Botnets

Why to talk about Botnets…

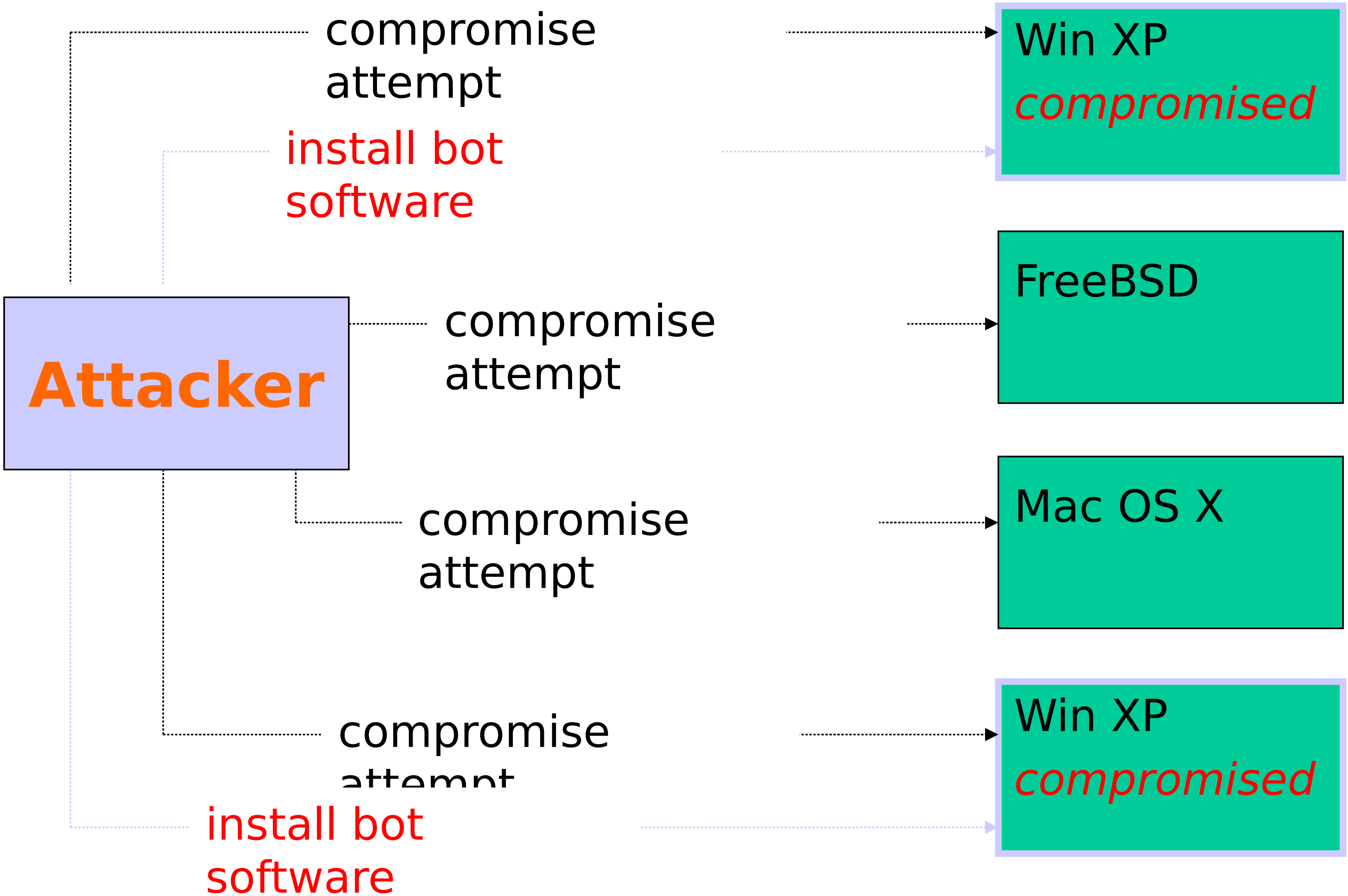
- Botnet could be a most powerful supercomputer in the world
- Recent attack on countries, e.g., Estonia
- Vehicle for cyber-terrorism and cyber crime
- Very serious security threat that could stop your national IT infrastructure

=> so we do need to understand botnet

Botnets

- Botnet = network of autonomous programs capable of acting on instructions
  - Typically a large (up to several hundred thousand) group of remotely controlled “zombie” systems
  - Machine owners are not aware they have been compromised
  - Controlled and upgraded via IRC/P2P/HTTP/...
- Used as the platform for various attacks
  - Distributed denial of service
  - Spam and click fraud
  - Launching pad for new exploits/worms

