Communication Structures of Botnets with Case Studies

Nicholas Cornhill
cornh044@morris.umn.edu

Division of Science and Mathematics
University of Minnesota, Morris

December 1, 2012

What Are Botnets

- Botnets are networks of computers infected with bot code
- Bot code allows a third party to control a computer
- The botmaster controls the botnet
- Botnets steal private information, send spam, or perform DDoS attacks among other activities

What is a Communication Structure

- Communication structures organize communication with the botnet
- Allows botmaster to control the botnet easily and quickly
- Knowing the communication structure is important to detect and take down a botnet
- There are two main kinds of communication structures:
    - Command and Control (C&C)
    - Peer-to-Peer (P2P)

1. Introduction

2. Communication Structures
    - C&C Botnets
    - P2P Botnet
    - Botnet Detection and Overlays

3. Case Studies
    - Miner Botnet
    - Waledac Botnet

4. Conclusion

C&C Communication Structure

- Bots communicate with one or more central servers (1)
- Host is infected with shellcode
- Shellcode directs host to download bot
- Then machine contacts a server and waits for orders

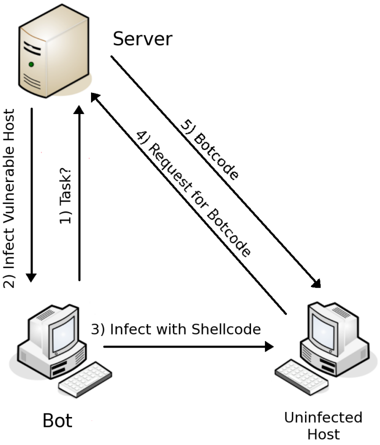


Figure: The infection process of a C&C botnet

C&C Analysis

Pros:

- Low latency (1)
- Simple to write (1)

Cons:

- Easy to detect
- Removal of central point takes down botnet (2)

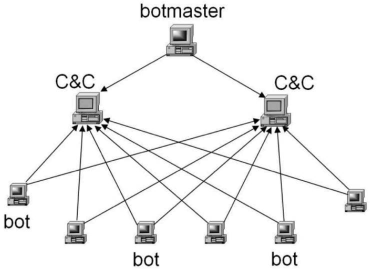


Figure: An example of how a C&C structured botnet may be set up.

P2P Communication Structure

- Decentralized structure
- Communication occurs directly with other bots
- Messages are passed through network

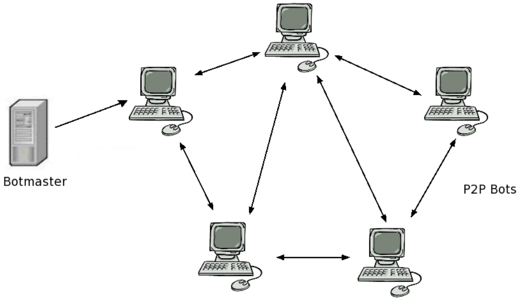


Figure: An example of how a P2P structured botnet may be set up.

P2P Communication Structure

- Host is infected with shellcode
- Bot must find other bots in the network
- Populate initial peerlist
- Use to diversify peerlist
- Process is repeated periodically

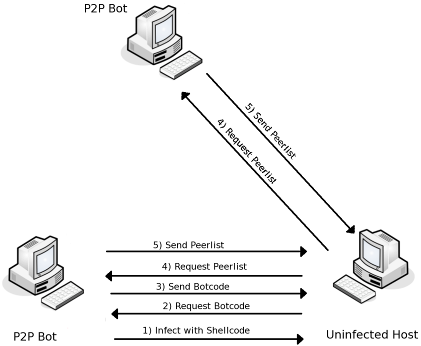


Figure: The infection process of a P2P botnet.

P2P Analysis

Pros:

- Hard to detect
- Very robust

Cons:

- High latency
- No guarantee of communication (2; 4)

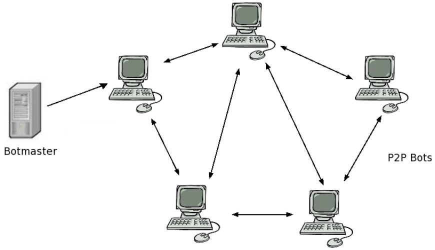


Figure: An example of how a P2P structured botnet may be set up.

Communication Structures and Botnet Detection

- Overlay topologies can detect botnets (5)
- Overlay topology is a description of a pattern in a graph
- An overlay can be based on a communication structure

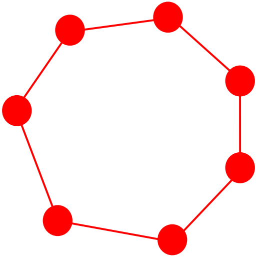


Figure: An example of a ring graph.

