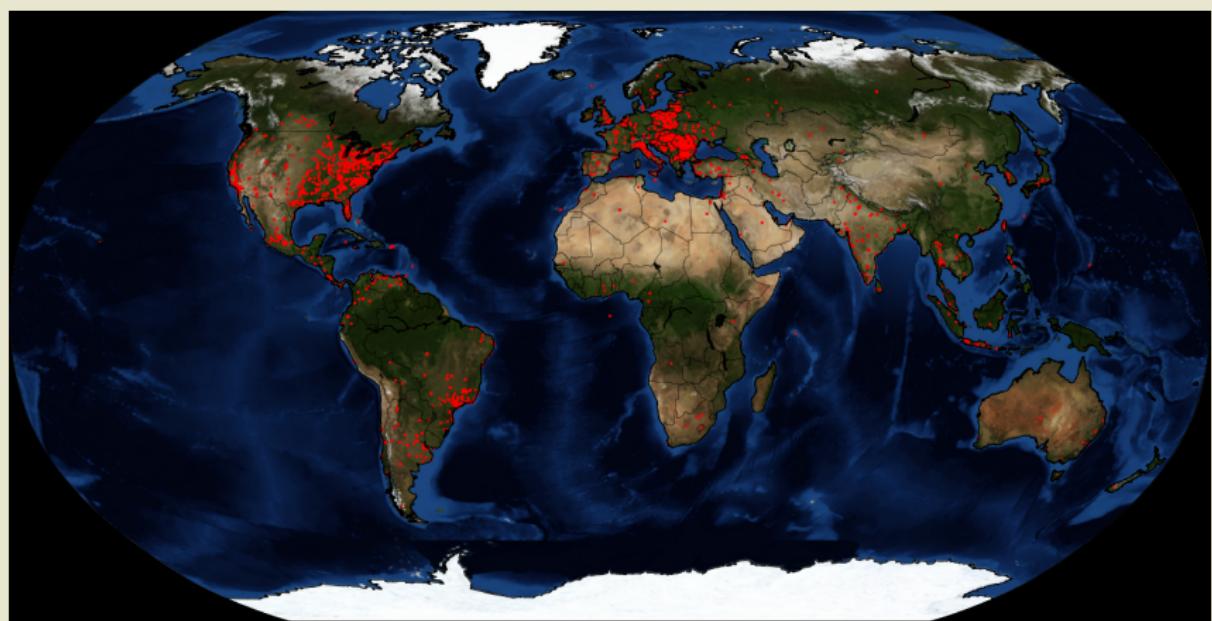
## The Zeus Bot

- 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



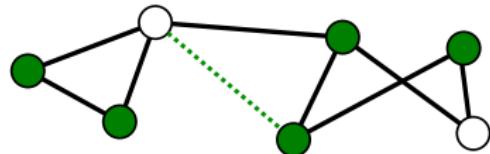
## P2P Zeus/Gameover

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



## P2P Layer

- Daily configuration updates
- Weekly binary updates



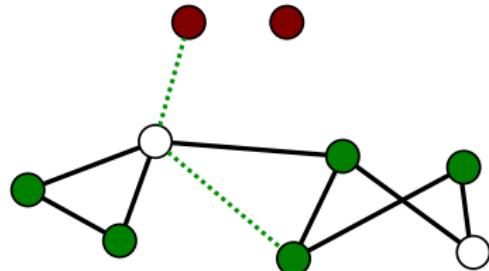
# Botnet Topology

## P2P Layer

- Daily configuration updates
- Weekly binary updates

## Proxy Nodes

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



# Botnet Topology

## P2P Layer

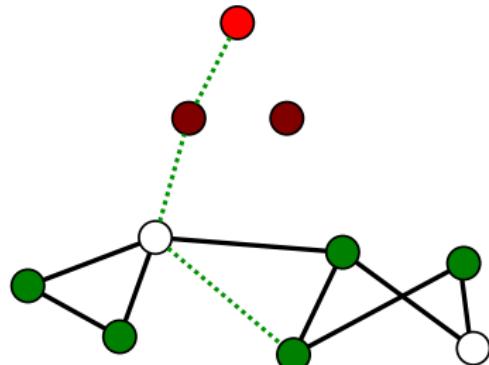
- Daily configuration updates
- Weekly binary updates