Building a Botnet



compromise attempt

Win XP *compromised*

install bot software

FreeBSD

Attacker

compromise attempt

compromise attempt

Mac OS X

compromise attempt

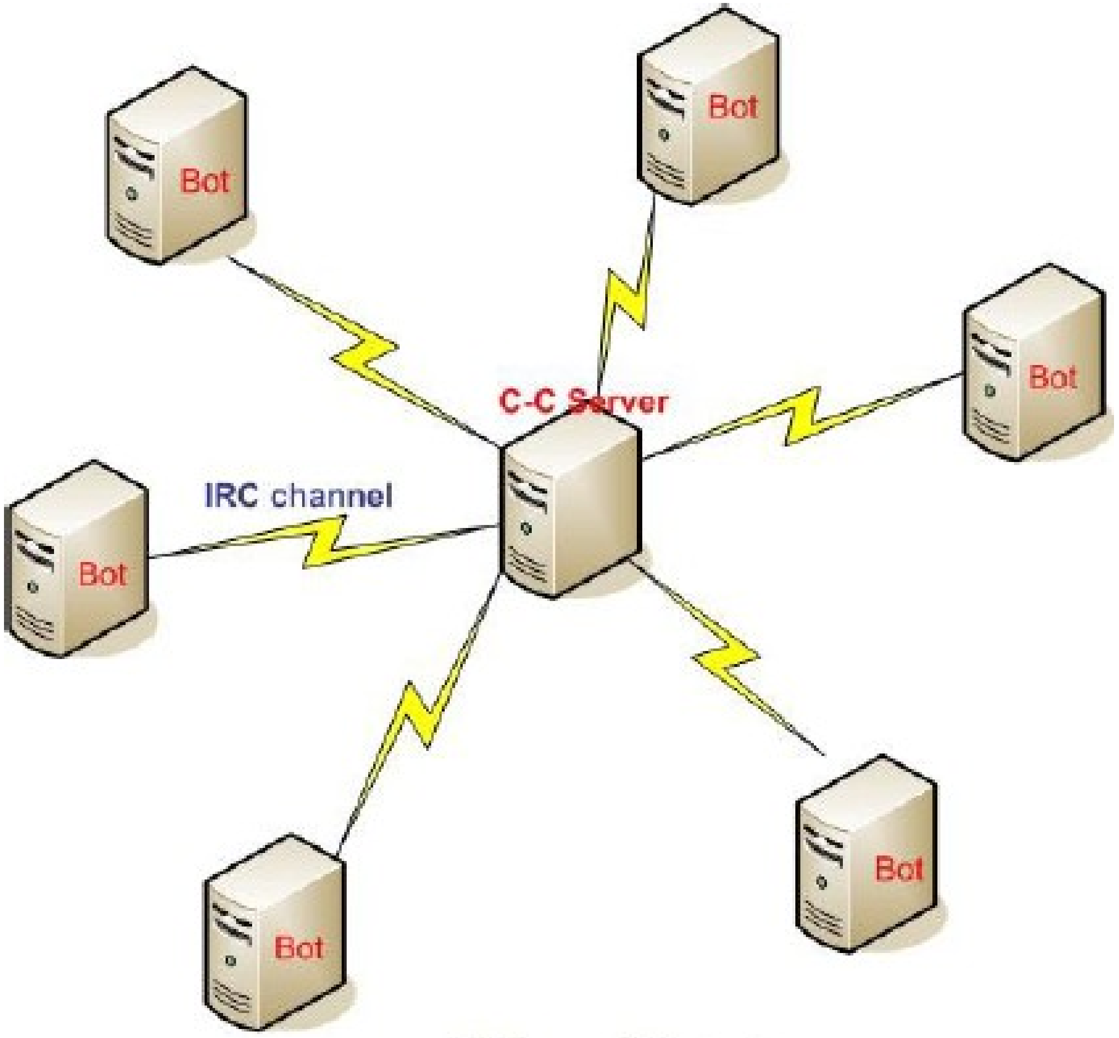
Win XP *compromised*

install bot software

Botnet construction

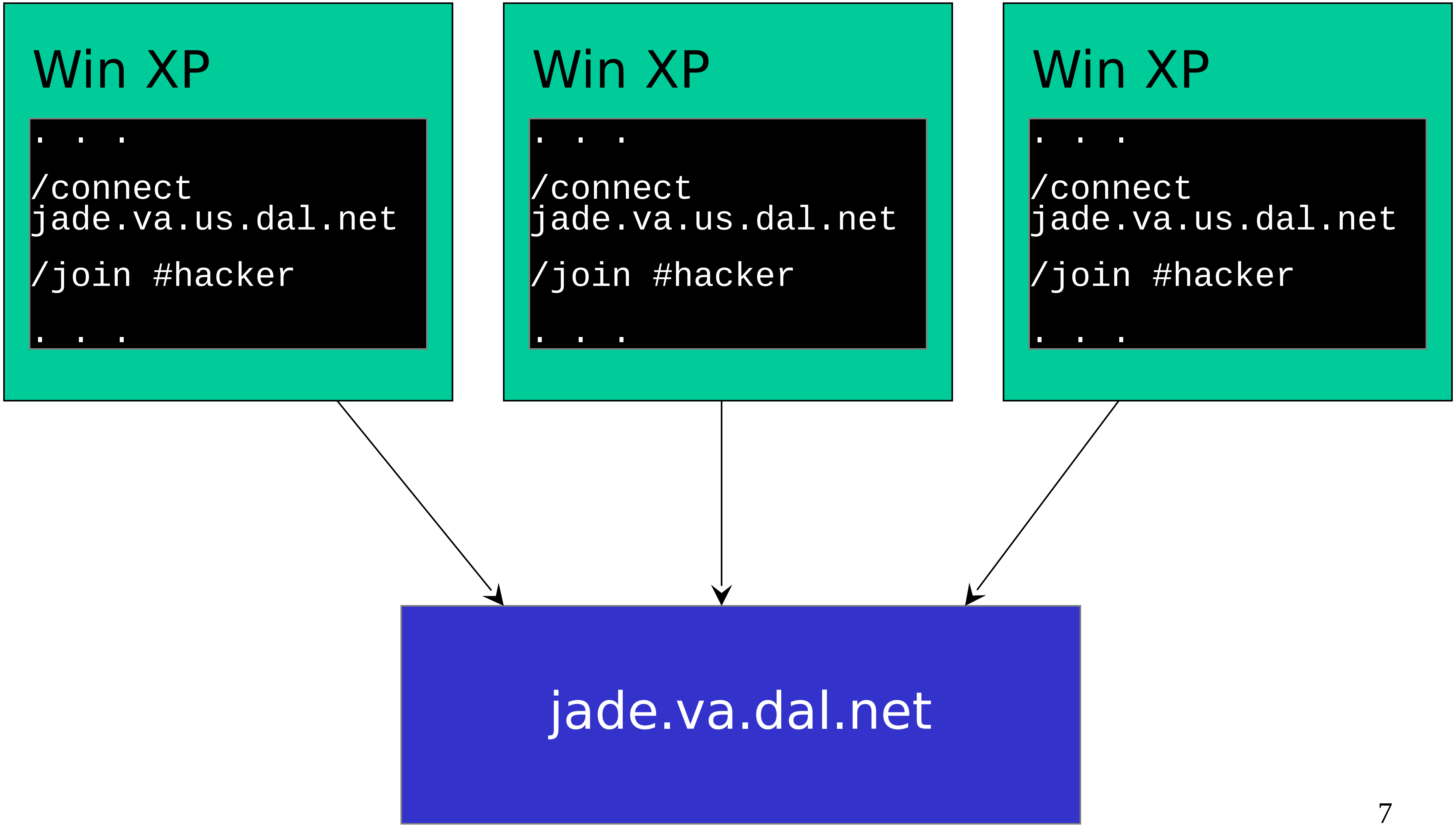
- First stage, exploit vulnerabilities (operating system's/browser's)
  - Next stage to download bot software, C&C instructions
  - Once the bot software is executed and connected to C&C server
- Bots connect to channel of C&C (IRC or HTTP) password protected channel
- Encryption layer between bot and C&C

