TAKEDOWN CLIENT-SERVER BOTNETS THE ISP-WAY

Quang Tran - Viettel Group

About me

- Living in Hanoi, Vietnam
- Do research in:
  - Reverse engineering
  - Malware analysis
  - Botnet tracking and sinkhole
- Love:
  - Travelling
  - Football
- Currently working at Viettel
- quangking quangtrm

Content

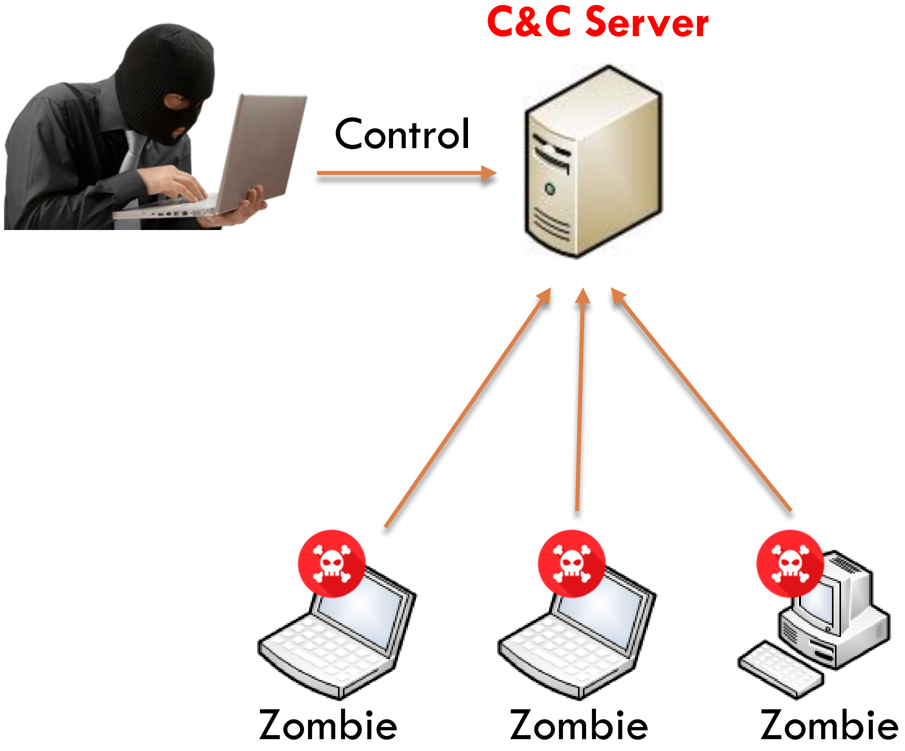
- Why ISP care about botnet takedown?
- Botnet infrastructure
- How botnet usually being taken down?
- ISP advantages
- Taking down a botnet
- Some examples
- Conclusion

Why ISP care about botnet takedown?

- Customer protection
- Network protection
- Law enforcement requests

Botnet infrastructure

- Client-Server botnet



- Centralized command-and-control server(s)
- Command-and-control servers using domain(s) and/or IP(s)
- Commands directly from command-and-control servers

How botnet usually being taken down?