## Proxy Nodes

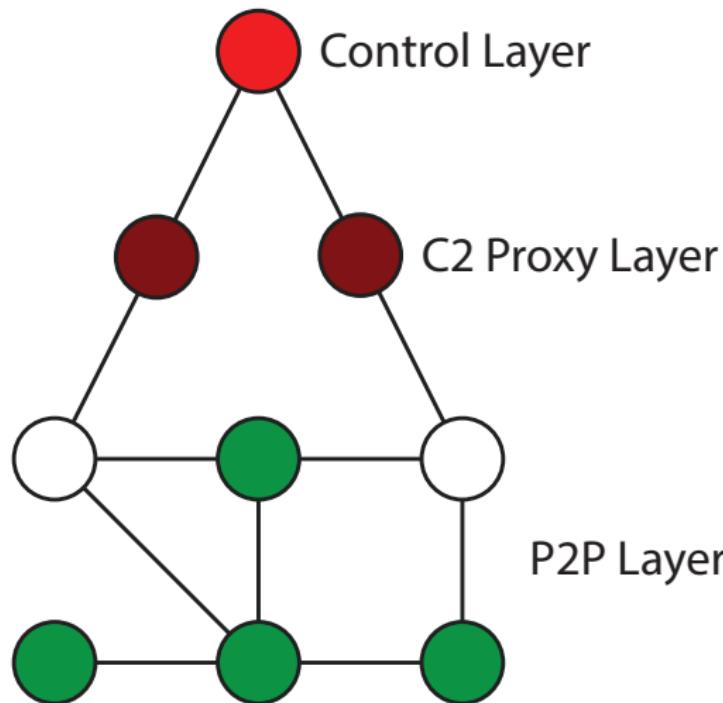
- Announced by special messages
- Route C2 communication
  - Stolen data
  - Commands