IRC Botnet



IRC based Botnets

Joining the IRC Channel



Win XP

```
. . .
/connect
jade.va.us.dal.net
/join #hacker
. . .
```

Win XP

```
. . .
/connect
jade.va.us.dal.net
/join #hacker
. . .
```

Win XP

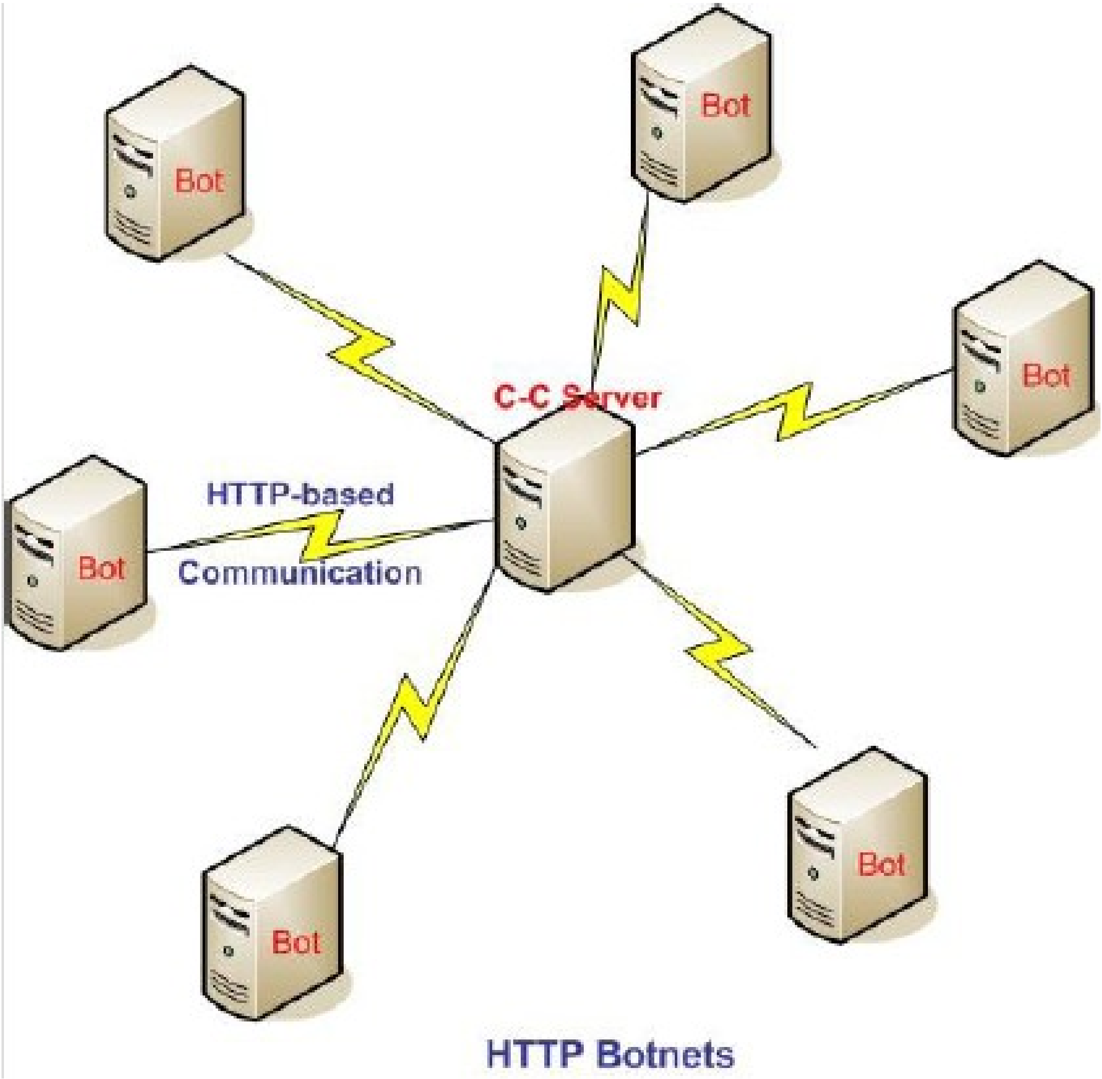
```
. . .
/connect
jade.va.us.dal.net
/join #hacker
. . .
```

jade.va.dal.net

Command and Control

```
(12:59:27pm) -- A9-pcgbdv (A9-pcgbdv@140.134.36.124)
has joined (#owned) Users : 1646

(12:59:27pm) (@Attacker) .ddos.synflood 216.209.82.62

(12:59:27pm) -- A6-bpxufrd
(A6-bpxufrd@wp95-81.introweb.nl) has joined (#owned)
Users : 1647

(12:59:27pm) -- A9-nzmpah (A9-nzmpah@140.122.200.221)
has left IRC (Connection reset by peer)

(12:59:28pm) (@Attacker) .scan.enable DCOM

(12:59:28pm) -- A9-tzrkeasv (A9-tzrkeas@220.89.66.93)
has joined (#owned) Users : 1650
```

