Computer Networks

COSC 6377

Lecture 18

Fall 2011

October 26, 2011

Announcements

- Start working on HW3 and P2
- P2 discussions next class
- Exam 2 in one week
- Volunteer for HW3 and P2

Security

- Securing Infrastructure
  - Performance
  - Basic availability
- End-user information
  - Privacy
  - Confidentiality
  - Integrity

Denial of Service

- Automated
  - Send lot of requests from a single host
  - Distributed DOS using Botnets
- Manual
  - Slashdotting
  - Popular content

Solutions

- Overprovisioning
- Limit ingress
  - Firewalls
- Limit egress
  - Identify and cut
- Main Challenges
  - Identification of “good” and “bad”
  - Identification of source

Making of a Worm

- Identifying vulnerable hosts
- Downloading code
- Perform malicious tasks
  - Copy files
  - Hijack and spoof programs and steal information
- Repeat
- Profit

Botnets

- Unwilling participants
- Bandwidth
  - DDOS
  - Spam emails
- Users
  - Stealing information

Botnets Ecosystem

- Recruiting computers “Zombies”
- Aggregators and Sellers

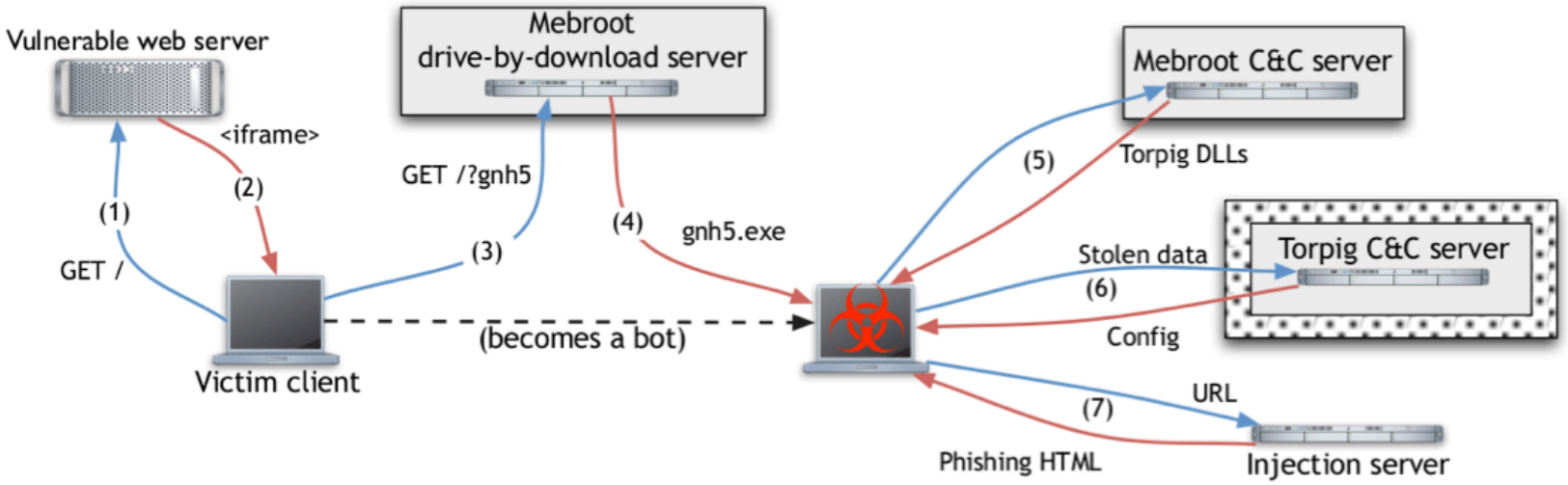
- Buyers that run specific apps on Botnets
  - Spam
  - Steal information

Studying Botnets

- Passive techniques
  - Observe the effects of malware
- Active techniques
  - Capture malware
- Hijacking

Command and Control

- Set of machines that orchestrate infection and malicious activities
- Desirable
  - Maintain control
  - Hard to detect



[Brett-Stone 09]

Domain Flux

- Use DNS to locate command and control node
- Each bot algorithmically generates domain names to lookup
- The transient domains point to C & C hosts

- Why use Domain Flux?

