Botnets

CS 598: Advanced Internet

Presented by: Imranul Hoque

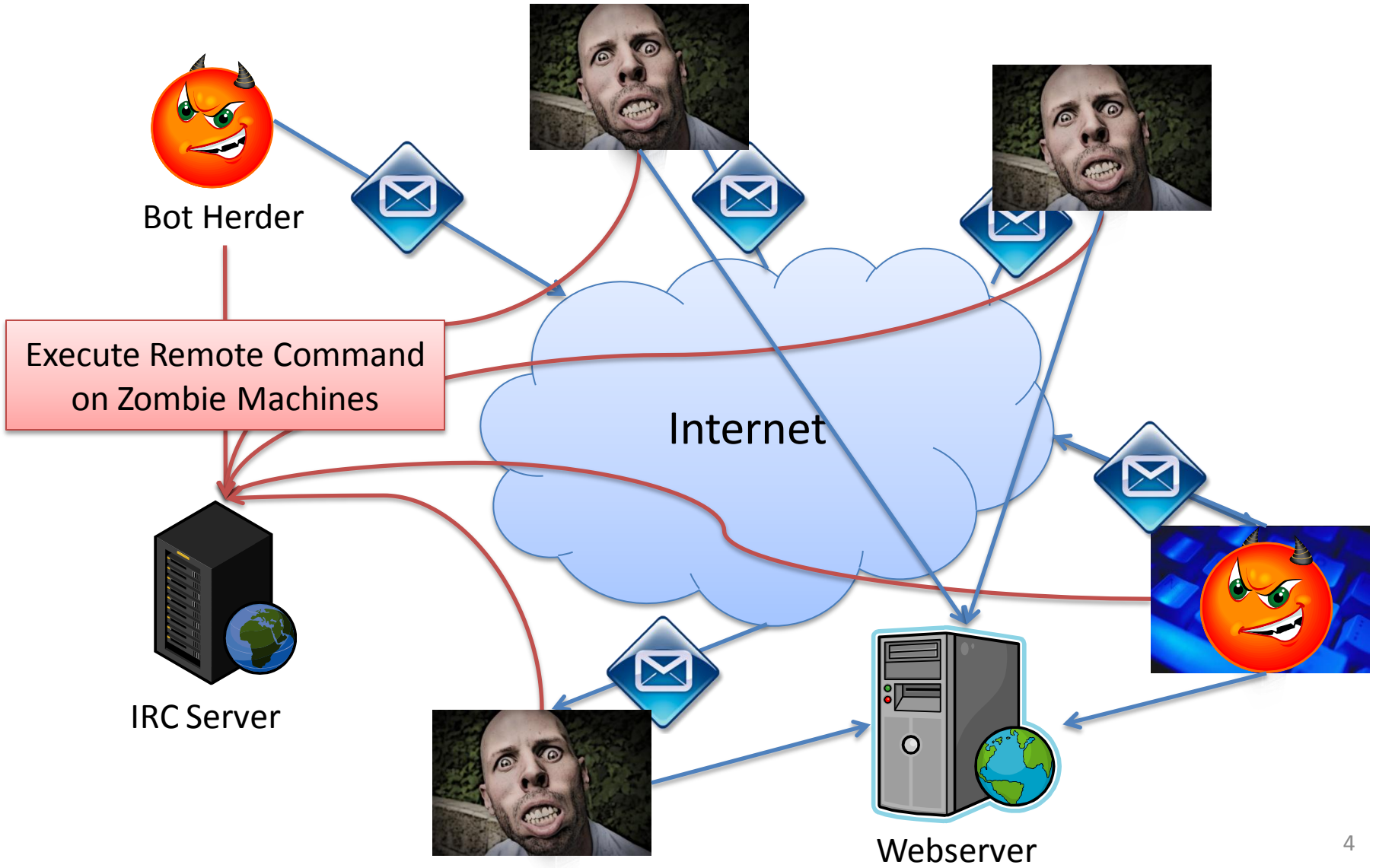
How to Study Botnets?