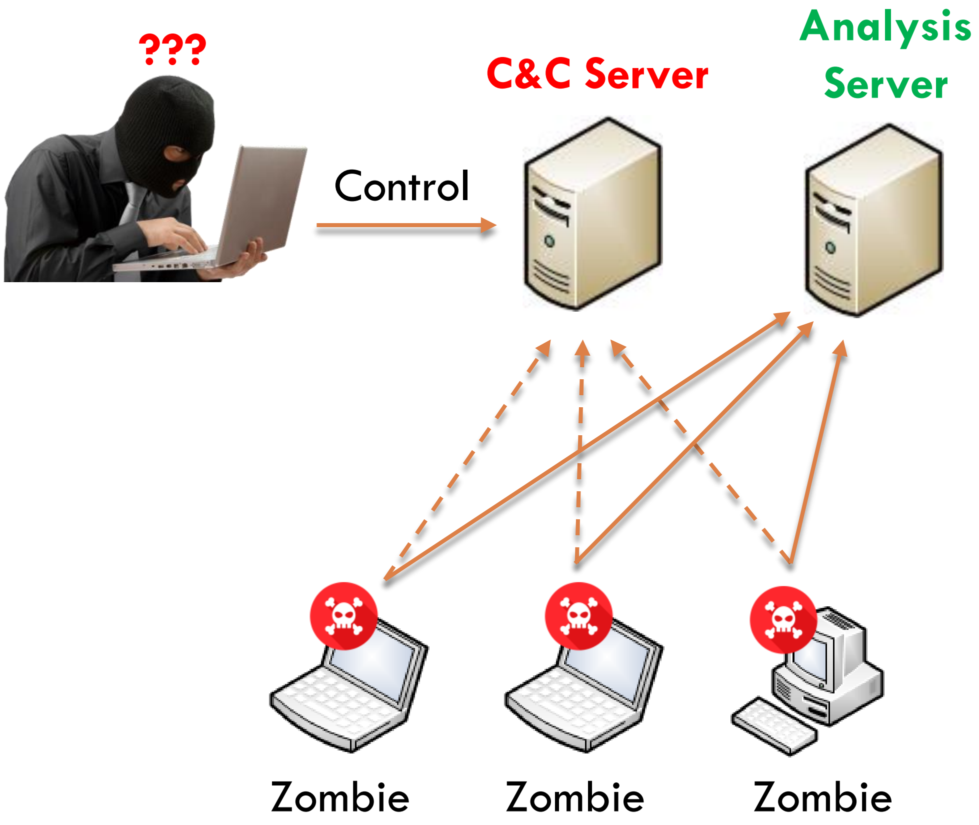
- Client-server botnet
  - Identify command-and-control servers: IP(s), domain(s)
  - Working with service providers to obtain the servers:
    - Re-buy expired domains
    - Request for domain/hosting termination or domain re-buy
- Disadvantages
  - Depend on service providers
  - Nothing to do with bullet-proof domains/hostings

ISP advantages

- Network control and monitor
  - Domain name server (DNS) system
  - Traffic monitoring/processing/routing
  - Deep packet inspection (DPI) framework

Taking down a botnet

- Methodology



- Redirect C&C traffic to ISP's analysis server
- Analysis server works totally the same as the real C&C server
- Send termination command to connected victim
- Inform customer if needed

