Botnets: Detection, Measurement, Disinfection & Defence

Project Findings – Technical Aspects

Daniel Plohmann

daniel.plohmann@fkie.fraunhofer.de

Fraunhofer FKIE

Botnets: Detection, Measurement, Disinfection & Defence
Project Findings – Technical Aspects

- **Approaches to detection & measurement of botnets**
  - Identified methods
  - Common characteristics
  - Conclusion: Size is not everything
- **Approaches to botnet countermeasures**
  - Identified methods and their targets
  - Current practices and challenges
  - Conclusion: complement and coordinate efforts
- **Question of Roles in the fight against botnets**
  - Legal aspects
  - Relevant stakeholders

Approaches to

DETECTION & MEASUREMENT OF BOTNETS

Approaches to detection & measurement of botnets
Identified Methods

- **Passive Techniques**
  - Packet Inspection
  - Analysis of Flow Records
  - DNS-based Approaches
  - Analysis of Spam
  - Analysis of Log Files
  - Honeypots
  - Evaluation of AV Feedback
- **Active Techniques**
  - Sinkholing
  - Infiltration
  - DNS Cache Snooping
  - Tracking of Fast-Flux Networks
  - IRC-based detection & monitoring
  - Enumeration of Peer-to-Peer Networks
- **Other Techniques**
  - Reverse Engineering
  - C&C forensics & abuse desks

Approaches to detection & measurement of botnets
Example method: Sinkholing

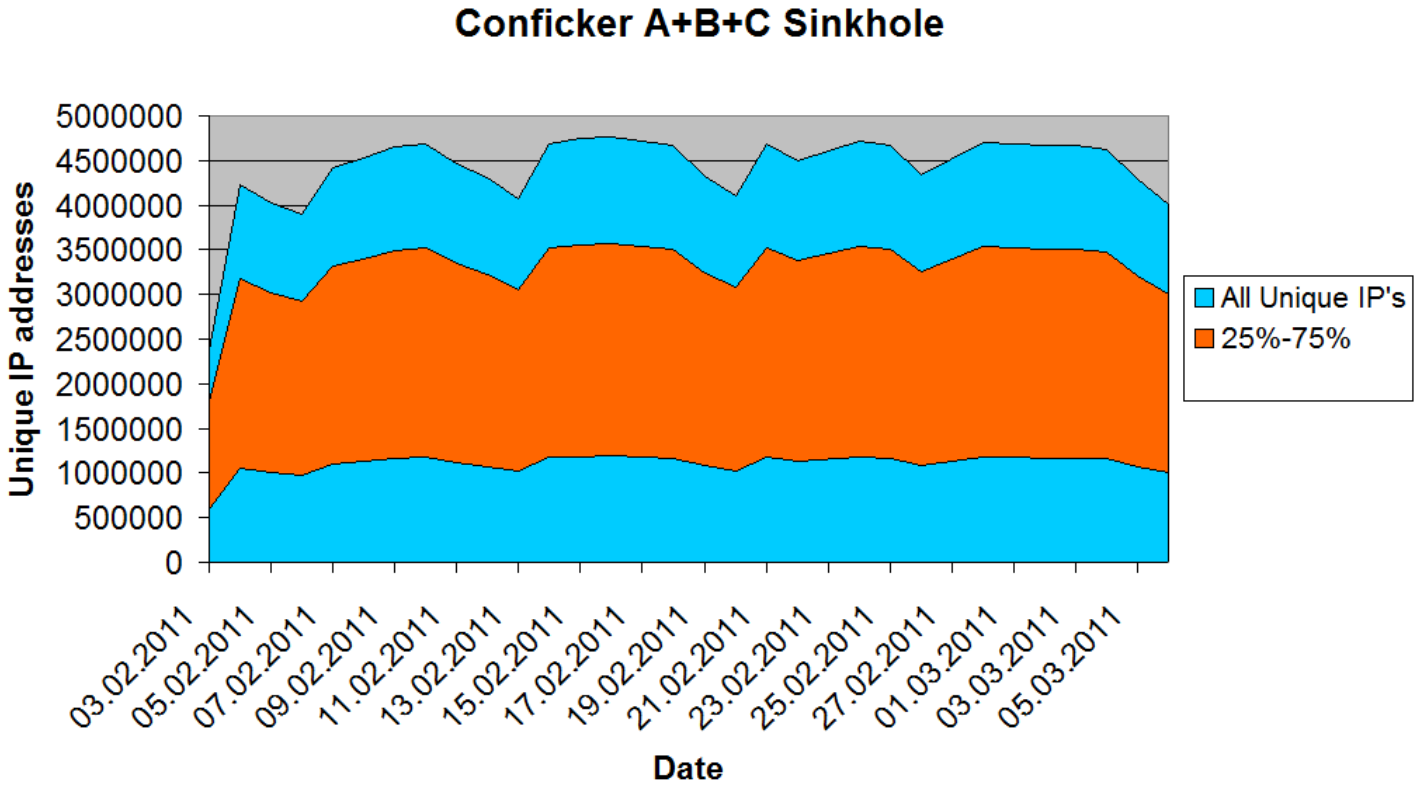
- **Conficker Sinkhole: “Population Data”**
  - „Many people equate one IP to one system, but that is not usually the case.“ (impact: NAT, mobile devices, dial-up, …)
  - „The daily numbers should represent the potential maximum level of the infection, but in previous test cases usually prove to be much less than that maximum. So, take the range of 25% to 75% of the values that we display as the possible infection population and you will be close to the real value. And yes, this is a very large range, and you can see why we do not like to quote any numbers for infection populations, and why you will see very high and low numbers get quoted regularly depending on the purpose of the person making the quote.“

