Botnets: detection & mitigation

I. Pustogarov

Papers

- Botnets: Measurement, Detection, Disinfection and Defence, European Network and information Security Agency (ENISA) tech report, 2011
  - Sections: 1.2, 3.1, 3.2, 3.3

- BotHunter: Detecting Malware Infection Through IDS-Driven Dialog Correlation, Gu et al., USENIX Security'07
  - Sections: 1, 2, 3, 4 (subsections from Sec 4 are NOT included)

Botnets – definition, features

- Botnets: networks of infected end-hosts, called bots, that are under the control of a human operator commonly known as a botmaster
- Bot software: advanced malware that makes the functionality of a compromised host available to the botmaster
- Bots can:
  - propagate like worms
  - hide from detection like many viruses
  - attack like many stand-alone tools
  - have an integrated command and control system

Propagation and compromise

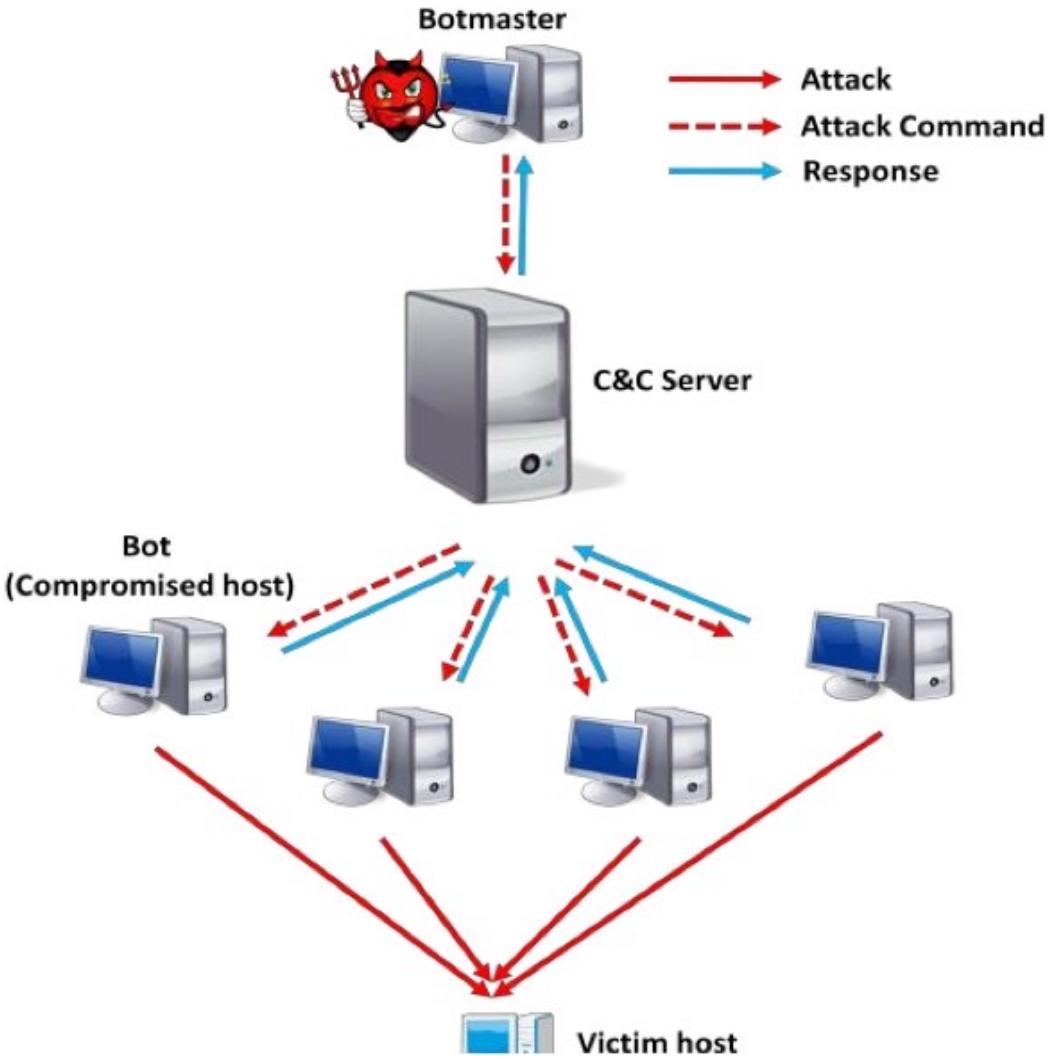
- How to put your bot in a user PC?
  - How about asking the user?
  - Users will not agree to do so, but generally they don't care if the machine is "usable" after an infection
- Several independent infection/propagation mechanisms
  - OS/browser/application vulnerabilities
  - Open file shares
  - P2P networks
  - Backdoors from a previous infection
  - Social engineering, "curious George" attacks
  - Trojaned applications