Taking down a botnet

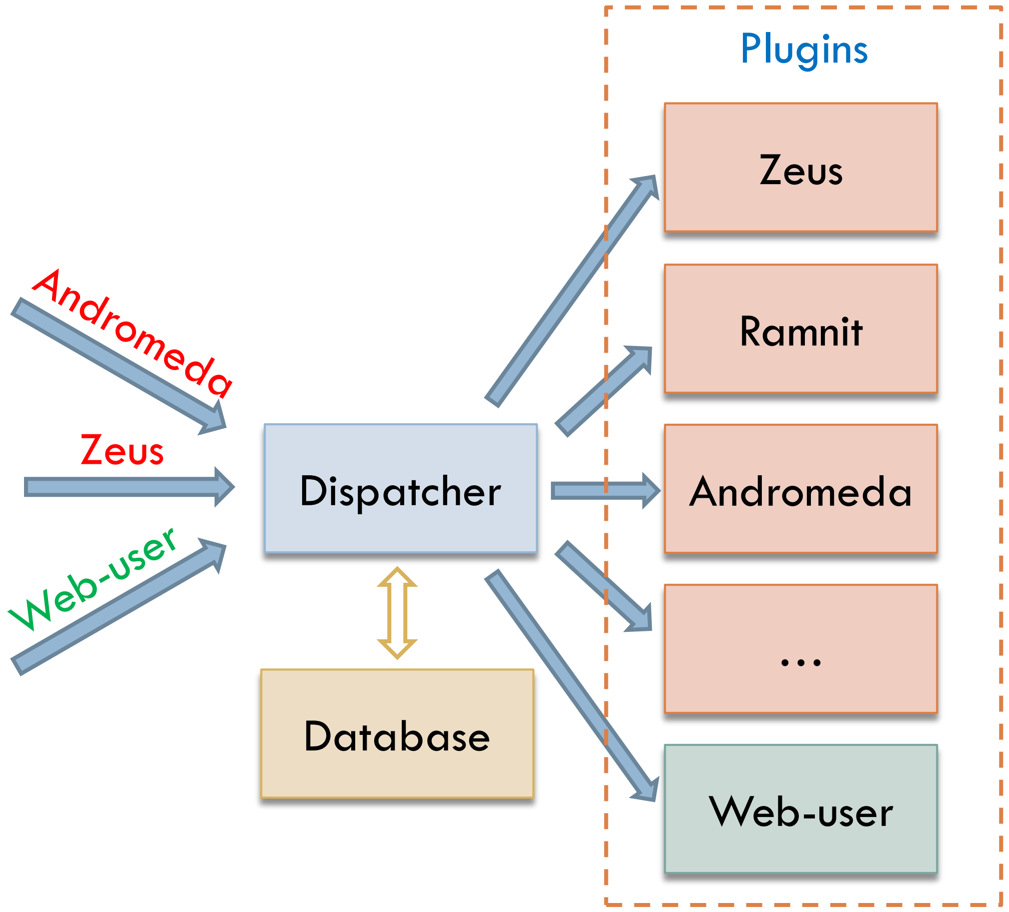
- Target selection
  - Collect information about any botnet found
  - Identify their C&C domain(s)/IP(s)
  - Statistic:
    - Which botnet is running in ISP network?
    - Which botnet has the largest number of customer infected?
    - Which botnet should be care first?
  - Search for some recently samples of chosen botnet

Taking down a botnet

- Reverse engineering
  - Deep reversing
    - Not just to identify C&C domain(s)/IP(s)
    - But to fully build bot protocol
  - Traffic analysis
    - Capture traffic from/to the real C&C servers
    - Ensure the protocol correctly match the captured traffic

Taking down a botnet

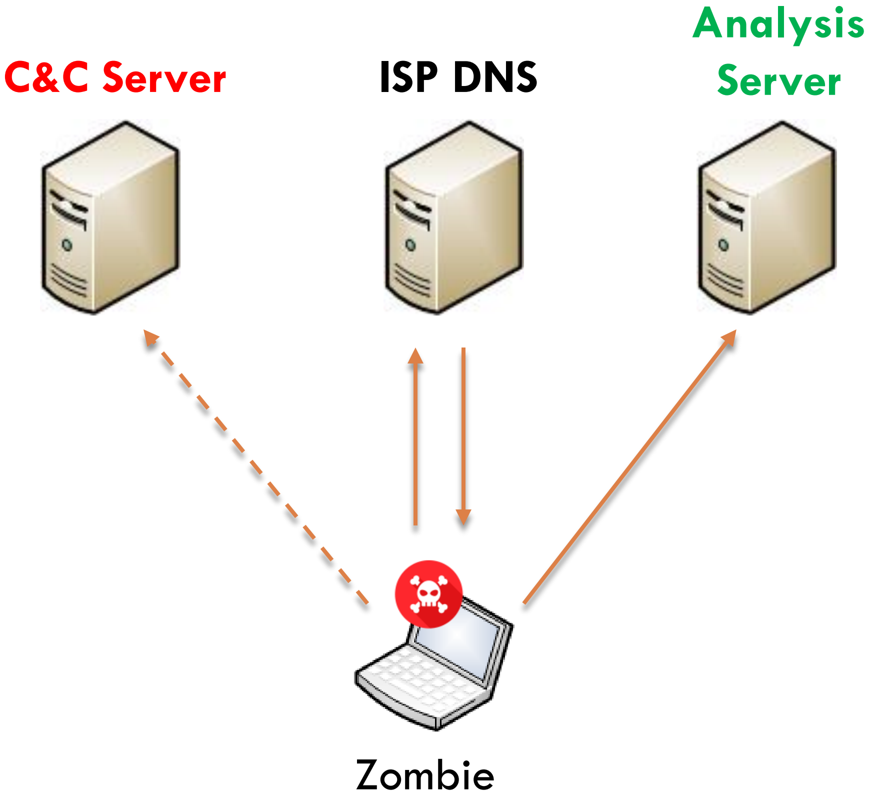
- Sinkhole server



- Identify botnet by content
- Serve each botnet by its own protocol
- Multiple botnet supported
- User notification supported