[Conficker Working Group Website: Section on infection tracking
http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking]

Approaches to detection & measurement of botnets

Example method: Sinkholing

- **Daily Conficker Sinkhole Data with 25-75% region marked**



[Conficker Working Group Website: Section on infection tracking
http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking]

Approaches to detection & measurement of botnets

Example method: Sinkholing

- **Case study: Torpig botnet takeover**
  - Botcount via unique identifer: 182.200 bots
  - Botcount via unique IP address (10days): 1.247.642 bots

~ x6.85

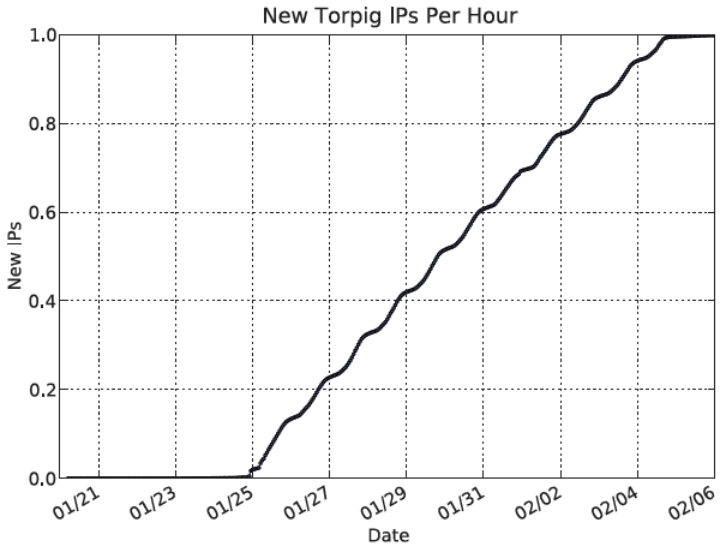


Figure 7: CDF – New unique IP addresses per hour.

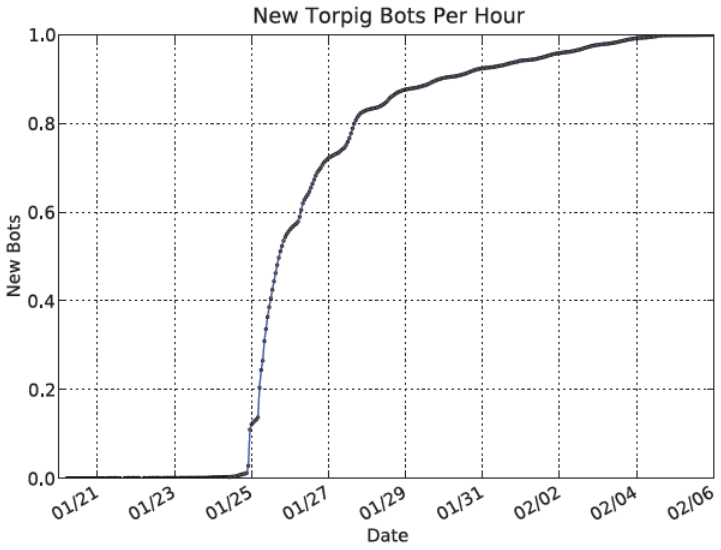


Figure 8: CDF – New bots per hour.

