



Botnet Communications and Protocols

EECS4482

Presented by: Edwin Gonzalez Dos Santos, Jacky Hoang,

Victor Vavan

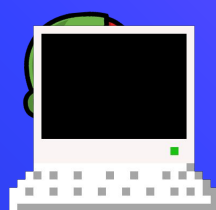
Outline

- ⬡ What's a botnet?
- ⬡ Botnet: Past and Present
- ⬡ Botnet Architecture
- ⬡ Botnet Protocols



What's a botnet?





Botnet: Past

- ⬡ Khan C. Smith
- ⬡ Phishing and spam botnet
- ⬡ 12% of all Earthlink's Email traffic
- ⬡ Estimated to have made around \$3 Million...
- ⬡ ... but sued for \$25 Million



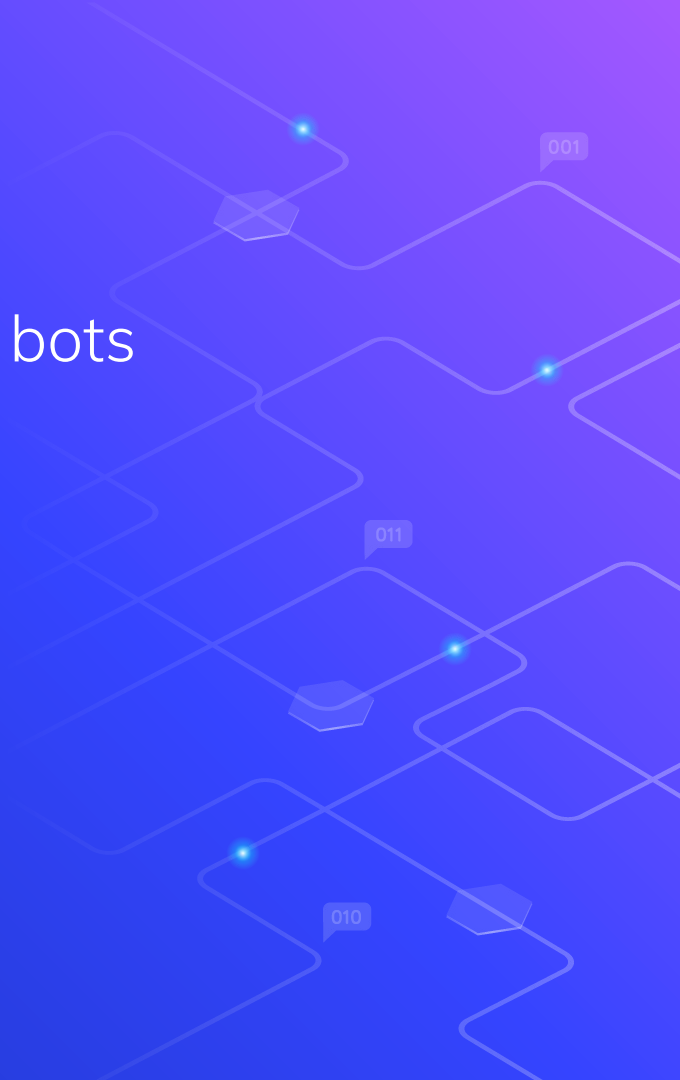
Botnet: Present

- Phorphiex / Trik botnet
 - Phorpiex trojan
 - 450,000 infected Windows computers
 - Sextortion and spam
 - \$115K in 5 months



Other Notable Botnets:

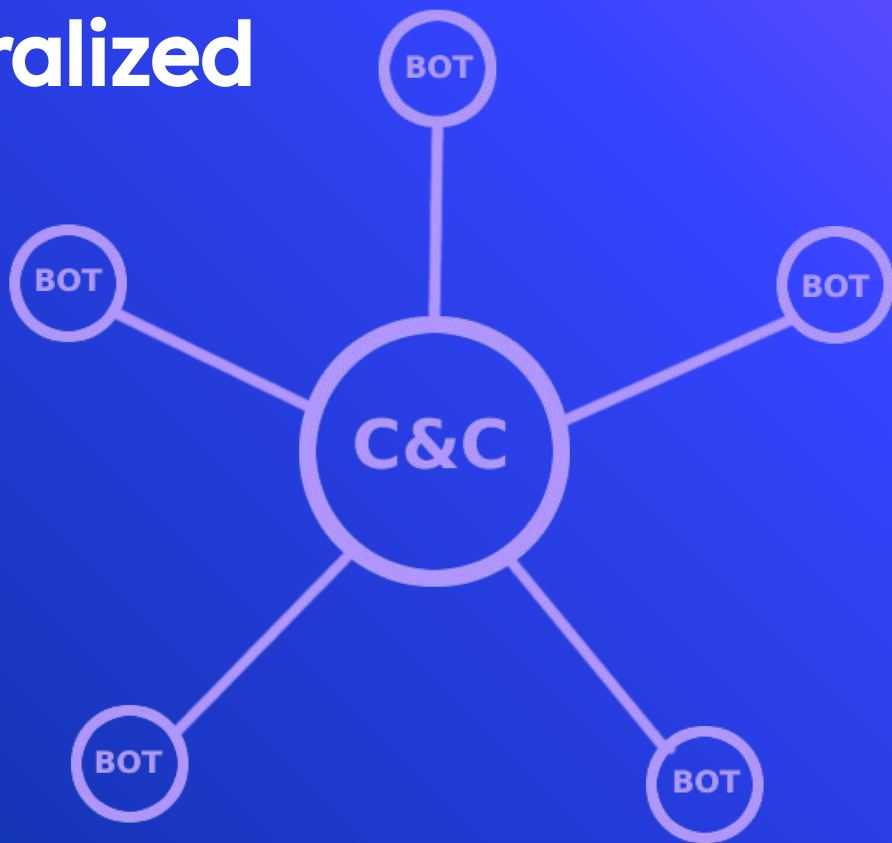
- ⬡ Storm (2007): 250,000 - 1,000,000 bots
- ⬡ Kraken (2008): 500,000 bots
- ⬡ Mirai (2016): 600,000 bots



Botnet Architecture



Centralized



Centralized

Advantages:

- **simple**
 - low latency
 - high scalability
 - easy implementation



Disadvantages:

- **low robustness**
 - single point (or a few points) of failure
 - easily detectable



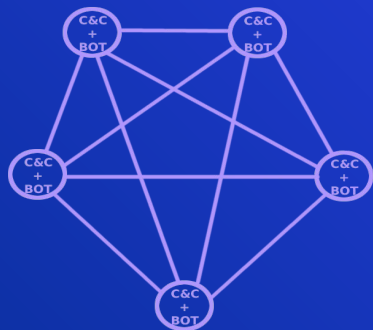
Decentralized Peer-to-Peer



Decentralized Peer-to-Peer (fully meshed)

Advantages:

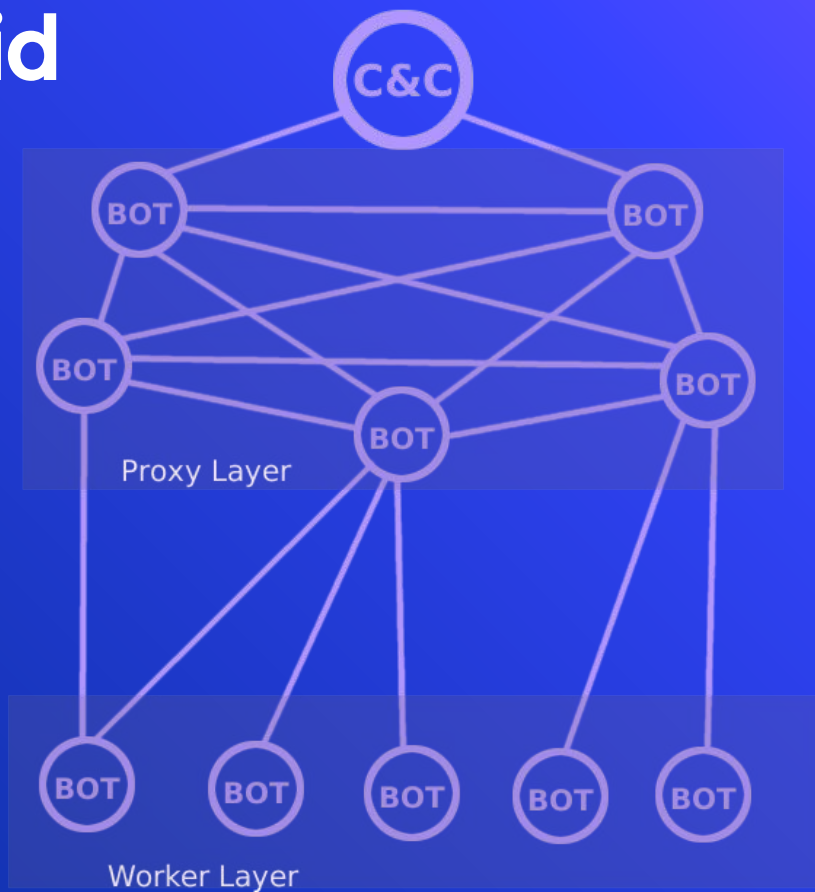
- **low latency**
 - no relaying
- **high robustness**
 - requires a minimum of 2 bots