Taking down a botnet

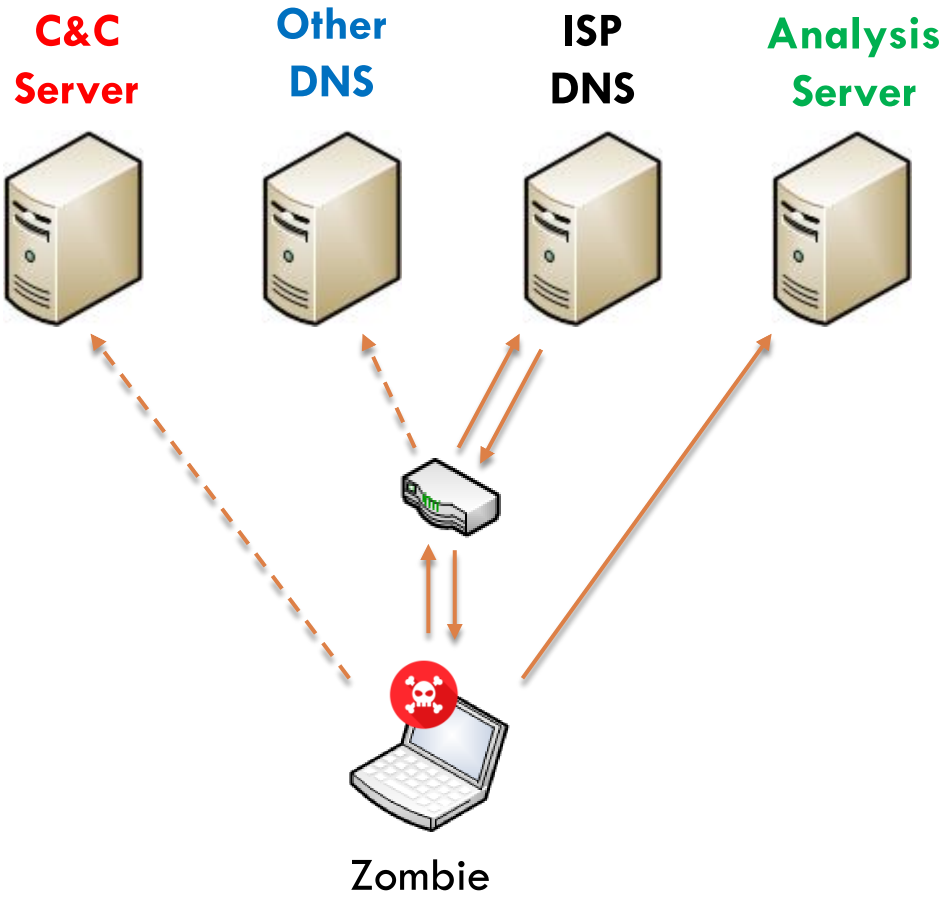
- Command-and-control redirection



- DNS Sinkhole
  - ISP DNS “point” C&C domains to analysis server’s IP

Taking down a botnet

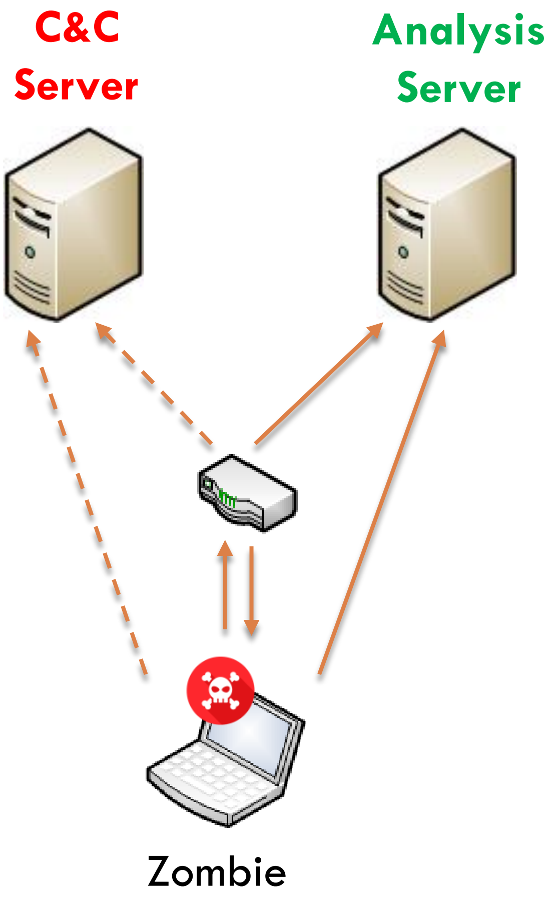
- Command-and-control redirection



- DNS Sinkhole
  - Routing DNS traffic to ISP DNS
  - ISP DNS “point” C&C domains to analysis server
  - Serve other benign traffic as usual