[„Your Botnet is my Botnet: Analysis of a Botnet Takeover“, Stone-Gross et al., 2009]

Approaches to detection & measurement of botnets
Common Characteristics

- **Most approaches aim at assessing the size of (single) botnets**
  - Typical identifier used: IP address
  - Rarely other identifiers available
  - Size seems a natural metric when thinking of threat level

Approaches to detection & measurement of botnets
Conclusion

- **Size is not everything**
  - Accurate threat characterisation far more complex than just numbers of compromised machines
  - Botnet size is rather a scaling factor
  - Functionality, activity, aggression have to be taken into concern
- **Interpret threat level in relation to impact on affected stakeholder**
  - Examples:
    - E-Commerce companies mainly interested in DDoS capabilities
    - Governments focus on risk of information theft (classified data)
    - …

Approaches to

BOTNET COUNTERMEASURES

Approaches to botnet countermeasures
Identified methods and their targets

- **Technical Countermeasures**
  - Blacklisting
  - Distribution of Fake & Traceable Credentials
  - BGP Blackholing
  - DNS-based methods
  - Takedown of C&C Servers
  - Packet Filtering / Port 25 Handling
  - Walled Gardens
  - P2P Countermeasures
  - Remote Disinfection
- **Social Countermeasures**
  - Dedicated Laws on Cybercrime
  - User Awareness raising and Special Training
  - Central Incident Helpdesks
  - Enhance Cooperation between Stakeholders

Approaches to botnet countermeasures
Current practices and challenges

- **Takedown of C&C Servers**
  - Abuse request to hosting provider: disconnect / power off server
  - Challenge: non-cooperative (bulletproof) hosting
- **Handling of C&C domains**
  - Abuse request to registrar in charge: deregistration
  - Register unused C&C domains in advance
- **De-Peering of rogue ISPs**
  - Benign ISP‘s decision cooperation needed to stop services
  - Court: Restraining order (e.g. FTC vs. 3FN / Pricewert)

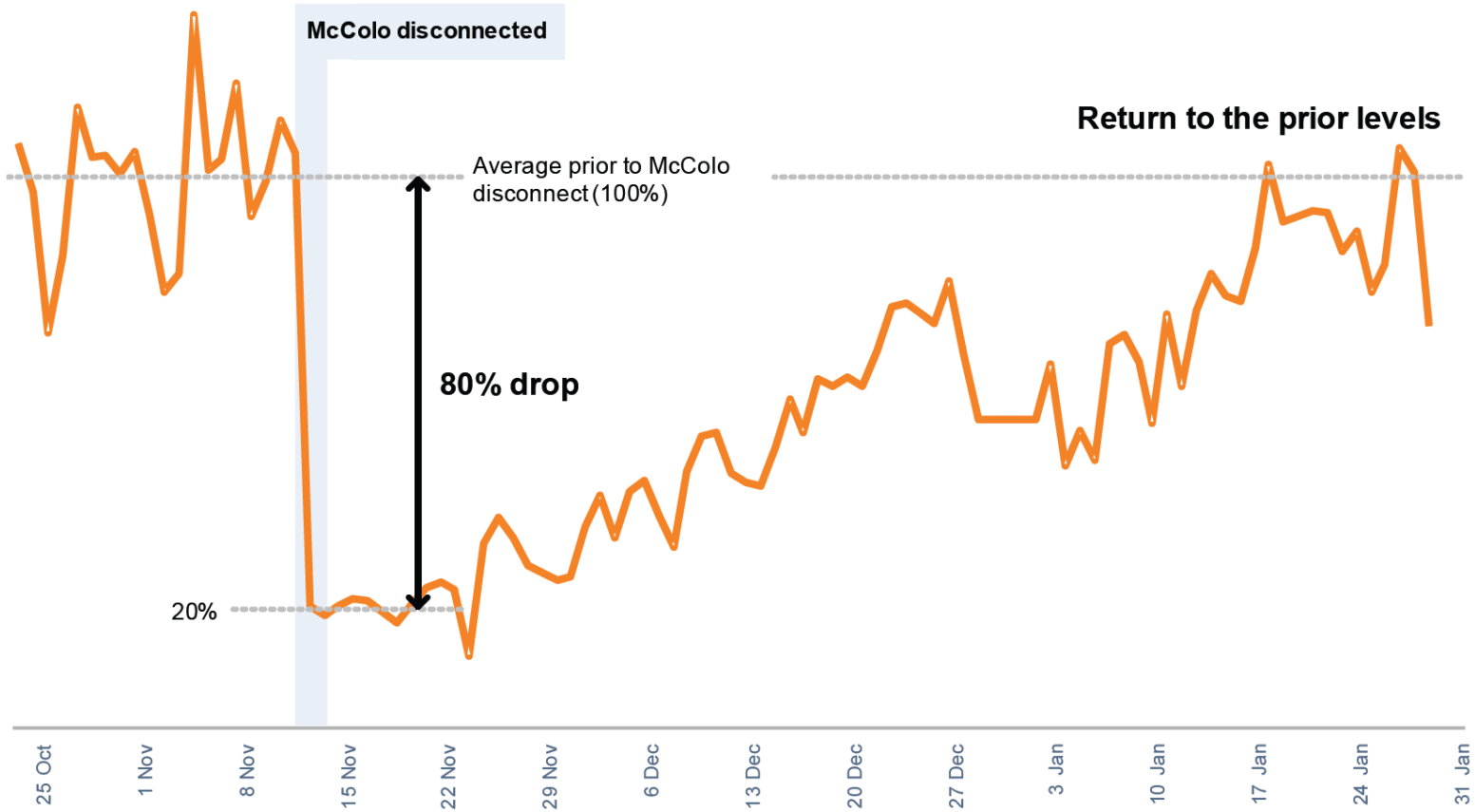
Approaches to botnet countermeasures
Current practices and challenges