Command and control

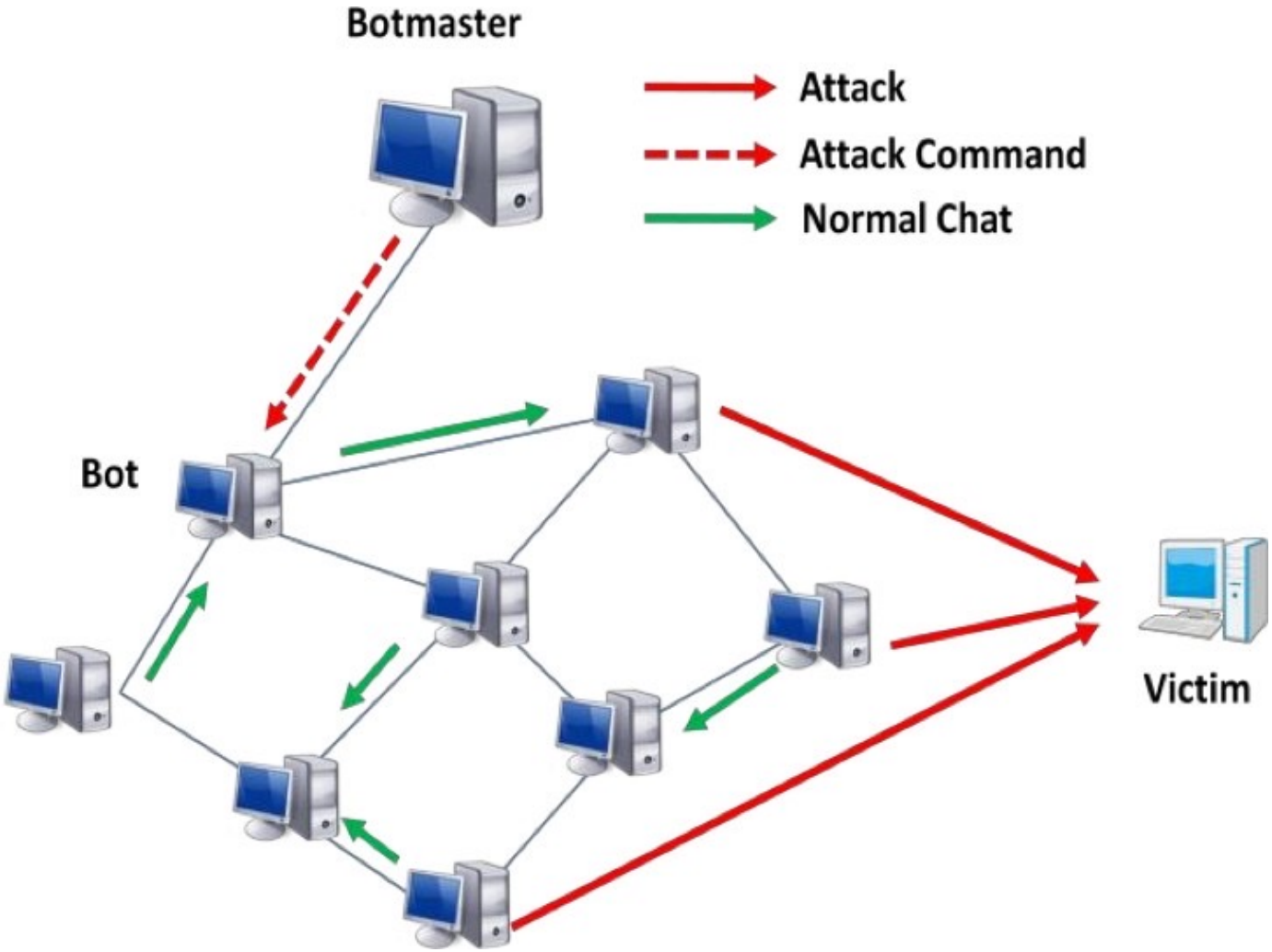
A central part in ALL botnet design

1. Centralized: better control and efficient attacks, but single-point vulnerability -- Channels: IRC, HTTP; servers can also be hierarchical
2. P2P: robust against disruption, but inefficient and unreliable from attackers' viewpoint
3. Locomotive
4. Hybdrid

Centralized architecture (IRC/HTTP)