Taking down a botnet

- Command-and-control redirection



- IP routing
  - Routing C&C IPs to analysis server
  - Analysis server uses iptables to NAT and serve bot requests

Taking down a botnet

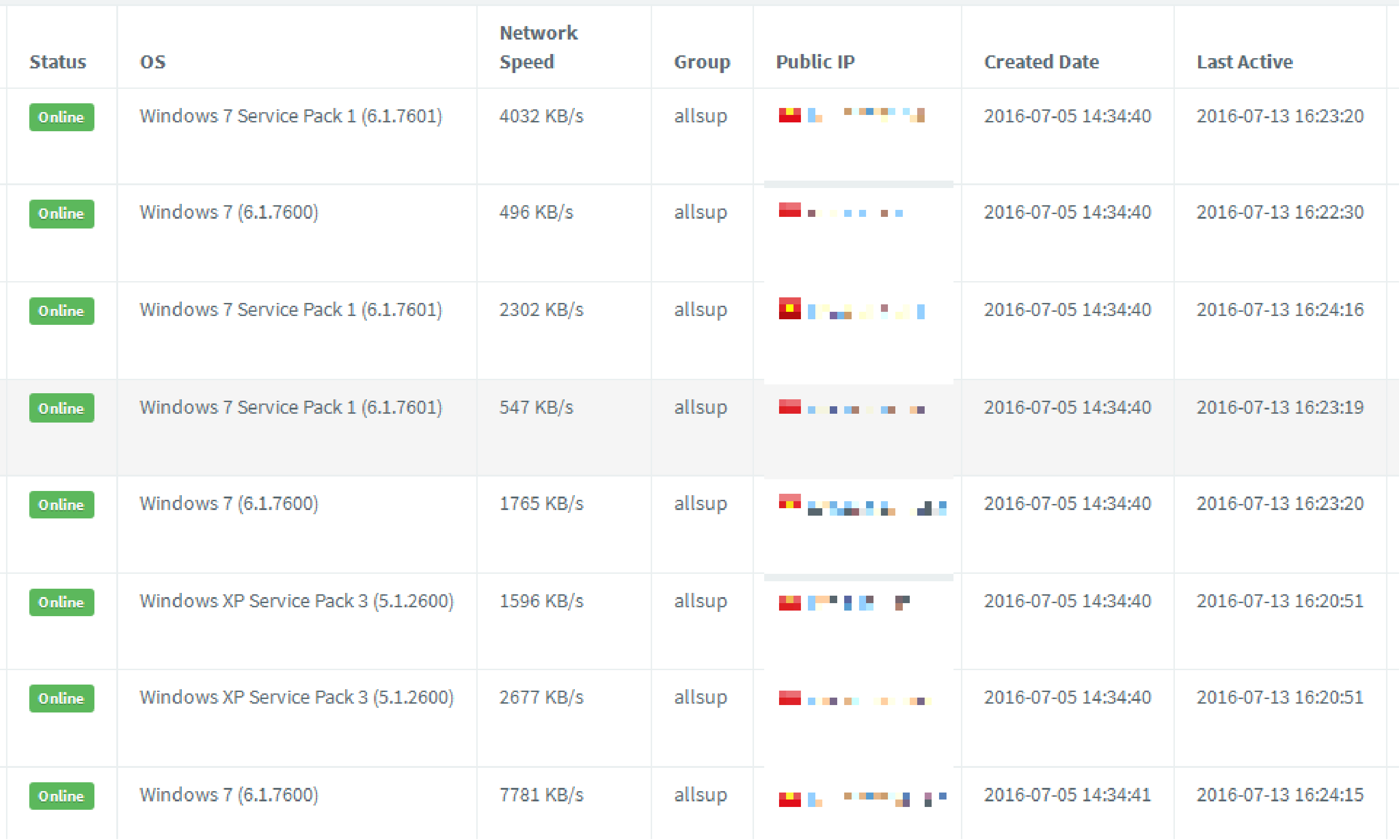
- Control and terminate botnet
  - Serve and save bot information to database
  - Send termination command(s) to bot
  - Notify users if needed