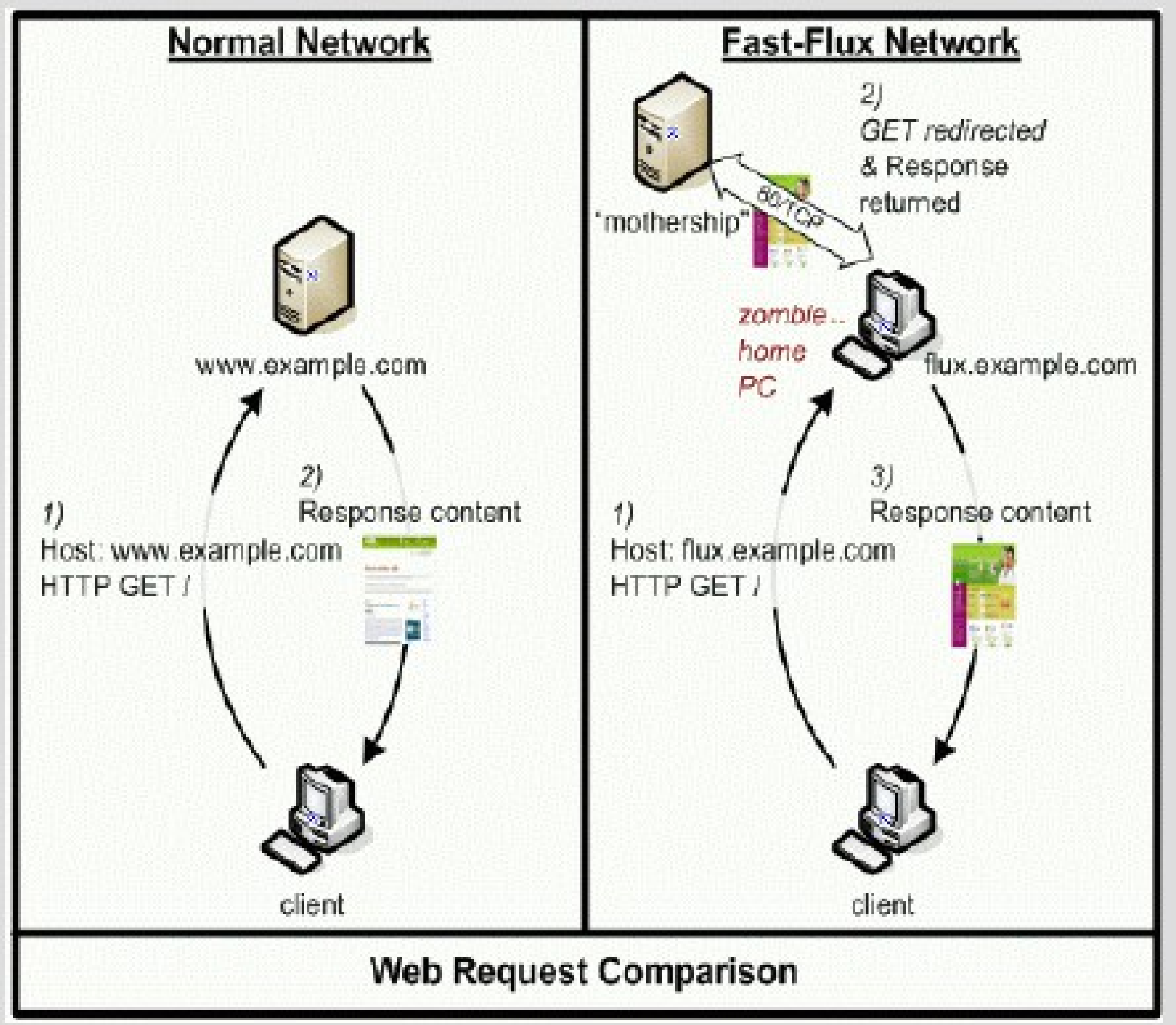
HTTP Botnet


Bot
Bot
C-C Server
Bot
Bot
HTTP-based
Communication
Bot
Bot
HTTP Botnets

Fast-Flux Network

- What if a mothership of Botnet goes offline?
- Fast-Flux service networks
  - A technique in which A and NS records of a domain change rapidly
  - Location (IP) of the domain changes rapidly when resolved
  - Used for load balancing across servers, resource configuration, etc…
  - Botherders effectivly use it to hide mothership

FastFlux network botnet



Source: Honeynet.org

Botnet propagation

[Abu Rajab et al.]

- Each bot can scan IP space for new victims
  - Automatically
    - Each bot contains hard-coded list of IRC servers’ DNS names
    - As infection is spreading, IRC servers and channels that the new bots are looking for are often no longer reachable
  - On-command: Target specific /8 or /16 prefixes
    - Botmasters share information about prefixes to avoid
- Evidence of botnet-on-botnet warfare
  - DoS server by multiple IRC connections (“cloning”)
- Active botnet management

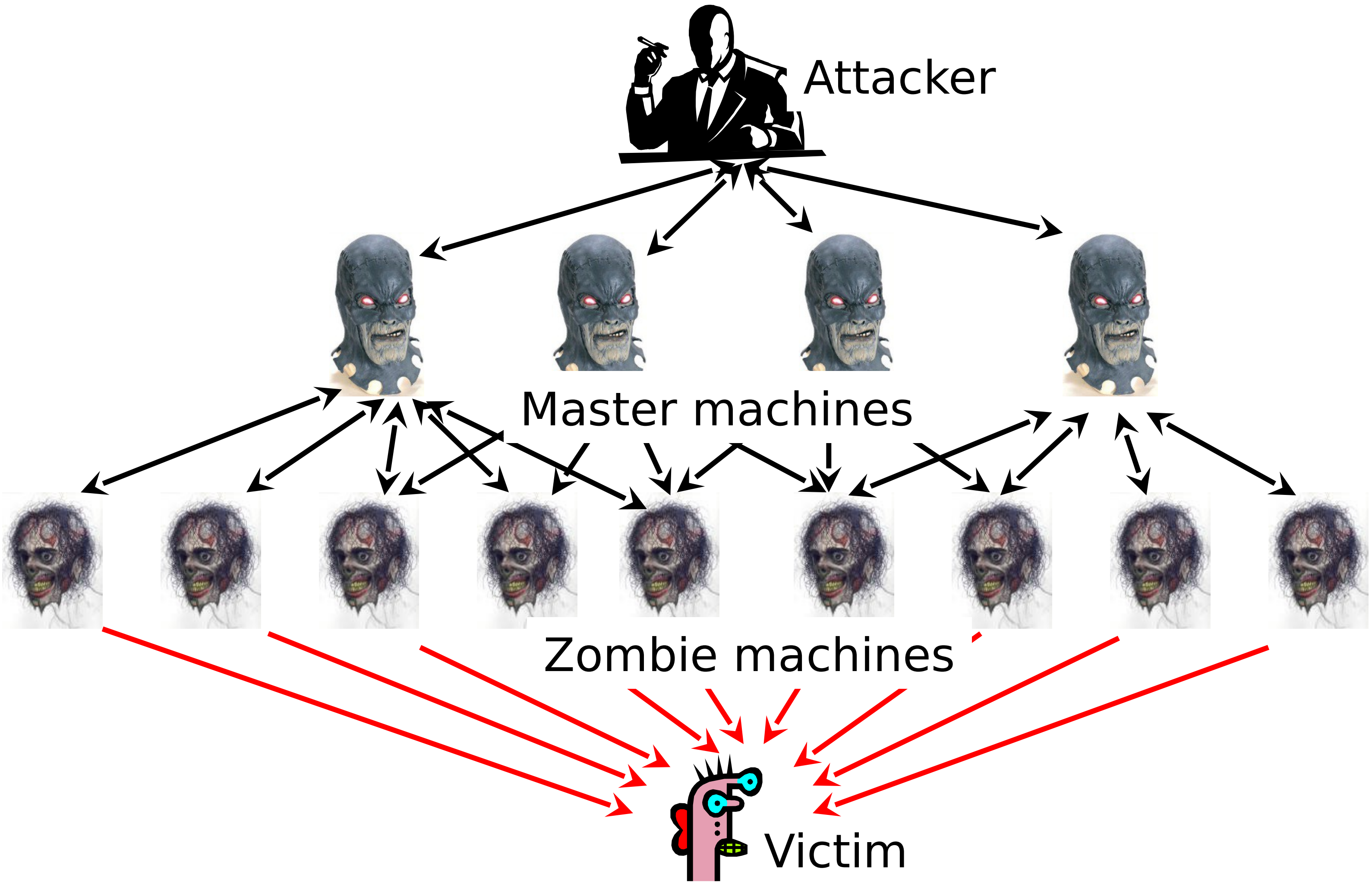
Denial of Service (DoS) Redux

- Goal: Overwhelm victim machine and deny service to its legitimate clients
- DoS often exploits networking protocols
  - Smurf: ICMP echo request to broadcast address with spoofed victim's address as source
  - Ping of death: ICMP packets with payloads greater than 64K crash older versions of Windows
  - SYN flood: "Open TCP connection" request from a spoofed address
  - UDP flood: Exhaust bandwidth by sending thousands of bogus UDP packets