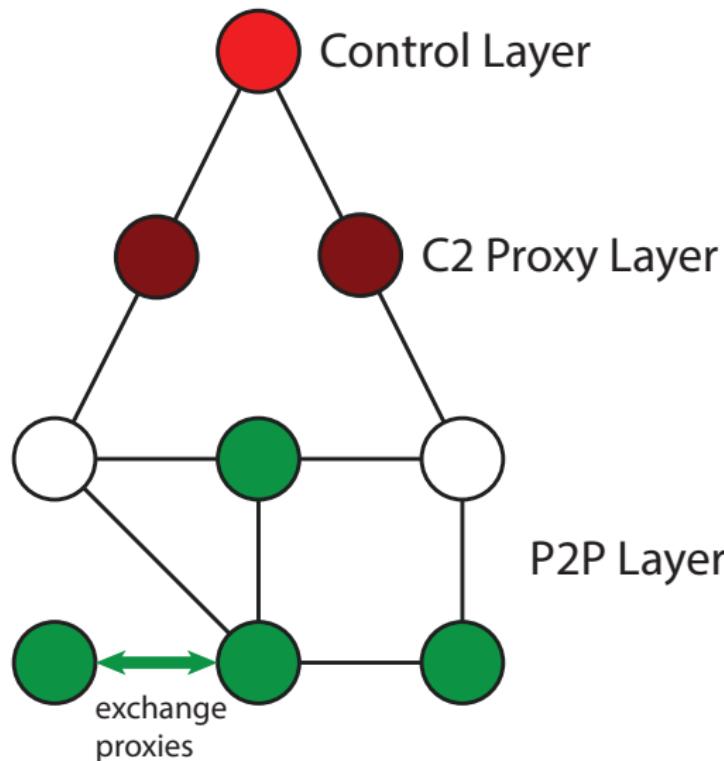
## C2 Proxies

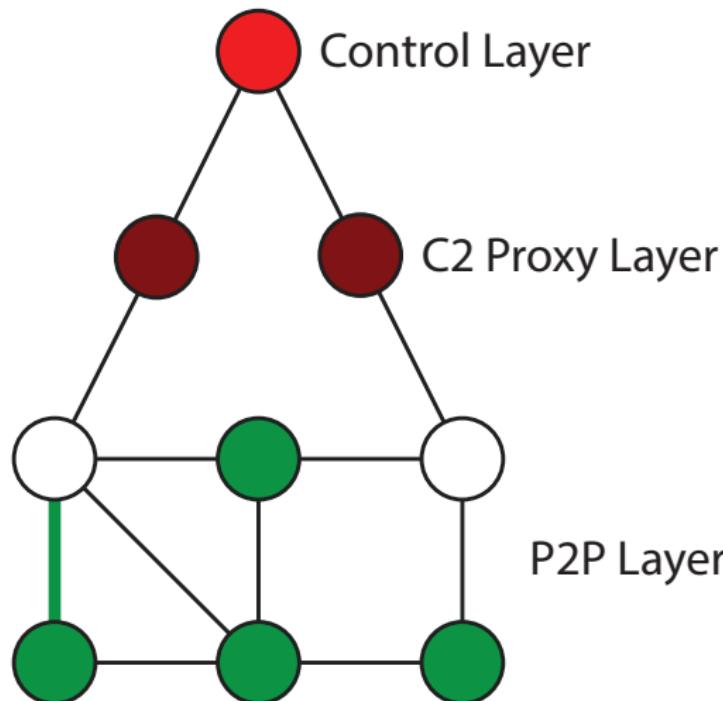
- Plain HTTP proxies
- Additional layer between botnet and backend