Examples

- Ramnit botnet
  - File virus
  - Protocol
    - Raw TCP (port 447, 443…)
    - Custom RC4 encrypted
  - Commands
    - Update
    - Download and execute
    - Take screenshot
    - Remote data access
    - Kill OS ☺

Examples

- Ramnit botnet sinkhole



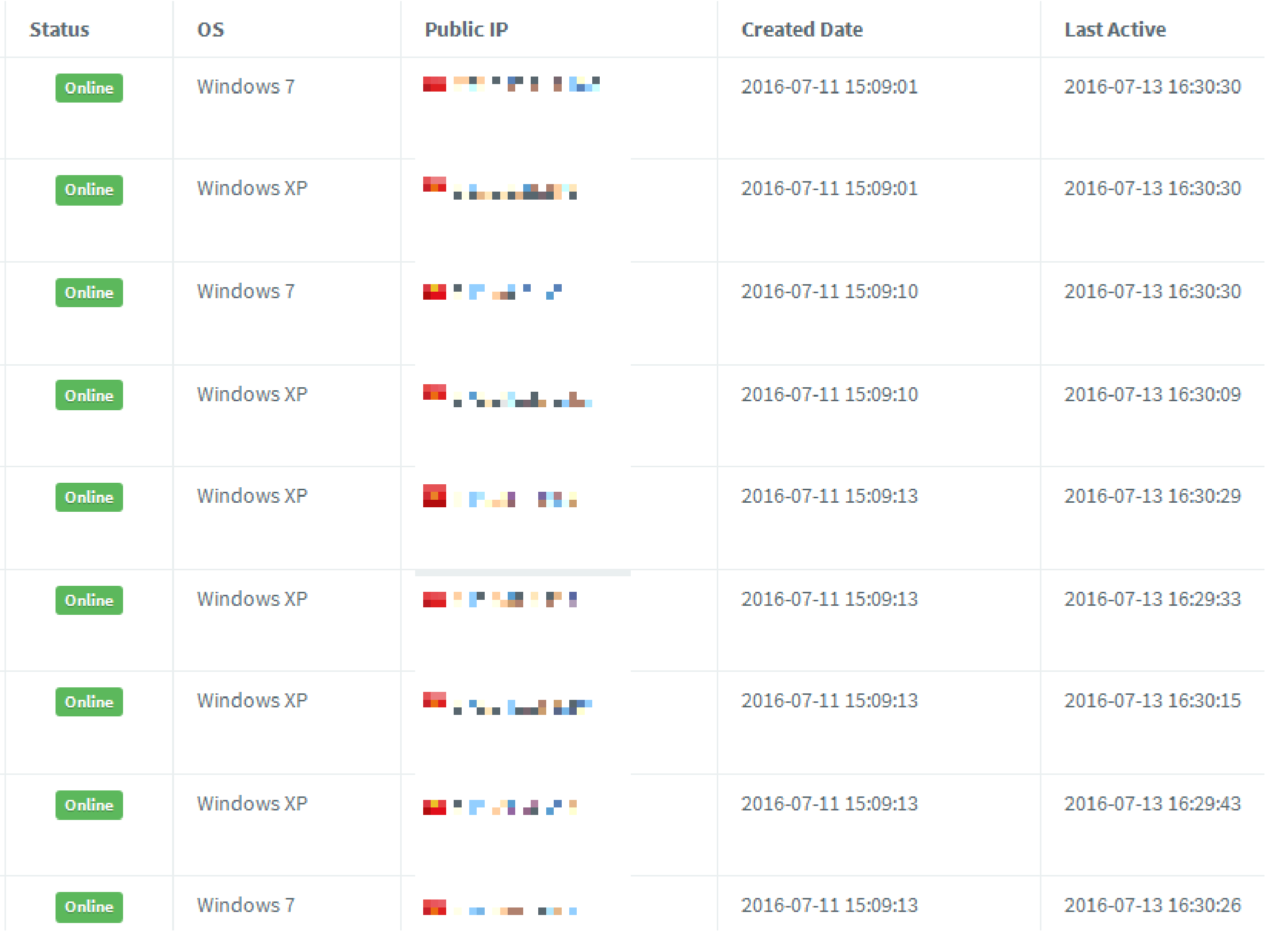
Status	OS	Network Speed	Group	Public IP	Created Date	Last Active
Online	Windows 7 Service Pack 1 (6.1.7601)	4032 KB/s	allsup	[redacted]	2016-07-05 14:34:40	2016-07-13 16:23:20
Online	Windows 7 (6.1.7600)	496 KB/s	allsup	[redacted]	2016-07-05 14:34:40	2016-07-13 16:22:30
Online	Windows 7 Service Pack 1 (6.1.7601)	2302 KB/s	allsup	[redacted]	2016-07-05 14:34:40	2016-07-13 16:24:16
Online	Windows 7 Service Pack 1 (6.1.7601)	547 KB/s	allsup	[redacted]	2016-07-05 14:34:40	2016-07-13 16:23:19
Online	Windows 7 (6.1.7600)	1765 KB/s	allsup	[redacted]	2016-07-05 14:34:40	2016-07-13 16:23:20
Online	Windows XP Service Pack 3 (5.1.2600)	1596 KB/s	allsup	[redacted]	2016-07-05 14:34:40	2016-07-13 16:20:51