Detecting Botnets Using Overlays

- Only cares about if communication occurred
- Encryption or other techniques to disguise data are not effective (3; 5)
- Must be used in conjunction with other detection techniques (5)

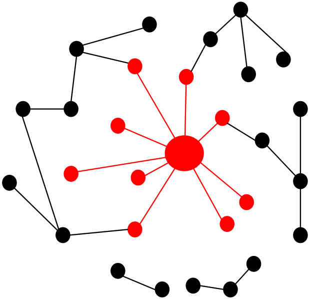


Figure: An example of a C&C overlay in use.

1. Introduction
2. Communication Structures
   - C&C Botnets
   - P2P Botnet
   - Botnet Detection and Overlays
3. Case Studies
   - Miner Botnet
   - Waledac Botnet
4. Conclusion

Background of Miner Botnet

- Active from December 20th, 2010 to February 2012
- DDoS attacked German and Russian Websites
- Started mining bitcoins around May 2011 (6)

Miner Botnet Communication Structure

- Started out as pure C&C botnet (6)
- P2P aspects added later on
- Hybrid communication structure
    - Increases robustness
    - Easier for botmaster to handle

Miner Botnet Communication Structure

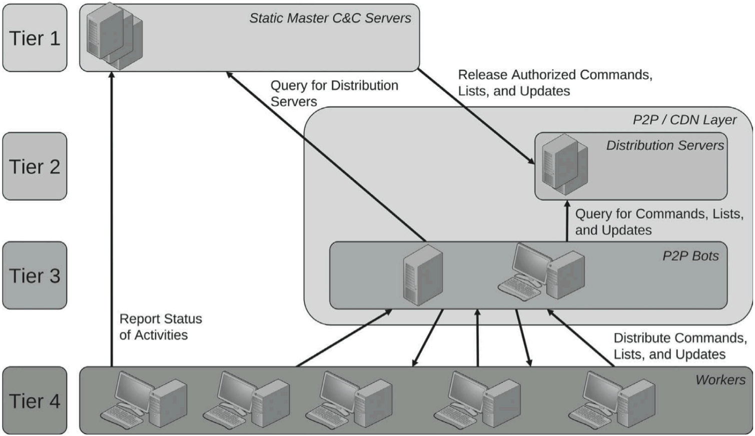
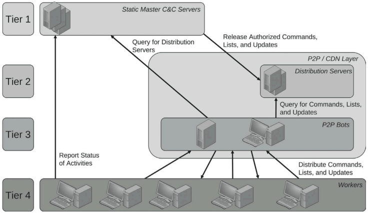

Tier 1
Static Master C&C Servers
Query for Distribution Servers
Release Authorized Commands, Lists, and Updates
Tier 2
P2P / CDN Layer
Distribution Servers
Query for Commands, Lists, and Updates
Tier 3
P2P Bots
Report Status of Activities
Distribute Commands, Lists, and Updates
Tier 4
Workers

Figure: The four tiered communication structure of the Miner botnet. Image taken from (6)

Analysis of Communication Structure


Tier 1
Static Master C&C Servers
Query for Distribution Servers
Release Authorized Commands, Lists, and Updates
Tier 2
P2P / CDN Layer
Distribution Servers
Query for Commands, Lists, and Updates
Tier 3
P2P Bots
Report Status of Activities
Distribute Commands, Lists, and Updates
Tier 4
Workers

- Very robust design
- Multiple back up systems
- More communications than a normal P2P network

1. Introduction

2. Communication Structures
   - C&C Botnets
   - P2P Botnet
   - Botnet Detection and Overlays

3. Case Studies
   - Miner Botnet
   - Waledac Botnet

4. Conclusion

The Waledac Botnet

- Was active from December 2007 to 2010 (7)
- Predecessor to Storm Botnet
- Somewhere between 70,000 to 160,000 members at peak

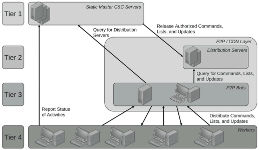
Around the size of Fargo, ND

CITY OF
Fargo

The Waledac Botnet

- Takedown occurred in Feburary 2010
- Headed by Microsoft
- Symantec and other Universities helped (8)
- Same communication structure as Miner botnet