P2P architecture



DNS de-registration and IP blocking

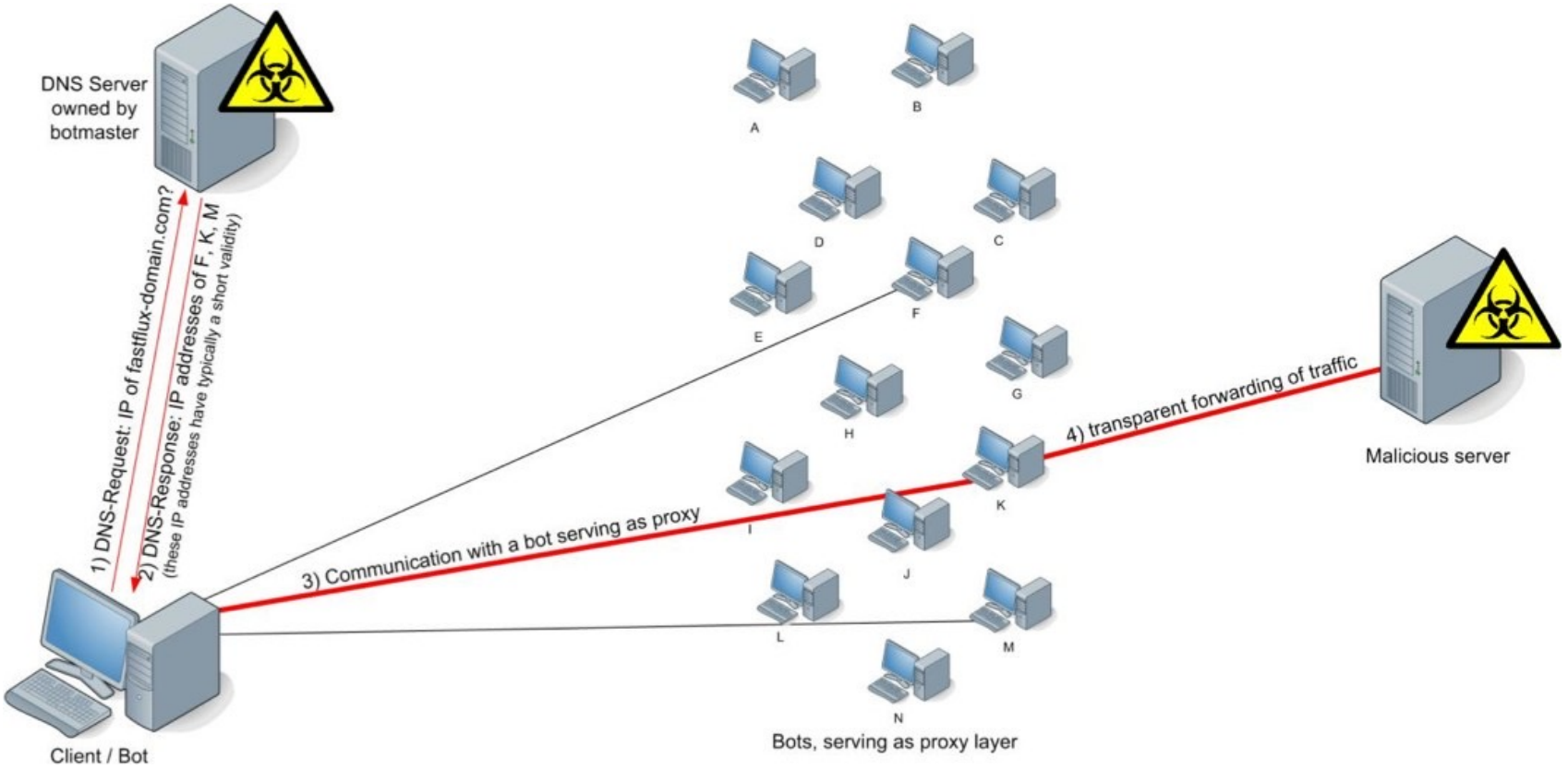
- Centralized C&C relies on DNS to move command servers from one IP to another
- How to hide your malware/phishing servers?
- De-registration of malicious domains can happen – result in loss of control
  - One main tool to dismantle botnets
- C&C server IPs may also be blocked