Online	Windows XP Service Pack 3 (5.1.2600)	2677 KB/s	allsup	[redacted]	2016-07-05 14:34:40	2016-07-13 16:20:51
Online	Windows 7 (6.1.7600)	7781 KB/s	allsup	[redacted]	2016-07-05 14:34:41	2016-07-13 16:24:15

Examples

- Andromeda botnet
  - Protocol
    - HTTP
    - Custom RC4 encrypted
  - Commands
    - Update
    - Download and execute (EXE, DLL)
    - Uninstall self

Examples

- Andromeda botnet sinkhole



Status	OS	Public IP	Created Date	Last Active
Online	Windows 7	[redacted]	2016-07-11 15:09:01	2016-07-13 16:30:30
Online	Windows XP	[redacted]	2016-07-11 15:09:01	2016-07-13 16:30:30
Online	Windows 7	[redacted]	2016-07-11 15:09:10	2016-07-13 16:30:30
Online	Windows XP	[redacted]	2016-07-11 15:09:10	2016-07-13 16:30:09
Online	Windows XP	[redacted]	2016-07-11 15:09:13	2016-07-13 16:30:29
Online	Windows XP	[redacted]	2016-07-11 15:09:13	2016-07-13 16:29:33
Online	Windows XP	[redacted]	2016-07-11 15:09:13	2016-07-13 16:30:15
Online	Windows XP	[redacted]	2016-07-11 15:09:13	2016-07-13 16:29:43
Online	Windows 7	[redacted]	2016-07-11 15:09:13	2016-07-13 16:30:26