- Passive analysis
  - Study spam e-mail, DNS queries by bot-infected machines, DNS blacklists, analyze network traffic, etc.
- Infiltration
  - Today's paper (Spamcraft)
- Hijack!
  - Collaboration with domain registrars, future prediction in case of domain flux
  - UCSB researchers hijack Torpig for 10 days!

This Talk

- Centralized botnet
  - Agobot
- P2P botnet
  - Storm
- Interesting facts
  - Death of Srizbi
  - Twitter-based Botnet Command Channel

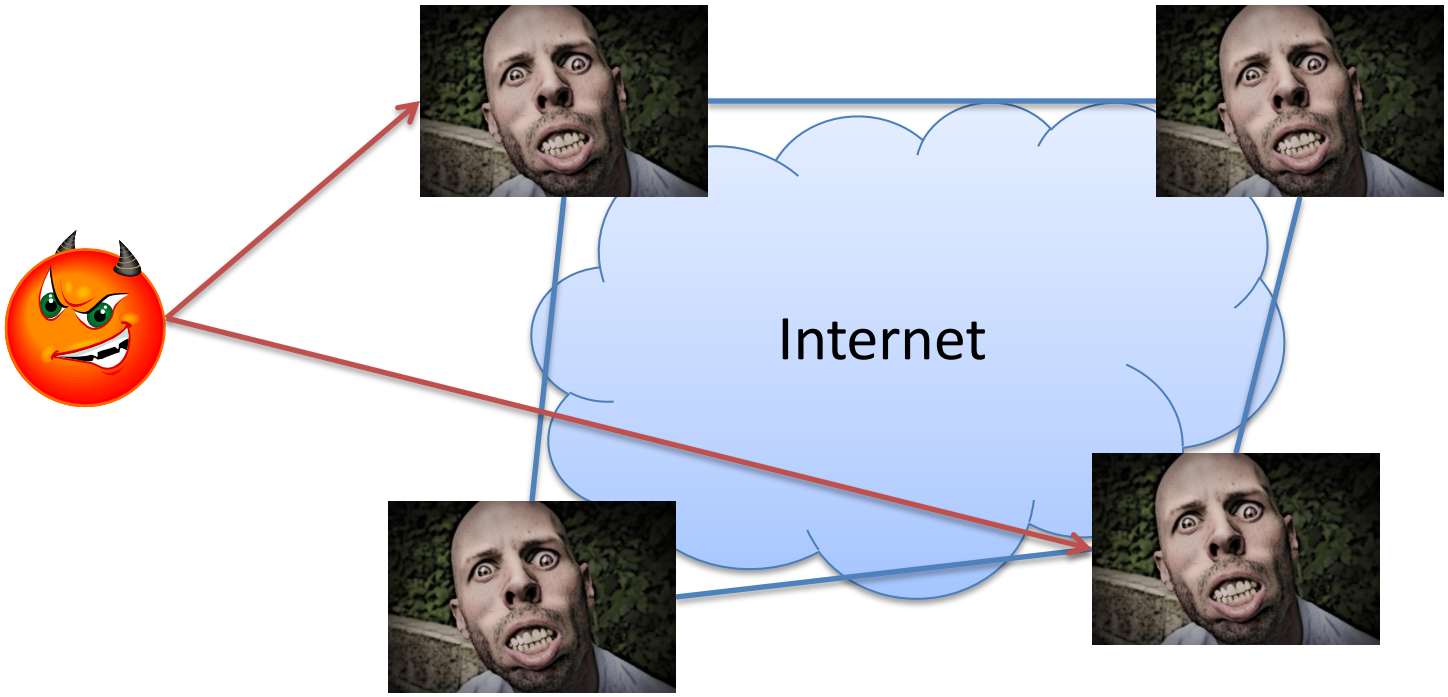
Botnet: The Old Way



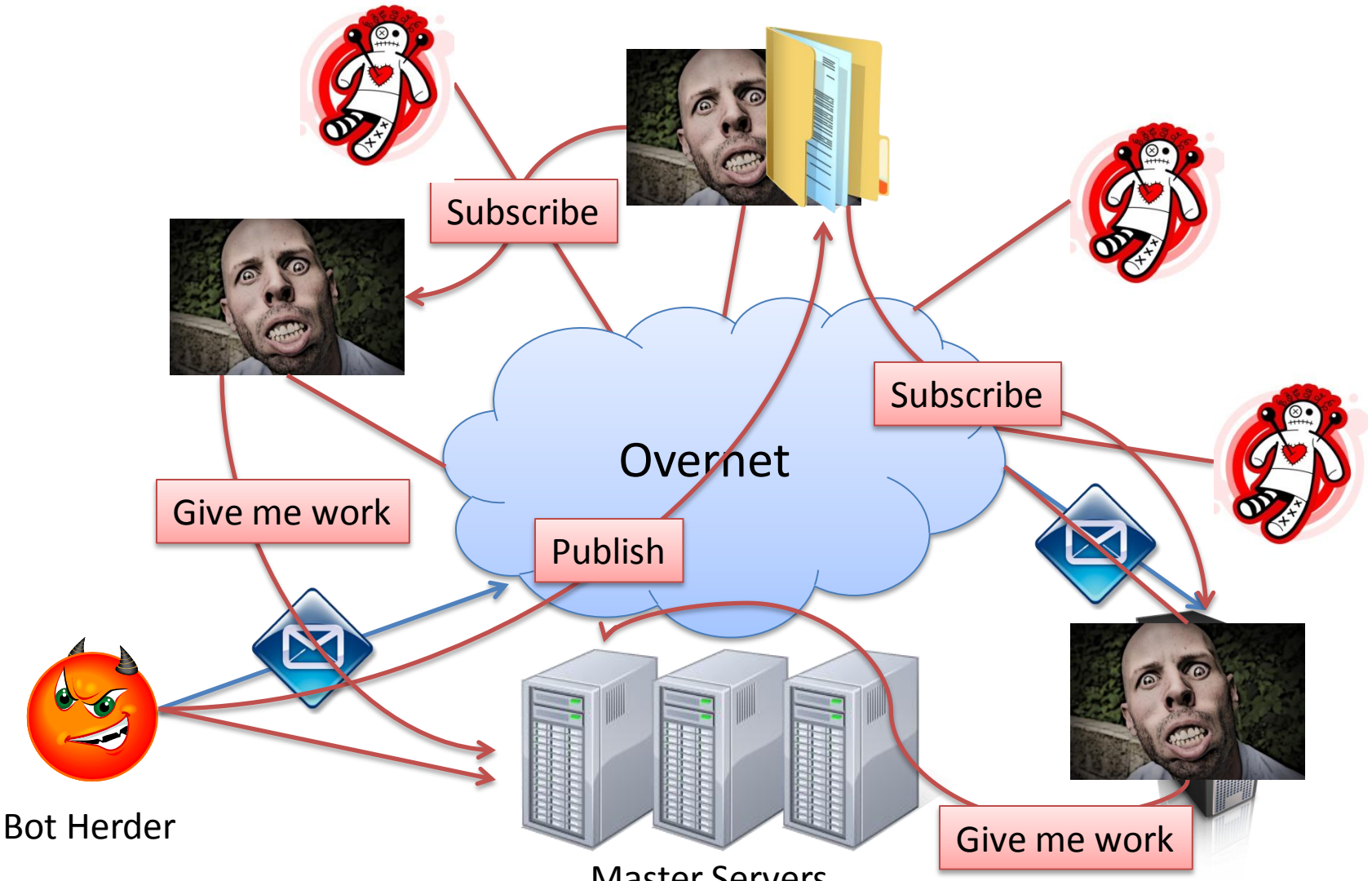
Example: Agobot

- Public source code release: 2002
- IRC based command and control
- DoS attack library
- Limited polymorphic obfuscations
- Harvests PayPal passwords, AOL keys, etc.
- Defends compromised systems
  - Killing anti-virus, testing for VMWare, altering anti-virus DNS entry
- Anti-disassembly mechanisms
  - Testing for debugger presence