Distributed Denial of Service (DDoS)

- Build a botnet of zombies
  - Multi-layer architecture: Use some of the zombies as “masters” to control other zombies
- Command zombies to stage a coordinated attack on the victim
  - Does not require spoofing (why?)
  - Even in case of SYN flood, SYN cookies don’t help (why?)
- Overwhelm victim with traffic arriving from thousands of different sources

DDoS Architecture



Attacker

Master machines

Zombie machines

Victim

DDoS Tools: Trin00

- Scan for known buffer overflows in Linux & Solaris
  - Unpatched versions of wu-ftpd, statd, amd, …
  - Root shell on compromised host returns confirmation
- Install attack daemon using remote shell access
- Send commands (victim IP, attack parameters), using plaintext passwords for authentication
  - Attacker to master: TCP, master to zombie: UDP
  - To avoid detection, daemon issues warning if

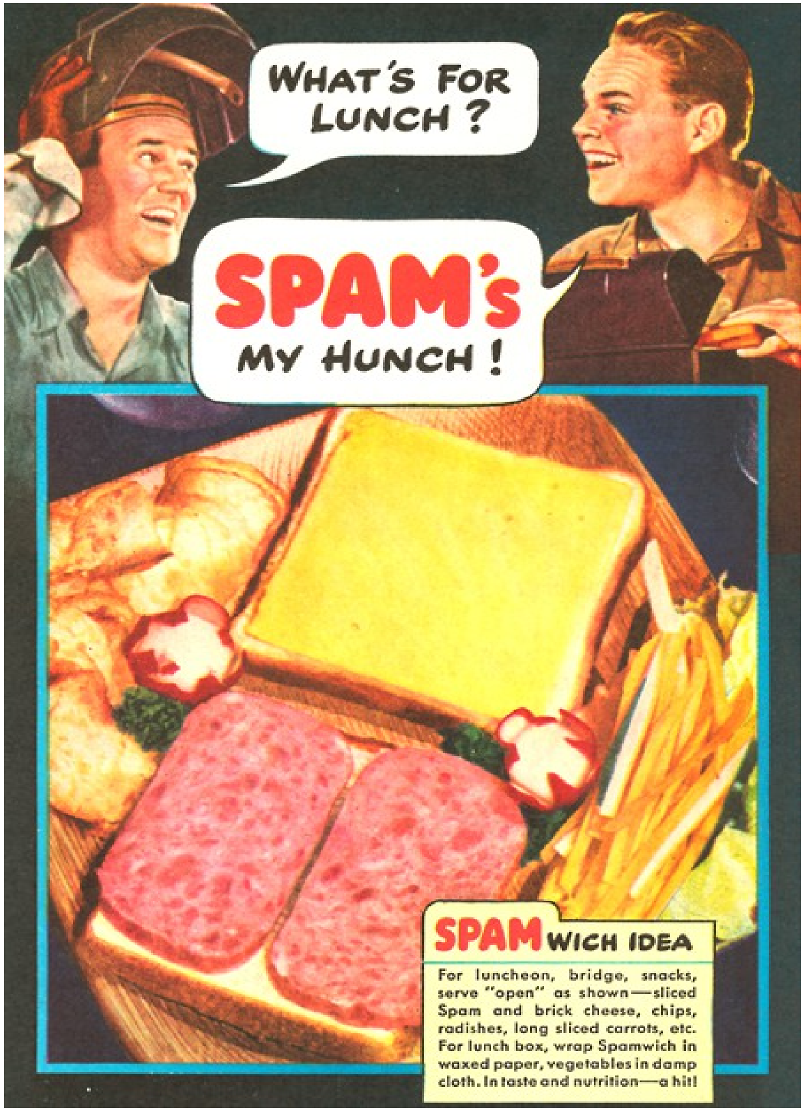
DDoS Tools: Tribal Flood Network

- Supports multiple DoS attack types
  - Smurf; ICMP, SYN, UDP floods
- Attacker runs masters directly via root backdoor; masters talk to zombies using ICMP echo reply
  - No authentication of master’s commands, but commands are encoded as 16-bit binary numbers inside ICMP packets to prevent accidental triggering
  - Vulnerable to connection hijacking and RST sniping
- List of zombie daemons’ IP addresses is encrypted in later versions of TFN master