- **Actions against botnet C&C infrastructure do not affect infections**
  - Systems remain instable and vulnerable
  - Many computers infected with multiple malware
  - Pay-per-install and update features can be used to extend botnet population
- **Incomplete takedowns may raise botnet resilience**
  - Infrastructure may be migrated after regaining control
  - „Teaching“ botmasters to update and enhance

Approaches to botnet countermeasures

Example: De-Peering

- **McColo shutdown Nov 2008**



[MessageLabs Intelligence: 2009 Annual Security Report. Symantec Hosted Services, 2009]

Fraunhofer FKIE

Approaches to botnet countermeasures
Missing pieces

- **Victim-side / social aspects**
  - Not explored enough
  - First steps in this direction visible
    - Germany: Anti-Botnet Initiative / HelpDesk
    - Netherlands: Covenant against botnets
    - Australia: Australian Internet Security Initiative
    - Japan: Cyber Clean Center
    - South Korea: Centralised mitigation efforts, E-Call Center

Approaches to botnet countermeasures
Conclusion

- **Complement approaches**
  - Continue good efforts against botnet infrastructure
  - Include victims stronger in fight against botnets
  - Notification services and Help-Desks are a promising approach
- **Enhance cooperation between stakeholders**
  - Coordinate activities: taskforces
  - Exchange gathered data and knowledge
  - Challenge: efficient information sharing

Question of

ROLES IN THE FIGHT AGAINST BOTNETS

Question of Roles
Legal Aspects

- **General aspects when fighting against (cyber-)crime**
  - Criminals do not respect law -> flexibility
  - Cybercrime is a global problem
- **Reflection in botnet countermeasures**
  - Countermeasures have to be performed within legal frameworks
  - Existing legal frameworks partially originate from old „telecommunication“ regulations
  - Legal situation differs on national level
- **Consequences**
  - Compliant approaches have limited impact
  - Technically possible and promising approaches are not justifiable under given law (and in regard of ethical responsibility)
  - We need these laws (data protection, privacy, …) -> find a good balance

Question of Roles
Relevant Stakeholders

- **Law enforcement**
  - Legally empowered to investigate and perform countermeasures
- **Governments**
  - Create incentives and regulate on actions against botnets
- **Internet Service Providers**
  - Central position because forwarding botnet traffic
- **Affected users and companies**
  - Physically possess infected machines
- **Researchers**
  - Provide intelligence and concepts against botnets

Coming up:
Recommendations and Best Practices

Questions?