Today's Botnet



Example: Storm

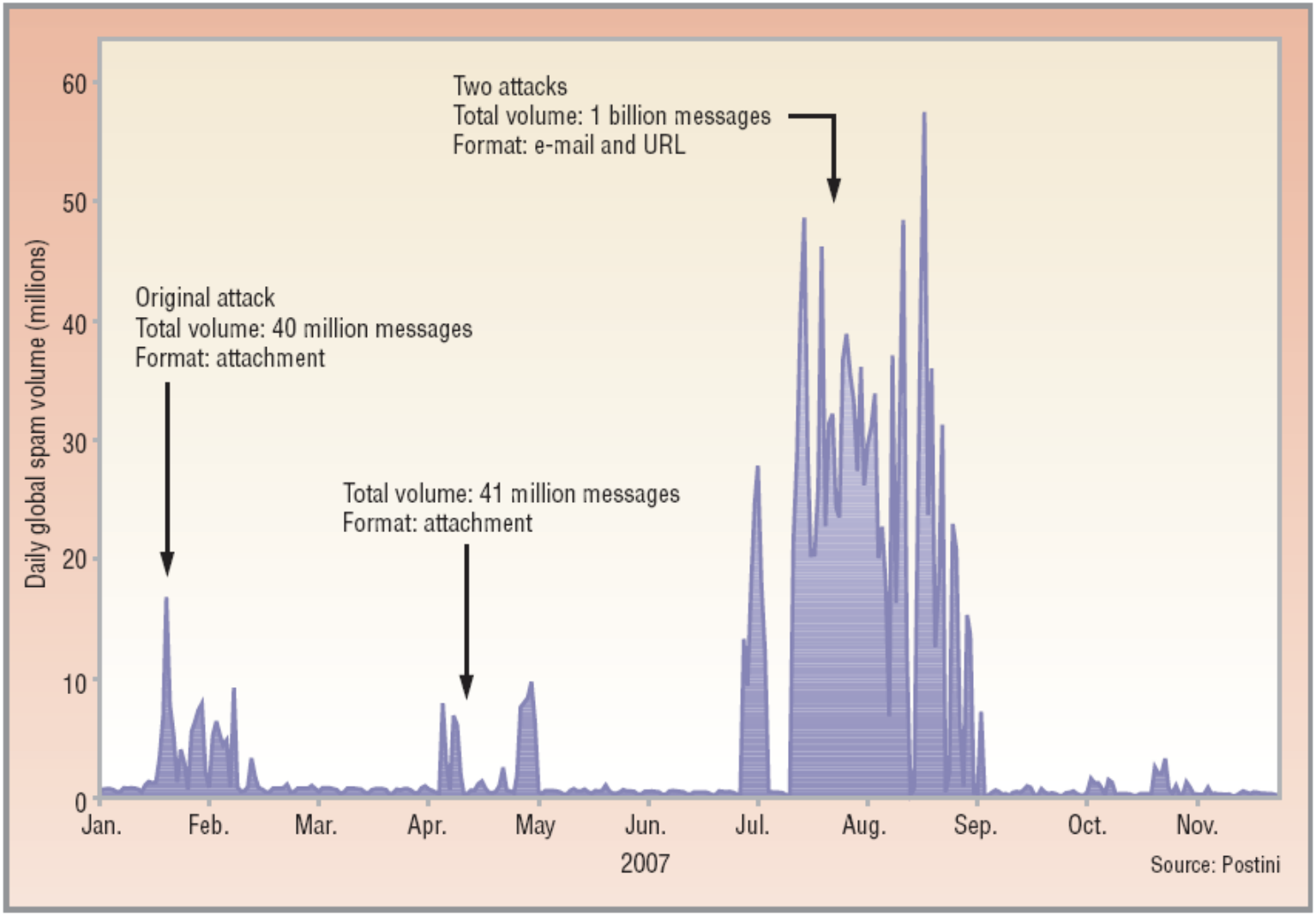


Storm: Features

- Appeared in 2006, gained prominence in Jan 2007
- First major botnet to employ P2P command and control architecture
- Recruits new bots using a variety of attack vectors
  - Email messages with exe
  - Email messages with link to infected sites
  - E-card spam
- User computing power of compromised machines
  - Sends and relays SPAM
  - Hosts the exploits and binaries
  - Conducts DDoS attacks
- First to spam with embedded mp3 (non-malicious)
- Provision for partial rental