- How to survive, if you are a botmaster?
  - Fast-Flux Service Networks (FFSN)
  - Similar to Content Delivery Networks (CDN)

Fast-flux

- One domain name is assigned to multiple (100's or 1000's) IP addresses
- IP addresses are swapped in and out of flux with extreme frequency (e.g., 5 minutes)

Example fast-flux



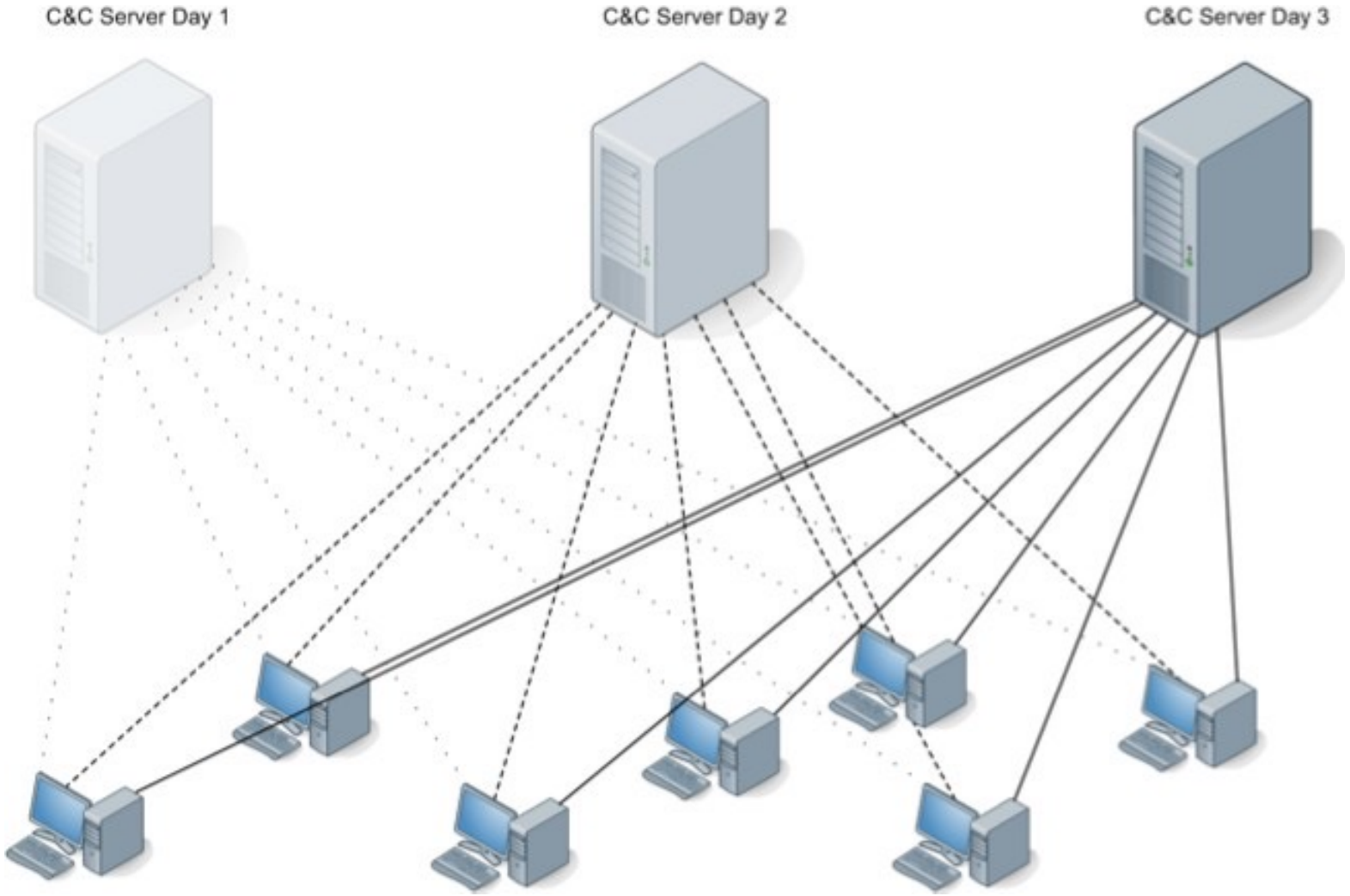
Dynamic domain names

- Still having a single domain is problematic
- Register multiple domains
  - But names can be learned in advanced and blocked
  - Bots can be reverse-engineered to extract domains

- Solution: Domain Generation Algorithms (DGA)
  - Generate domain names depending on one or more external information sources serving predictable seed values that can be accessed by bots and botmasters
  - Seed values: timestamp, Twitter trends

“Locomotive” botnet

(improved survival for a centralized C&C botnet)



Hybrid C&C

- A mixture of P2P and Centralized can be exploited
- A recent example: the Necurs botnet
  - See: https://www.technadu.com/necurs-botnet-evolves-carry-payloads-hide-better/60029/
  - Old botnet from 2012, but survived (current infection: over 570,000)
  - Payloads include: DDoS, crypto mining, ransomware
  - Dismantled by Microsoft and partners (March 2020): https://blogs.microsoft.com/on-the-issues/2020/03/10/necurs-botnet-cyber-crime-disrupt/
- The central C&C server distributes peer lists to bots – at certain intervals
- If the C&C cannot be reached, P2P and DGA domains are used for communication

Botnet usage

- Known uses:
  - DDoS, spam, credentials theft, click-fraud
  - Pay-per-install (malware/adware/badware)
  - Political agenda:
    - Estonia attack (2007),
    - GhostNet (2009), Shadow network (2010)
    - Stuxnet (2010), Flame (2012)

Measurement and detection Techniques

- Passive techniques
  - Data collected from observations – honeypots
  - Does not interfere with botnet activities
    - Transparent to botmaster
- Active techniques
  - Actively interact with the botnet to understand it
  - Better understanding and measurements
  - Bot activities may be disrupted – detectable by botmaster
  - Researchers may be targeted by botmaster
- Reverse engineering of bots
  - Several anti-reverse engineering techniques are used: obfuscation, encryption, dynamic updating