Hijacking Torpig

- Predict future domains
- Register those domains
- When bots contact, send valid replies

Hijacking Challenges

- Large number of domains
- Small effort required to increase the number of domains significantly

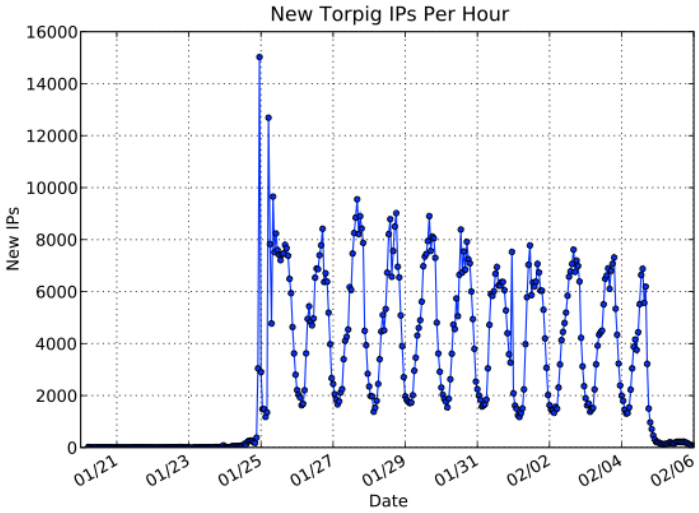


Figure 5: New unique IP addresses per hour.

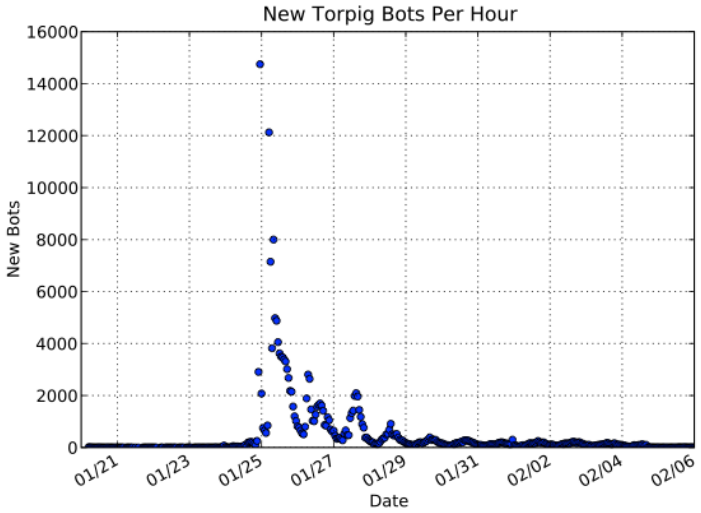


Figure 6: New bots per hour.

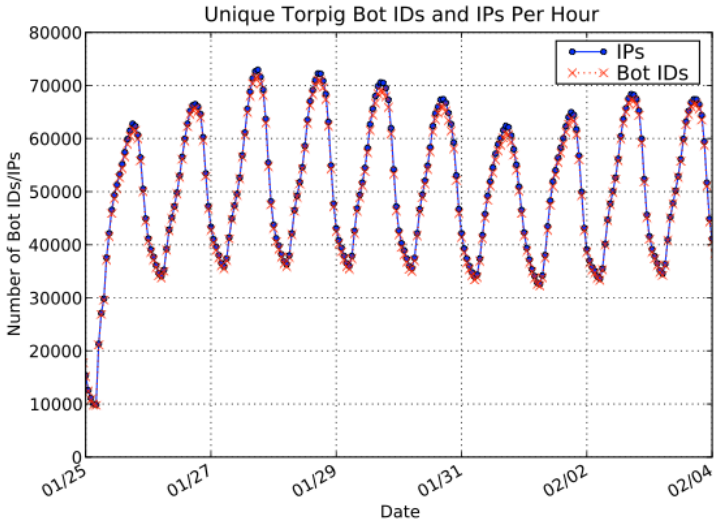


Figure 9: Unique Bot IDs and IP addresses per hour.

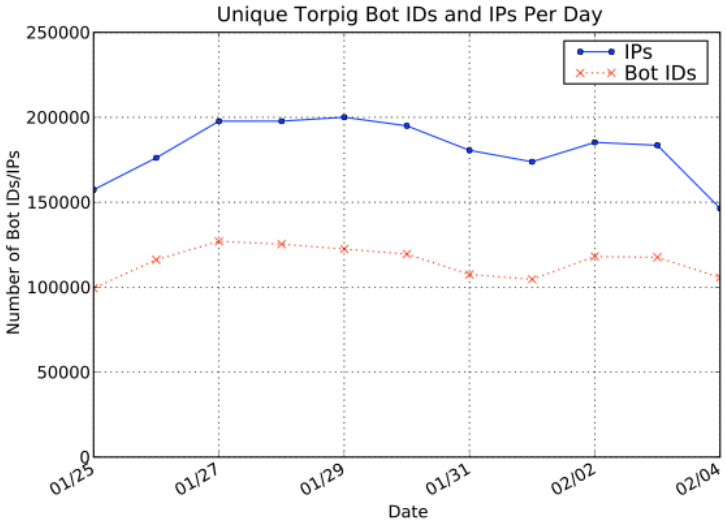


Figure 10: Unique Bot IDs and IP addresses per day.