Slide from: CS463

Effectiveness of Storm



Anti-malware Response

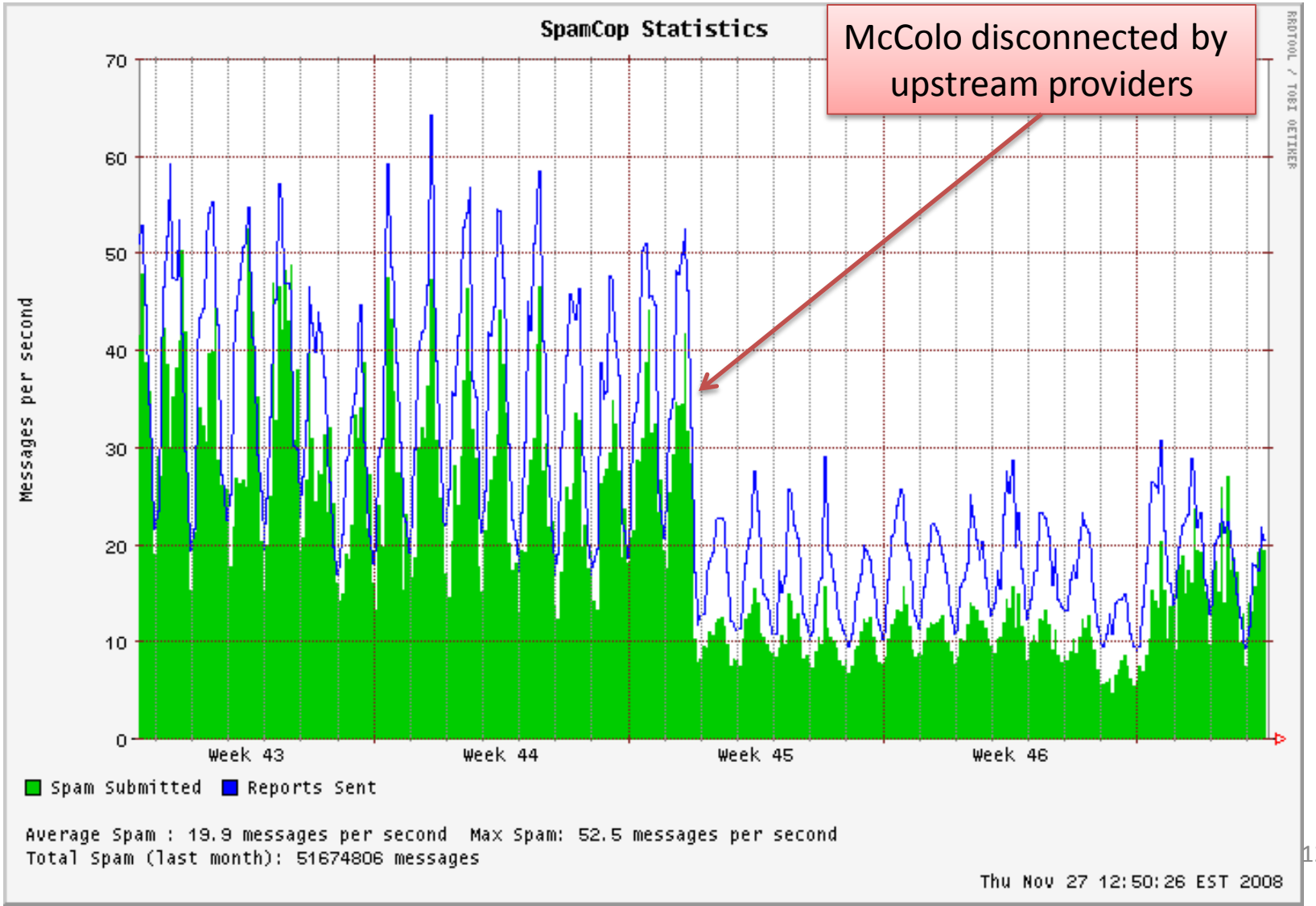
- Botnet variations make signature-based detection difficult
  - New email subject lines and file attachment names
  - Re-encoded malware binary twice per hour
- Anti-malware Response
  - Microsoft Malicious Software Removal Tool patch issued in September 2007
    - Correlated with 20% drop in size of the Storm Worm botnet
    - Shows that aggressive removal of bots from botnet can make a significant impact on the size of the botnet