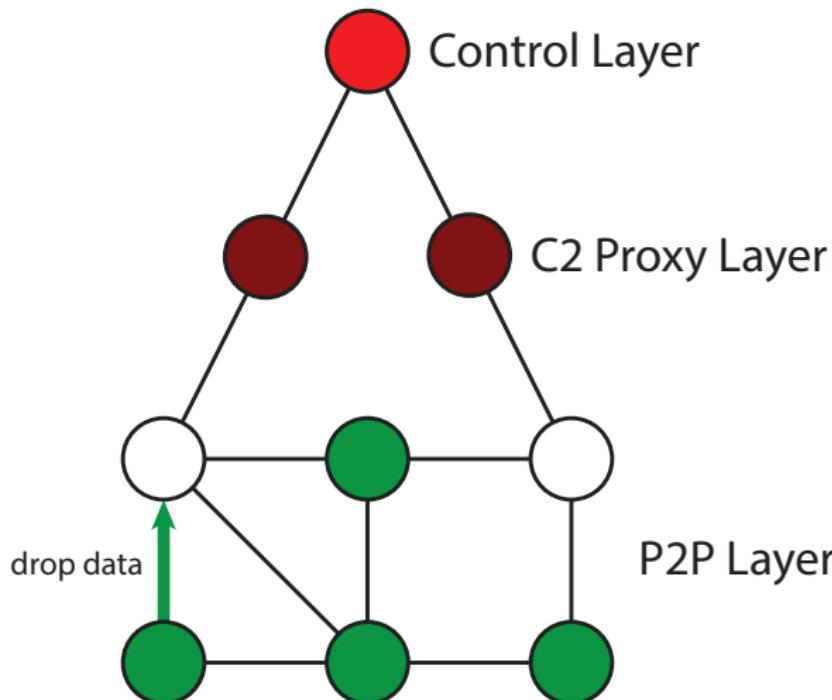
# C2 Communication



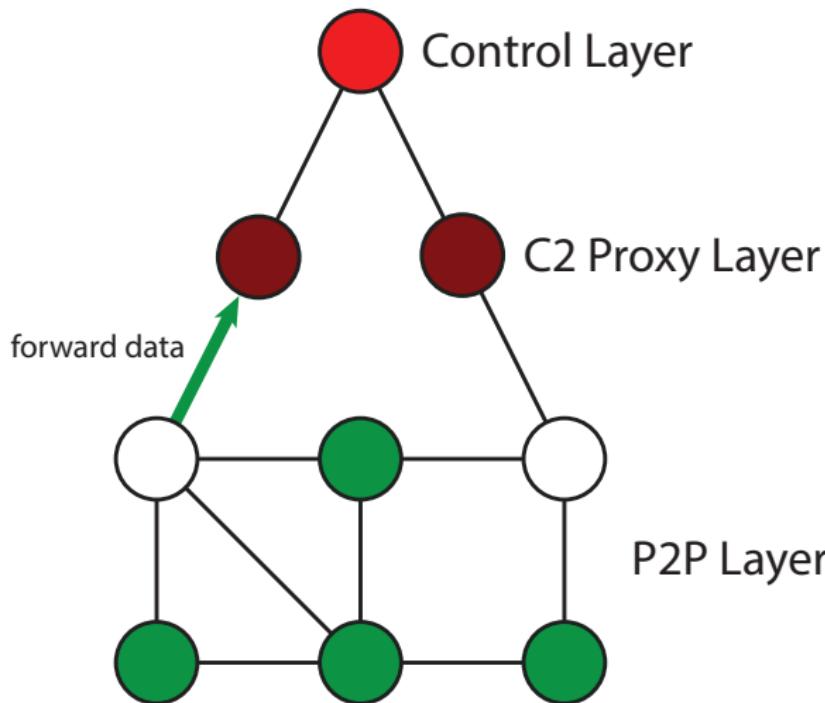




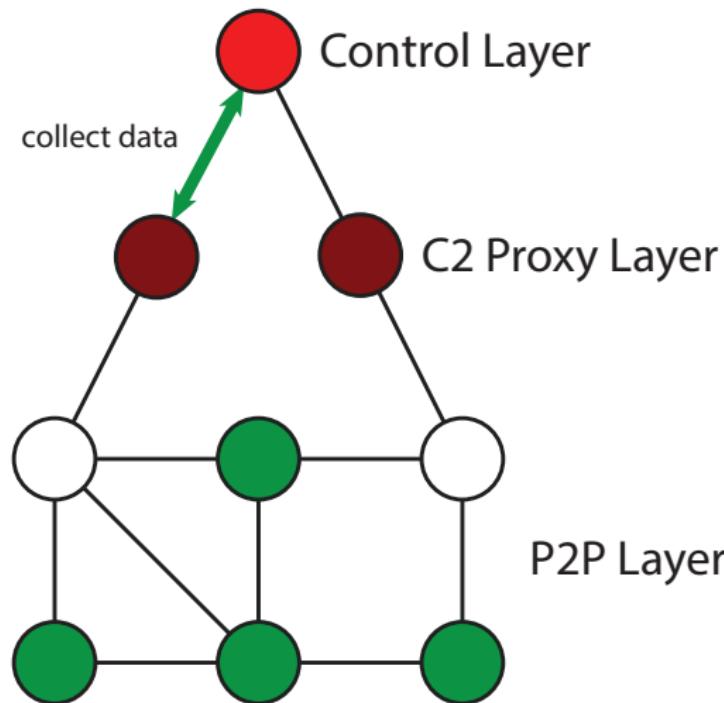
## C2 Communication



## C2 Communication



# C2 Communication



## 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  
xthzltayhiusmbdbllrgukvts.com  
fqgyssobrgtopmftxslbqeql.net  
nvqmjszfzdcmxsmdsgofeil.org  
...

## 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