Disadvantages:

- **low scalability**
 - 65,535 maximum bots if using TCP/UDP
- **high visibility**
 - too many connections
 - requires many coordination messages
- **hard to implement**

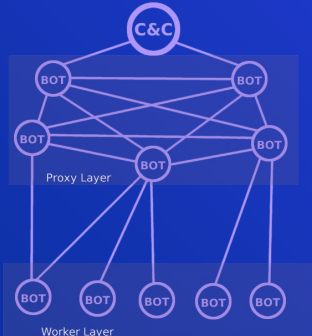
Hybrid



Hybrid

Advantages:

- high scalability
- low visibility
 - if the number of bots in proxy layer is kept low
- **medium robustness**
 - entry nodes point to C&C



Disadvantages:

- hard to implement
- high latency
 - relaying



Botnet Protocols



Communicating within the botnet

- Choice of protocol dependant on architecture of the botnet
- Not uncommon to use a combination of protocols
 - Especially true in hybrid botnets

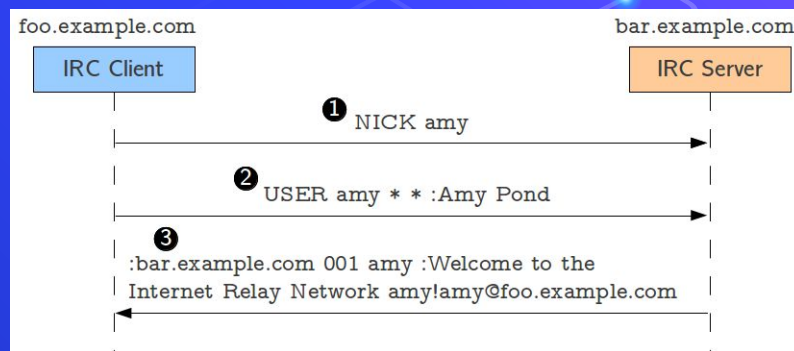


Centralized Botnets

◈ IRC

- Designed for text based communication
- IRC clients implement file sharing over Direct Client-to-Client (DCC)
- Declining usage

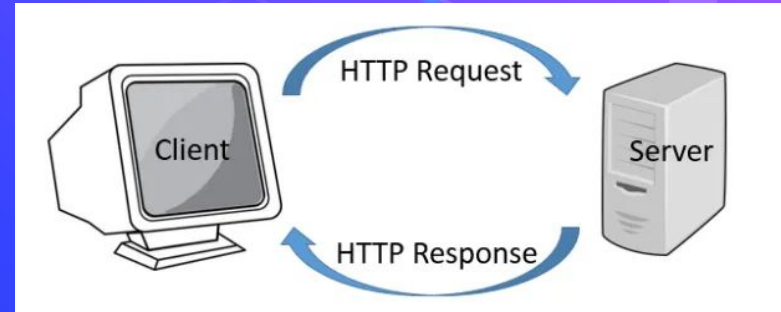
```
@output
<- niven.freenode.net 366 jibbler :
<- phobos!*lala@aocp01518410pcs.reding01.pa.comcast.net PRIVMSG #jollito :http://develop
<- karlcow!*Karla@modencable208.168-70-69.mc.videotron.ca PRIVMSG #jollito :http://dud.hu/
<- surly!*waka@i.get.stabby.net NOTICE #jollito : from phobos :) http://redirx.com/?i
<- golbeck!*chatzilla@ocp05039086pcs.elkrdg01.nd.comcast.net PRIVMSG #hacksack :CashBot,
<- CashBot!*PircBot@ocp05039086pcs.elkrdg01.nd.comcast.net PRIVMSG #hacksack :I'm sorry.
<- JustinCase!*Justin@080sa142.pool014.at101.earthlink.net PRIVMSG #jollito :HI BETSY DEV!
<- patfme!*patfme@ocp04398552pcs.nrockv01.nd.comcast.net QUIT :Remote closed the connection
<- alekibangot!*Danixer@f241.brno.mistral.cz JOIN :$suppybot
<- Betsy_Devine!*Snak8h0003931fac8a.ne.client2.attbi.com PRIVMSG #jollito :Hi Justin!!
-> niven.freenode.net JOIN #test
<- jibbler!*pjn2@torax.ukc.ac.uk JOIN #test
-> niven.freenode.net MODE #test
<- niven.freenode.net 353 jibbler = #test :jibbler Pticed hilbert
<- niven.freenode.net 366 jibbler #test :End of /NAMES list.
<- niven.freenode.net 324 jibbler #test :n
<- niven.freenode.net 329 jibbler #test 1080320728
<- niven.freenode.net 477 jibbler #test :[freenode-info] please register your nickname...
<- golbeck!*chatzilla@ocp05039086pcs.elkrdg01.nd.comcast.net PRIVMSG #hacksack :CashBot,
<- mhlandry!*mhlandry@ip68-96-36-114.no.no.cox.net PRIVMSG #java :there's no way to make
-> niven.freenode.net PRIVMSG #test :hello world
<- Betsy_Devine!*Snak8h0003931fac8a.ne.client2.attbi.com PRIVMSG #jollito :Phobos, Slate?
-> niven.freenode.net PRIVMSG jibbler :testing 1 2 3 ...
<- jibbler!*pjn2@torax.ukc.ac.uk PRIVMSG jibbler :testing 1 2 3 ...
```