Slide from: CS463

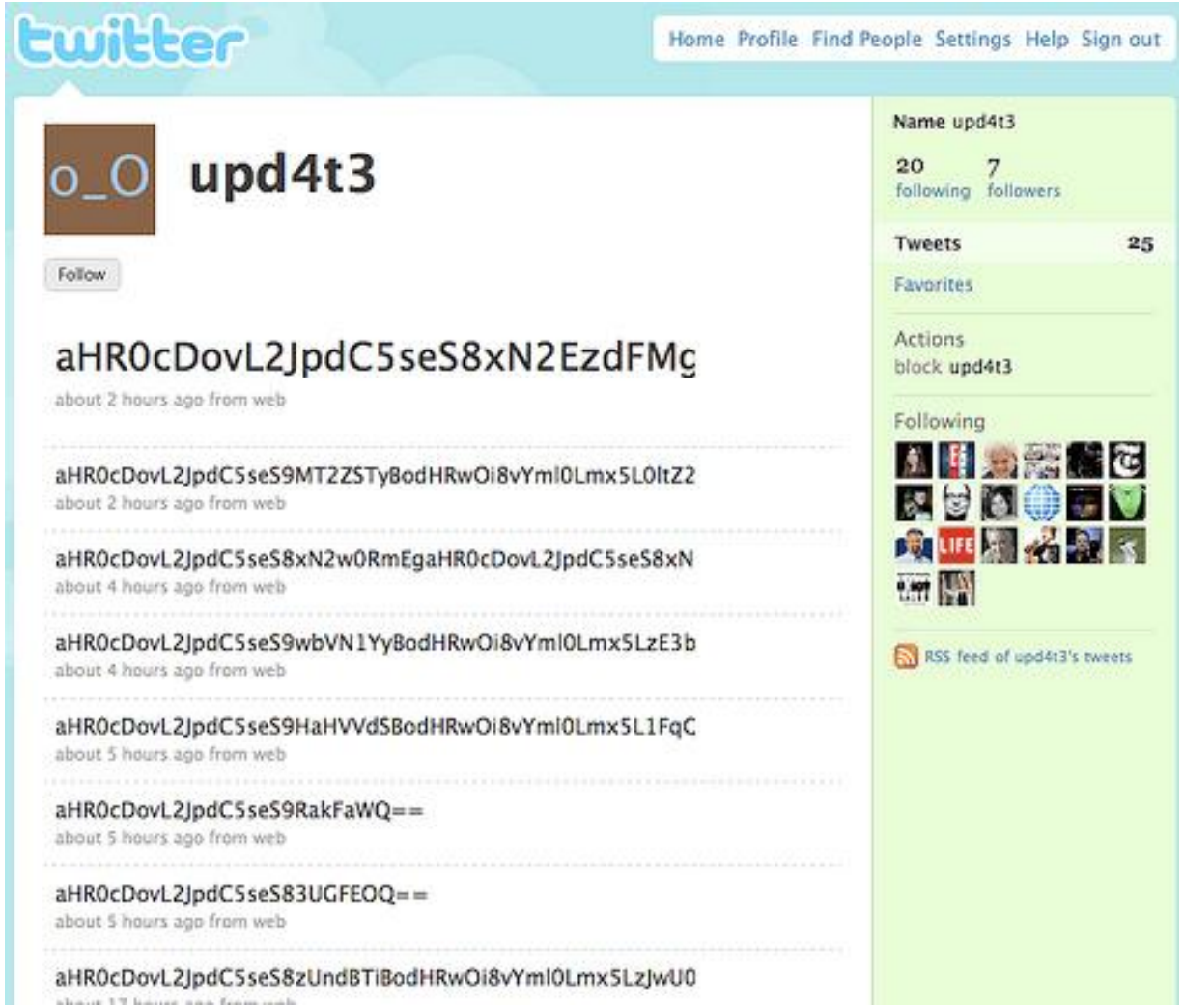
Spamcraft

- Objective
  - Analyze spam templates and e-mail target list
  - Analyze how harvested e-mails are used
- Methodology
  - Request workload from proxy bot
  - Insert marker e-mails in worker harvest and report
- Important results
  - Frightening scale
  - Web based harvesting << bot-based harvesting

Srizbi


SpamCop Statistics
McColo disconnected by upstream providers
Messages per second
70
60
50
40
30
20
10
0
Week 43
Week 44
Week 45
Week 46
Spam Submitted
Reports Sent
Average Spam : 19.9 messages per second Max Spam: 52.5 messages per second
Total Spam (last month): 51674806 messages
Thu Nov 27 12:50:26 EST 2008

Twitter


twitter
Home Profile Find People Settings Help Sign out
o_O
upd4t3
Follow
aHR0cDovL2JpdC5seS8xN2EzdFMg
about 2 hours ago from web
aHR0cDovL2JpdC5seS9MT2ZSTyBodHRwOi8vYml0Lmx5L0ltZ2
about 2 hours ago from web
aHR0cDovL2JpdC5seS8xN2w0RmEgaHR0cDovL2JpdC5seS8xN
about 4 hours ago from web
aHR0cDovL2JpdC5seS9wbVN1YyBodHRwOi8vYml0Lmx5LzE3b
about 4 hours ago from web
aHR0cDovL2JpdC5seS9HaHVVdSBodHRwOi8vYml0Lmx5L1FqC
about 5 hours ago from web
aHR0cDovL2JpdC5seS9RakFaWQ==
about 5 hours ago from web
aHR0cDovL2JpdC5seS83UGFEOQ==
about 5 hours ago from web
aHR0cDovL2JpdC5seS8zUndBTiBodHRwOi8vYml0Lmx5LzJwU0
Name upd4t3
20 following
7 followers
Tweets 25
Favorites
Actions
block upd4t3