DDoS Tools: Stacheldraht

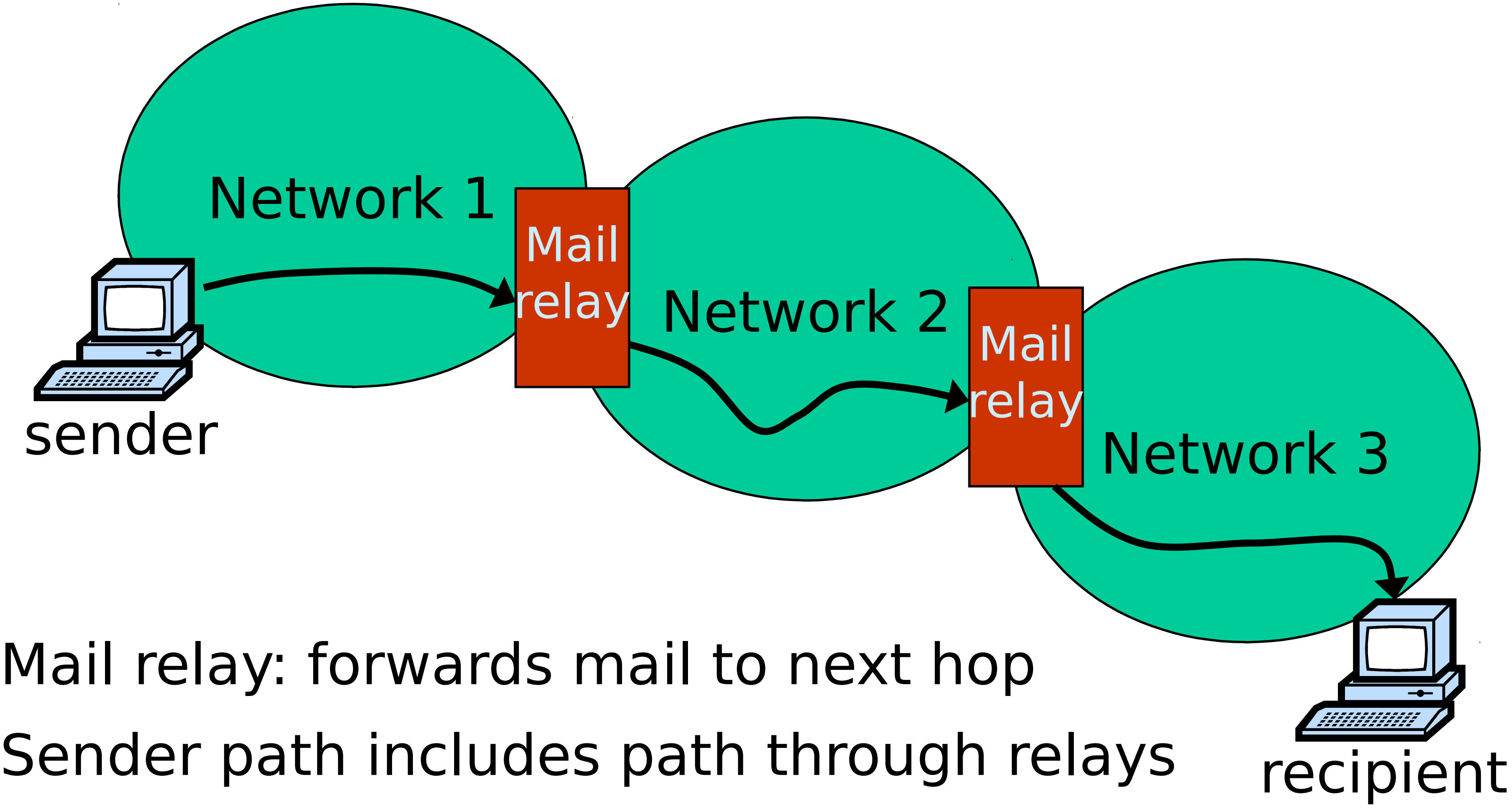
- Combines “best” features of Trin00 and TFN
  - Multiple attack types (like TFN)
- Symmetric encryption for attacker-master connections
- Master daemons can be upgraded on demand
- February 2000: Crippled Yahoo, eBay, Amazon, Schwab, E*Trade, CNN, Buy.com, ZDNet
  - Smurf-like attack on Yahoo consumed more than a Gigabit/sec of bandwidth
  - Sources of attack still unknown

Spam



For luncheon, bridge, snacks, serve "open" as shown—sliced Spam and brick cheese, chips, radishes, long sliced carrots, etc. For lunch box, wrap Spamwich in waxed paper, vegetables in damp cloth. In taste and nutrition—a hit!

Email in the early 1980s



- Mail relay: forwards mail to next hop
- Sender path includes path through relays

Email spoofing

- Mail is sent via SMTP protocol
  - No built-in authentication
- MAIL FROM field is set by the sender
  - Classic example of improper input validation
- Recipient’s mail server only sees IP address of the direct peer from whom it received the msg

Open relays

- SMTP relay forwards mail to destination
  1. Bulk email tool connects via SMTP (port 25)
  2. Sends list of recipients via RCPT TO command
  3. Sends email body (once for all recipients!)
  4. Relay delivers message
- Honest relay adds correct Received: header revealing source IP
- Hacked relay does not

A closer look at spam

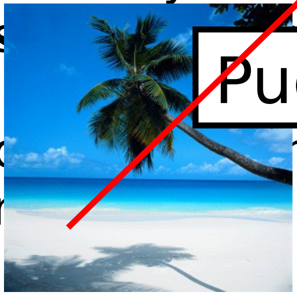
```
Received: by 10.78.68.6 with SMTP id q6cs294373hua;
          Mon, 12 F                            PST)
Received: by 10.90.113.18 with SMTP id
l18mr17307116agc.1171291410432;
          M                  6:43:30 -0800 (PST)
Return-Path:                .ro>
Received: from onelinkpr.net ([203.169.49.172])
        by mx.google.com with ESMTP id
30s                 2007.02.12.06.43.18

Rec         neutral (google.com: 203                neither permitted
nor
          by best guess record for                  nlwee@aviva.ro)
Message-ID: <20050057765.stank.203.169.49.172@ASAFTU>
From: "Barclay Morales" <wvnlwee@aviva.ro>
To: <raykwatts@gmail.com>
Subject: You can order both Viagra and Cialis.
```

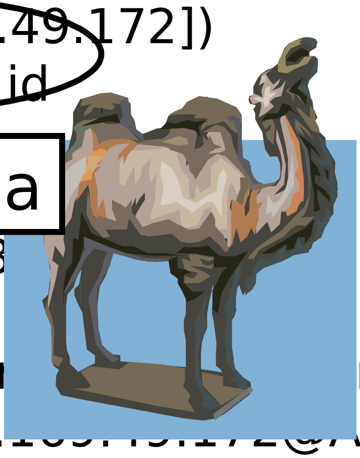
Inserted by relays

Bogus!