Centralized Botnets

⬡ HTTP

- Ubiquitous
- Uses request/response structure
- Inferior to IRC in many regards
 - No group communication
 - Higher latency
- More common in botnets



P2P botnets

⬡ P2P Protocols

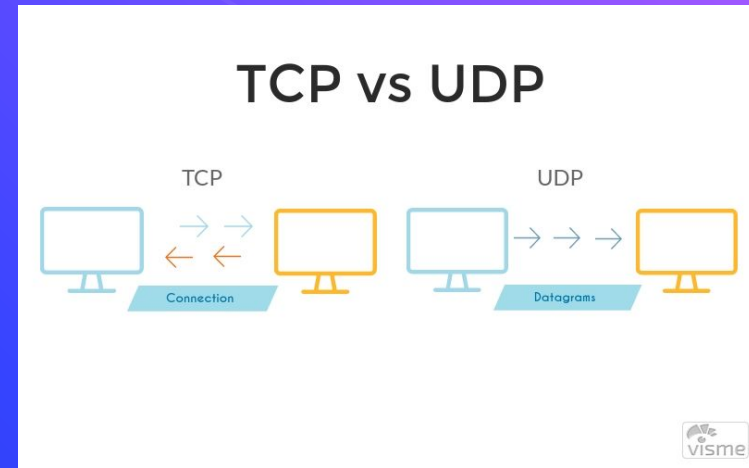
- Many options to choose from
- Examples
 - Bittorrent
 - Gnutella
- Most have all the features you need built in
 - Message relaying
 - Reliability



P2P botnets

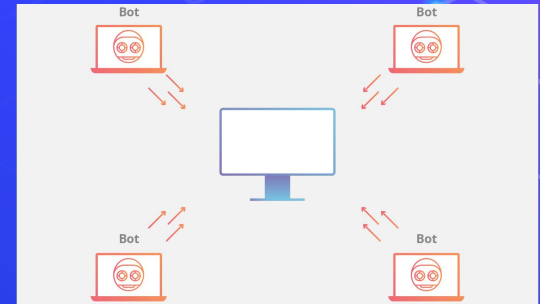
Neoteric Protocols

- UDP
 - Lacks features
 - More lightweight than TCP
 - 8 bytes vs 20 bytes
 - Allows more concurrent connections



Communicating with the web

- Send spam emails
 - Simple Mail Transfer Protocol
- Generate ad revenue
 - HTTP, HTTPS
- DDoS attack
 - HTTP, UDP and TCP



Questions?



Works Cited

- <https://www.bizjournals.com/atlanta/stories/2002/07/22/story4.html?page=all>
- <https://www.zdnet.com/article/phorpiex-botnet-made-115000-in-five-months-just-from-mass-spamming-sextortion-emails/>
- <https://pdfs.semanticscholar.org/bfae/82b6ff8044ac7d20c8c2556b62088af4a415.pdf>
- https://publik.tuwien.ac.at/files/publik_262720.pdf
- <https://defintel.com/blog/index.php/2016/11/how-does-a-botnet-attack-work.html>
- <https://web.archive.org/web/20071012115210/http://www.networkworld.com/news/2007/080207-black-hat-storm-worms-virulence.html>
- <https://www.whiteops.com/blog/9-of-the-most-notable-botnets>

Art and Graphics

- <https://opengameart.org>
- www.openpixelproject.com
- <https://www.slidescarnival.com/aliena-free-presentation-template/4597>