Following
RSS feed of upd4t3's tweets

Related Materials

- A Storm (Worm) Is Brewing. Brad Smith. IEEE Computer, vol. 41, no. 2, pp. 20-22, Feb. 2008.
- Spamalytics: An Empirical Analysis of Spam Marketing Conversion. C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. Voelker, V. Paxson, and S. Savage. Proceedings of the 15th ACM Conference on Computer and Communications Security (ACM CCS), Alexandria, Virginia, pp. 3-14.
- On the Spam Campaign Trail. Kreibich, C., Kanich, C., Levchenko, K., Enright, B., Voelker, G. M., Paxson, V., and Savage, S. 2008. *Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats*, San Francisco, California.
- Measurements and Mitigation of Peer-to-Peer-based Botnets: A Case Study on Storm Worm. Holz, T., Steiner, M., Dahl, F., Biersack, E., and Freiling, F. *Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats*, San Francisco, California.
- An Inside Look at Botnets. Paul Barford and Vinod Yegneswaran. Advances in Computer Security, Springer 2007.
- Your Botnet is My Botnet: Analysis of a Botnet Takeover. Brett Stone-Gross, Marco Cova, Lorenzo Cavallaro, Bob Gilbert, Martin Szydlowski, Richard Kemmerer, Christopher Kruegel, and Giovanni Vigna. Proceedings of CCS 2009, Chicago, Illinois.

Discussion

- How would you design tomorrow's botnet?
- Preventive measures against tomorrow's botnet?
- A botnet in the clouds?