Chair for Network Architectures and Services
Department of Informatics
TU München – Prof. Carle

Peer-to-Peer Systems and Security

Chapter 2
2.4 Botnets

Dipl.-Inform. Heiko Niedermayer
Prof. Dr. Georg Carle

Vorlesung SS 2009

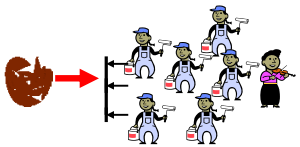
Overview

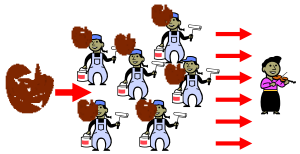
- Motivation
- Botnet Basics
- Fast-Flux Networks
- Peer-to-Peer and security concepts
- Conficker
- Conclusion

Motivation

Motivation

- Peer-to-Peer network can be used for security and resilience.
  - e.g. Censorship-resistance
- Can Peer-to-Peer networks also be used as a tool for attacks?
  - Control all or a subgroup of peers to launch an attack?
  - Attacker subnetwork?
  - Operate as botnet.





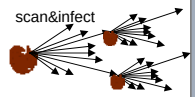
Virus / Worm / Bot

Virus

- Malware that attaches itself to a host software or script.
- If the host is executed, the malware is executed.

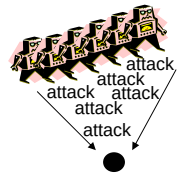
Worm

- Self-replicating malware.
- Uses network to distribute itself.
  - Exploits weaknesses in operating system or networked software.



Bot

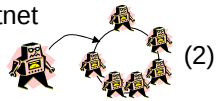
- Program to automate task, here: focus on malicious bots.
- Often self-replicating malware.
  - Like worms, but more passive as bots do not want to be detected.
- Bots (also called Zombies) are used to launch distributed attacks.
  - Distributed Denial-of-Service (DDoS), Spam, …



Botnets are Business

(1) Botnet master (herder) uses a weakness / hole to enter other computers.

(2) Infected computers register themselves in the botnet and wait for commands of their master.



(3) Someone pays the herder to use some of the bots for attacks, Spam, or illegal sites (4).

- Contrary to worms, the botnet is not the attack itself. Its use is to launch subsequent attacks. Botnets are used for cybercrime and cyberwar.

Bots and Botnets

A bot needs

- Mechanisms to infect other computers
  - Exploit weakness in software, protocols, passwords, …
- Command & Control interface
  - For the owner (herder) and for users of the botnet.
- Attack code
  - For DDoS, Spam, Phishing, etc.
- Code for self-protection
- Download and Update of bot software

Infection

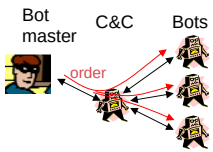
Infection

- Exploit weakness in networked software or operating system.
  - Use the protocol of the flawed software to find other nodes.
    - Email, P2P network, …
  - Scan network (IP scan, Port scan)
    - Applications listen on specific port or typical port ranges.
    - Check if node is infectable, then infect.
  - Drive-by download attacks
    - When a user visits a website, browser downloads malicious software without user knowledge. Browser weaknesses may allow subsequent execution.
- Without software or hardware weakness
  - Use autorun functionality on USB sticks and other external devices.
    - Copy bot onto the device.
  - Hide bot in a useful application as trojan horse.
  - Guess passwords, use default passwords that might not have been changed.
  - Emails with malicious attachments (e.g. „Iloveyou.exe“)
  - …

Command & Control / IRC

Command & Control

- Bot master controls the botnet via C&C hosts on infected machines.
- Command & Control channel is usually hidden and bots may redirect messages from the bot master to hide its identity.



IRC-based botnets (old)

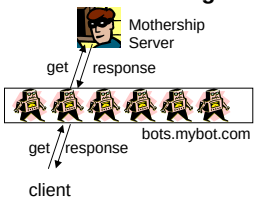
- Use Internet Relay Chat as C&C.
- Bots know a DNS name.
  - *mybotnet.dyndns.org*
  - IP of current IRC server, dynamic DNS.
- IRC server is installed on infected host.
- The bot master gives the bots orders via chat.
  - Execute attack.
  - Download and update new software packets for the bot.
  - …

Fast Flux Networks

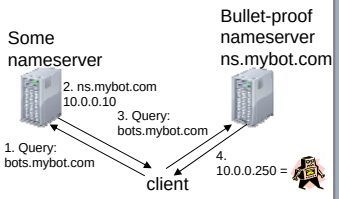
Fast Flux

- Maps a domain to many IP addresses.
- Round robin of addresses with short TTL of DNS Ressource Records.
  - e.g. valid for 3 min.
- A subset of bots is used in the fast flux. The bots operate as gateways / proxies to the mothership.
- Single-Flux
  - A name server that is bullet-proof is used to manage a third-level-domain.
  - The DNS resolution will return a different bot everytime.