Puerto Rico

Mongolia



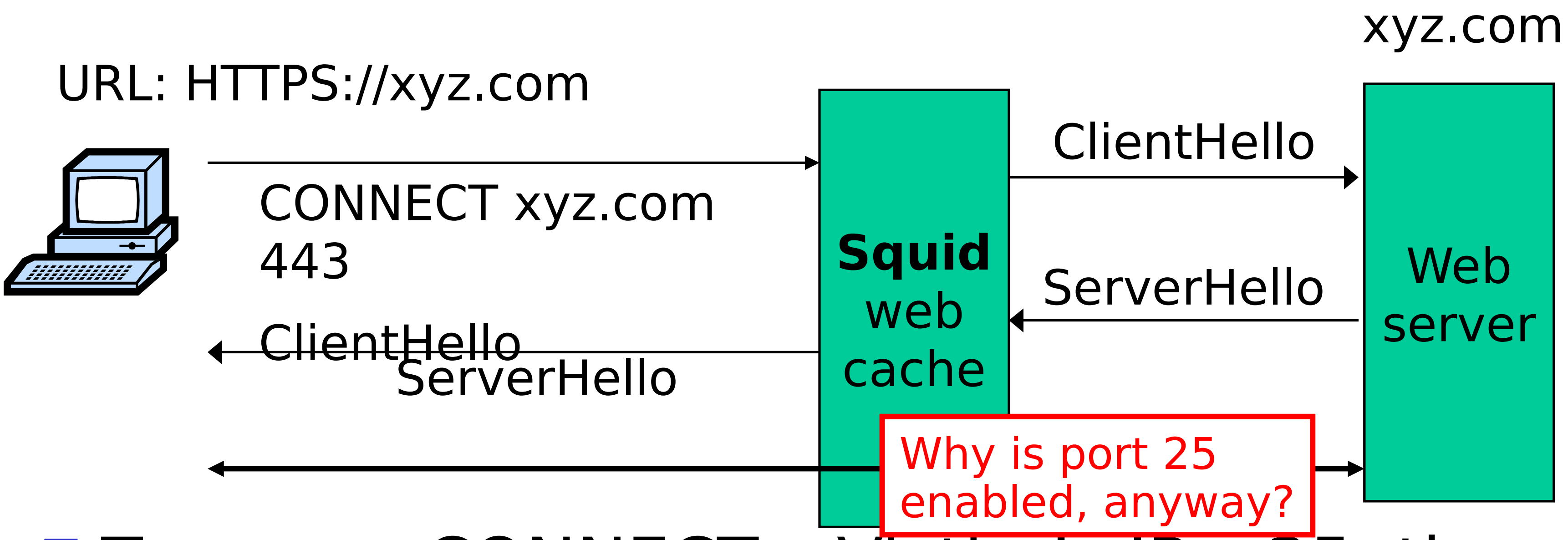


Why hide sources of spam?

- Many email providers blacklist servers and ISPs that generate a lot of spam
  - Use info from spamhaus.org, spamcop.net
- Real-time blackhole lists stop 15-25% of spam at SMTP connection time
  - Over 90% after message body URI checks
- Spammers’ objective: evade blacklists
  - Botnets come very handy!

Open HTTP proxies

- Web cache (HTTP/HTTPS proxy), e.g., squid



xyz.com

URL: HTTPS://xyz.com

CONNECT xyz.com 443

ClientHello

ServerHello

Squid web cache

ClientHello

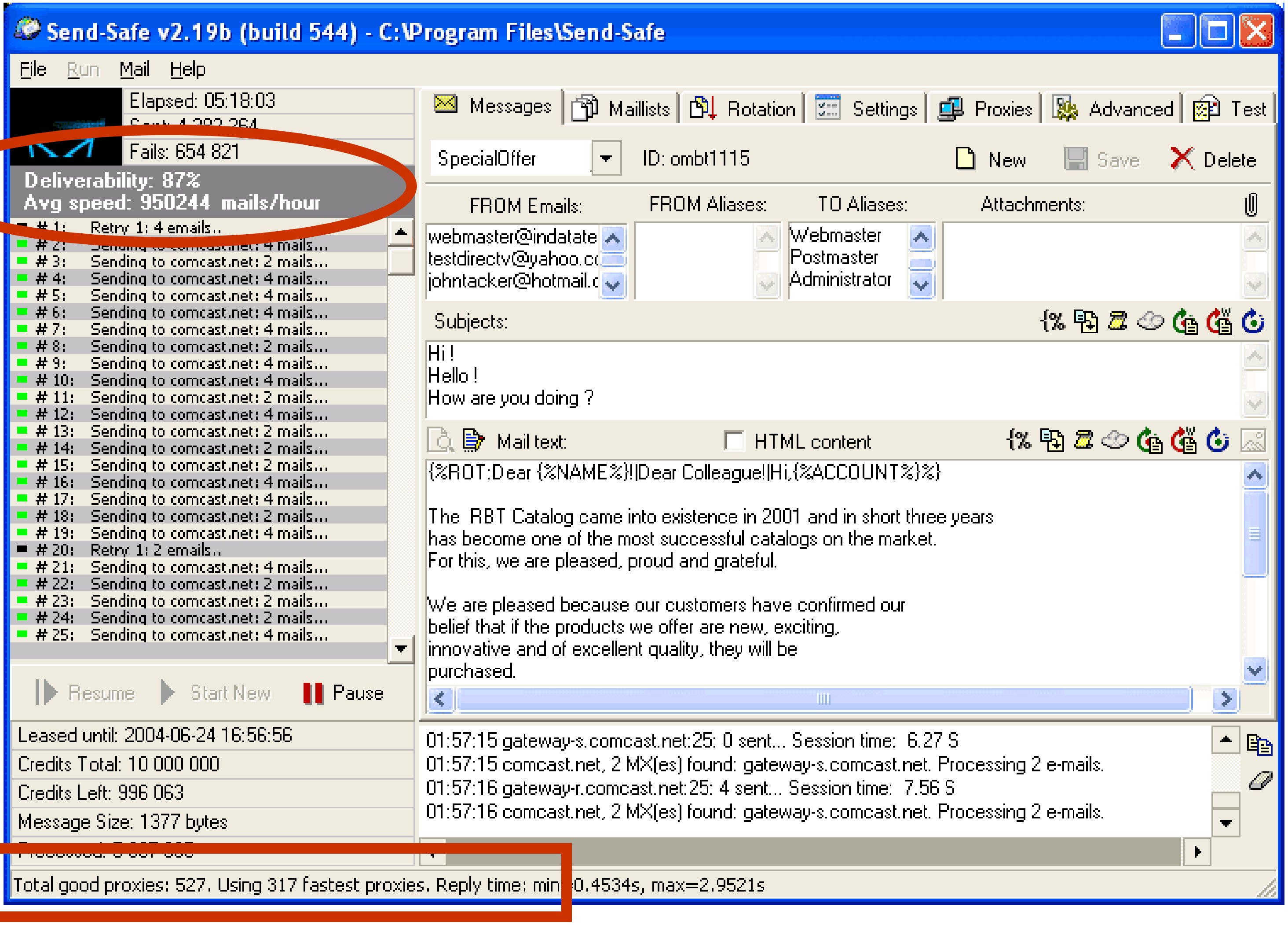
ServerHello

Web server

Why is port 25 enabled, anyway?

- To spam: CONNECT <Victim’s IP> 25, then issue SMTP Commands
  - Squid becomes a mail relay

Send-safe spam tool



Elapsed: 05:18:03
Sent: 4 382 264
Fails: 654 821
Deliverability: 87%
Avg speed: 950244 mails/hour

```
# 1:   Retry 1: 4 emails..
# 2:   Sending to comcast.net: 4 mails...
# 3:   Sending to comcast.net: 2 mails...
# 4:   Sending to comcast.net: 4 mails...
# 5:   Sending to comcast.net: 4 mails...
# 6:   Sending to comcast.net: 4 mails...
# 7:   Sending to comcast.net: 4 mails...
# 8:   Sending to comcast.net: 2 mails...
# 9:   Sending to comcast.net: 4 mails...
# 10:  Sending to comcast.net: 4 mails...
# 11:  Sending to comcast.net: 2 mails...
# 12:  Sending to comcast.net: 4 mails...
# 13:  Sending to comcast.net: 2 mails...
# 14:  Sending to comcast.net: 2 mails...
# 15:  Sending to comcast.net: 2 mails...
# 16:  Sending to comcast.net: 4 mails...
# 17:  Sending to comcast.net: 4 mails...
# 18:  Sending to comcast.net: 2 mails...
# 19:  Sending to comcast.net: 4 mails...
# 20:  Retry 1: 2 emails..
# 21:  Sending to comcast.net: 4 mails...
# 22:  Sending to comcast.net: 2 mails...
# 23:  Sending to comcast.net: 2 mails...
# 24:  Sending to comcast.net: 2 mails...
# 25:  Sending to comcast.net: 4 mails...
```