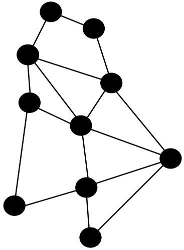
Disrupting the Upper Levels


Tier 1
Static Master C&C Servers
Release Authorized Commands, Lists, and Updates
Query for Distribution Servers
Tier 2
P2P / CDN Layer
Distribution Servers
Query for Commands, Lists, and Updates
Tier 3
P2P Bots
Report Status of Activities
Distribute Commands, Lists, and Updates
Tier 4
Workers

- Microsoft court order blocked 277 domain names (8)
- Removed the entire upper two levels of the botnet
- Botnet would have still survived
- Effective until botmaster purchased new domain names

Disrupting the Lower Levels

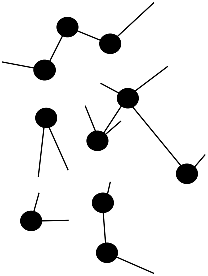
- Used Peerlist poisoning (7; 9)
- Fake bots are added to botnet
- Plant non-existent bots into peerlists
- Causes ability to propagate messages to degrade



An example of a botnet before peerlist poisoning

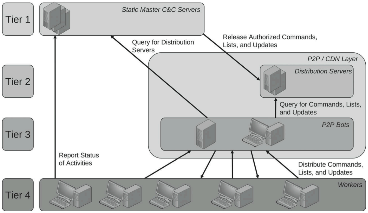
Disrupting the Lower Levels

- Used Peerlist poisoning (7; 9)
- Fake bots are added to botnet
- Plant non-existent bots into peerlists
- Causes ability to propagate messages to degrade



An example of a botnet after peerlist poisoning

Composite Effect


Tier 1
Tier 2
Tier 3
Tier 4
Static Master C&C Servers
Query for Distribution Servers
Release Authorized Commands, Lists, and Updates
P2P / CDN Layer
Distribution Servers
Query for Commands, Lists, and Updates
P2P Bots
Report Status of Activities
Distribute Commands, Lists, and Updates
Workers

- Neither level strictly necessary
- Both levels had to be disrupted in unison
- Short window of opportunity

Conclusion

- Knowing how the botnet is set up is critical for takedown
- Decision to use P2P or C&C networks is a trade-off
- Mixing the two systems creates a very robust botnet

Questions

Questions?

Bibliography I

[1] M. Abu Rajab, J. Zarfoss, F. Monrose, and A. Terzis. A multifaceted approach to understanding the botnet phenomenon. In *Proceedings of the 6th ACM SIGCOMM conference on Internet measurement*, IMC '06, pages 41–52, New York, NY, USA, 2006. ACM.

[2] M. Bailey, E. Cooke, F. Jahanian, Y. Xu, and M. Karir. A survey of botnet technology and defenses. In *Conference For Homeland Security, 2009. CATCH '09. Cybersecurity Applications Technology*, pages 299 –304, march 2009.

[3] H. Choi, H. Lee, and H. Kim. Botgad: detecting botnets by capturing group activities in network traffic. In *Proceedings of the Fourth International ICST Conference on COMmunication System softWAre and middlewaRE*, COMSWARE '09, pages 2:1–2:8, New York, NY, USA, 2009. ACM.

[4] M. Jelasity and V. Bilicki. Scalable stealth mode P2P overlays of very small constant degree. *ACM Trans. Auton. Adapt. Syst.*, 6(4):27:1–27:20, Oct. 2011.

Bibliography II

[5] S. Nagaraja, P. Mittal, C.-Y. Hong, M. Caesar, and N. Borisov. Botgrep: finding p2p bots with structured graph analysis. In *Proceedings of the 19th USENIX conference on Security*, USENIX Security'10, pages 7–7, Berkeley, CA, USA, 2010. USENIX Association.

[6] D. Plohmann and E. Gerhards-Padilla. Case study of the Miner botnet. In *Cyber Conflict (CYCON), 2012 4th International Conference on*, pages 1 –16, june 2012.

[7] G. Sinclair, C. Nunnery, and B. Kang. The Waledac protocol: The how and why. In *Malicious and Unwanted Software (MALWARE), 2009 4th International Conference on*, pages 69–77. IEEE, 2009.

[8] Wikipedia. Waledac botnet — wikipedia, the free encyclopedia, 2012. [Online; accessed 12-November-2012].

[9] J. Williams. What we know (and learned) from the Waledac takedown. `http://blogs.technet.com/b/mmpc/archive/2010/03/15/what-we-know-and-learned-from-the-waledac-takedown.aspx`, Mar. 2010.

The End

FREEDOM!