Fast Flux Hosting



Single Flux DNS

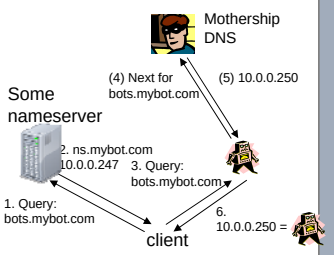


Fast Flux Networks

Fast Flux II

- Double-Flux
  - The fast flux principle is applied to the name server as well.
  - Bots operate as nameservers and the name server for the domain changes frequently.
  - The DNS operation is done by the mothership and the bots operate as proxies.
  - Needs cooperation of registrar in order to continously change the nameserver.
- Fast Flux has legitimate use-cases
  - Akamai and other services use fast flux to provide resilient access to highly frequented websites.
  - Fast Flux is used to circumvent cencorship in repressive regimes.
  - Differentiation of good and bad fast flux is a problem.

Double Flux DNS



Changing Domain Names

Observation

- Fast Flux relies on the cooperation of nameservers.
- What if domains get dropped or access to the nameserver gets blocked?

⇒ Change domain names regularily.

Random Domain Names

- Current bots like Conficker change the domains frequently according to a pseudo random number generator.
- Bots connect to some of the random domain names within a botspecific time-interval.
- Advantages
  - Before a provider recognizes the abuse the botnet shifts to another domain.
  - If a domain is shut down, the bots are not lost, but connect to a new one.

Peer-to-Peer concepts for Botnets

Peer-to-Peer botnets

- Organize bots in P2P network.
- Self-organization among bots.
- Hide mothership behind P2P routing.
  - Who gave the command?
- Option: Use existing Peer-to-Peer infrastructure to hide in.
- Discussion / Trade-Offs
  - Routing may be used to reach and scan botnet by others than bot master.
  - Activity may reveal computer as being infected by the bot. However, activities necessary for the network to grow and remain.
    - Scan network to infect new machines.
    - Form and maintain Peer-to-Peer network.
  - Opposite alternative: Be silent and hide
    - There is a proposal to rely on neighbor set given at the time of infection.
      - Good: Avoids leakage of other nodes, harder for network IDS to detect bots,..
      - Bad: Stable enough? Routing? How to infect / still scanning the network?

Security Concepts for bots

Communication and Orders

- Public key cryptograhpy instead of passwords for orders.
- Messages and payload protected with HMAC and symmetric encryption.
- Signature of code and updates.

Self-Protection

- Root kit and other local obfuscation → against detection
  - Stop scanners, operating system updates, …
- Avoid IP ranges of OS and security companies → against analysis
- Avoid attacking own computer
  - e.g. Conficker does not start when Ukranian keyboard is used.
- Some bots patch the exploited weakness.

Conficker

Conficker

- Botnet that appeared late 2008, size estimation > 10 million computers.
- Modular structure
  - Infection only contains a basic bot.
  - Further modules downloaded from botnet, e.g. a scareware module in April 2009.
- Self-Protection
  - Cryptography
    - Updates and orders are secured with 4096 bit RSA signatures (OpenSSL library).
    - MD6 und RC4 for message protection.
  - Analysis
    - Obfuscation of code to fight analysis.
    - Blacklisting of IP ranges from security companies, Microsoft, etc.
  - Stops windows update, virus scanners, safe-mode, … (varies from version to version)
- Infection
  - MS08-067 server service vulnerability, but also uses other ways to spread like USB drives and network shares.
- Changing domain names
  - Conficker.C 50000 per day from 110 tld suffixes. A bot randomly checks 500 of them.
    - Current date determined from standard websites with time information.
    - Collides with existing 150-200 websites per day.

Conclusion

Conclusion

- Botnets are increasing threat on the Internet
  - Used for DDoS, Spam, …
- Technology
  - …from IRC-based to Peer-to-Peer…
  - …from weak to strong security….
  - …from monolithic bots to modular bots with updates and plugins…
- Conficker