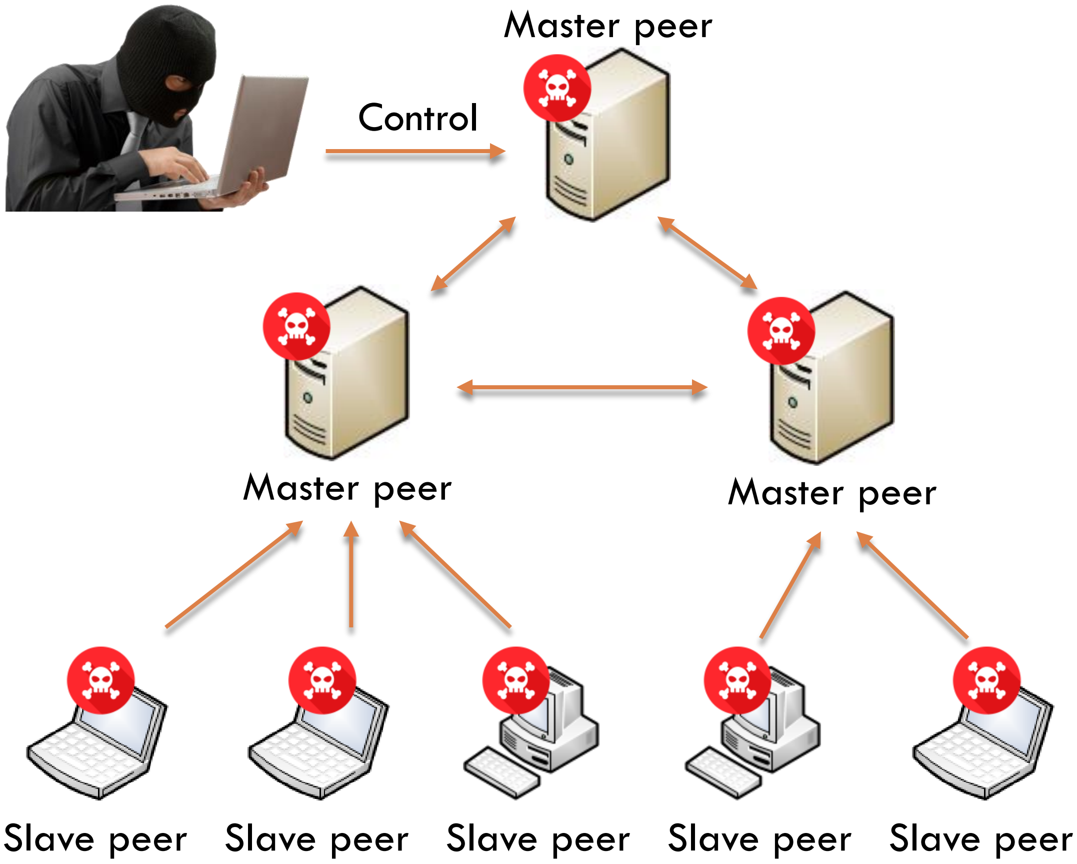
Conclusion

- Pros
  - Easy and quick to deploy
  - Work with most client-server botnet
  - Fit for any ISP
  - Easy to co-operate between ISPs, countries
- Cons
  - Not work on anti-takeover botnet (bots verify server before executing commands)

Thank you!

Botnet infrastructure

- □ Peer-to-Peer botnet



- Peer-to-peer network
- Two types of peer: Master and Slave
- Commands received from master peers
- Bot owner controls some master peers

How botnet usually being taken down?

- Peer-to-peer botnet
  - Join peer-to-peer botnet network
  - Identify owner’s master peers
  - Pretend to be a master peer
  - Send commands to isolate owner’s peers from network
  - Send commands to remove botnet itself