Leased until: 2004-06-24 16:56:56
Credits Total: 10 000 000
Credits Left: 996 063
Message Size: 1377 bytes
Processed: 5 037 085

SpecialOffer ID: ombt1115

FROM Emails:
webmaster@indatate
testdirectv@yahoo.cc
johntacker@hotmail.c

FROM Aliases:

TO Aliases:
Webmaster
Postmaster
Administrator

Attachments:

Subjects:
Hi !
Hello !
How are you doing ?

Mail text: □ HTML content

{%ROT:Dear {%NAME%}!|Dear Colleague!|Hi,{%ACCOUNT%}%}

The RBT Catalog came into existence in 2001 and in short three years
has become one of the most successful catalogs on the market.
For this, we are pleased, proud and grateful.

We are pleased because our customers have confirmed our
belief that if the products we offer are new, exciting,
innovative and of excellent quality, they will be
purchased.

```
01:57:15 gateway-s.comcast.net:25: 0 sent... Session time:  6.27 S
01:57:15 comcast.net, 2 MX(es) found: gateway-s.comcast.net. Processing 2 e-mails.
01:57:16 gateway-r.comcast.net:25: 4 sent... Session time:  7.56 S
01:57:16 comcast.net, 2 MX(es) found: gateway-s.comcast.net. Processing 2 e-mails.
```

Total good proxies: 527. Using 317 fastest proxies. Reply time: min=0.4534s, max=2.9521s

Open relays vs. open proxies

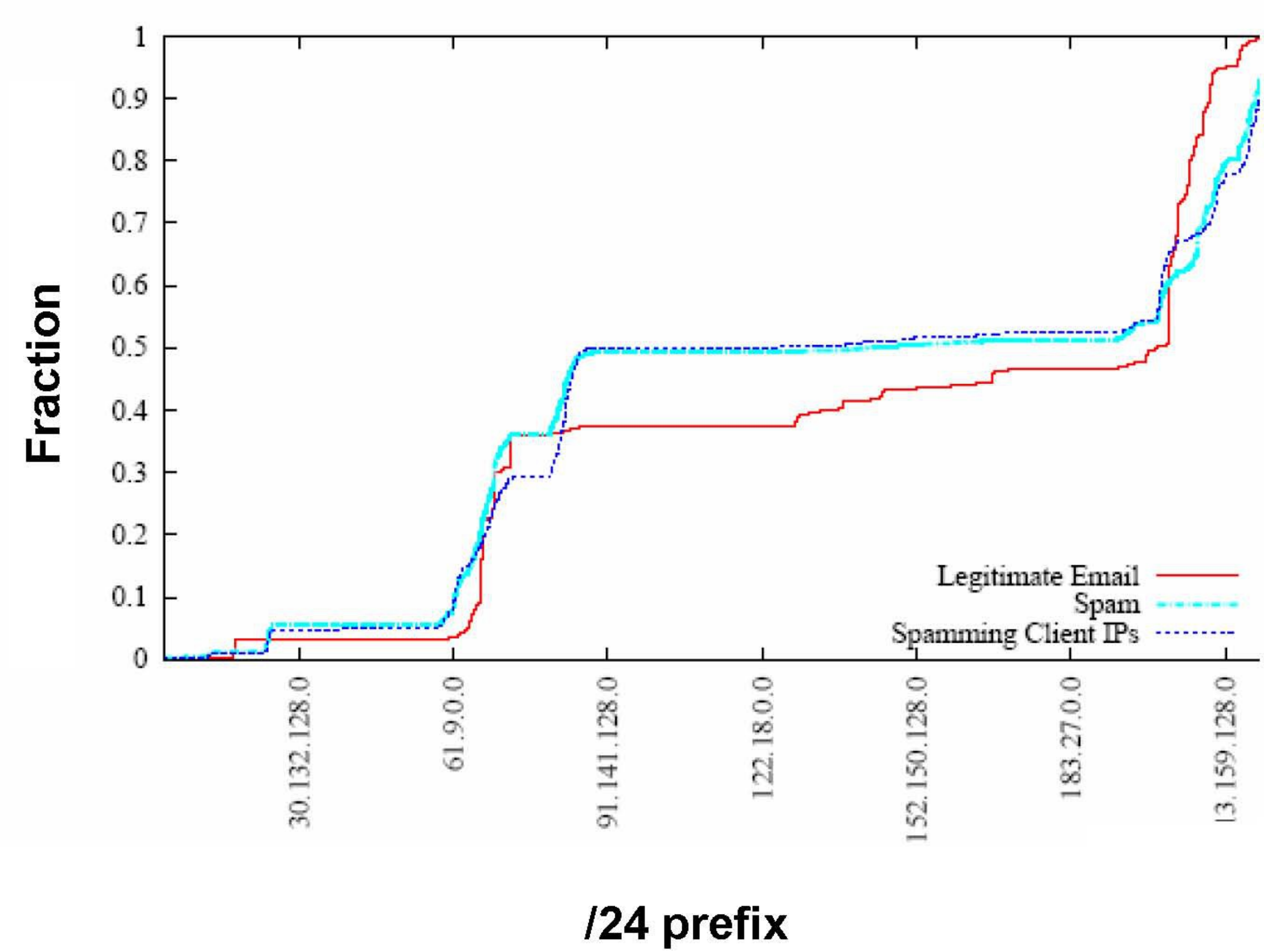
- Open proxy
  - Spammer must send message to each recipient through the proxy
- Open relay
  - Takes a list of addresses and sends to all
  - Can host an open relay on a zombie
- Listing services for open proxies and relays
  - http://www.multiproxy.org/
    http://www.stayinvisible.com/
    http://www.openproxies.com/ ($20/month)

Bobax worm

- Infects machines with high bandwidth
  - Exploits MS LSASS.exe buffer overflow vulnerability
- Slow spreading (and thus hard to detect)
  - On manual command from operator, randomly scans for vulnerable machines
- Installs hacked open relay on infected zombie
  - Once spam zombie added to blacklist, spread to another machine
  - Interesting detection technique: Look for botmaster's DNS queries (trying to determine who is blacklisted)

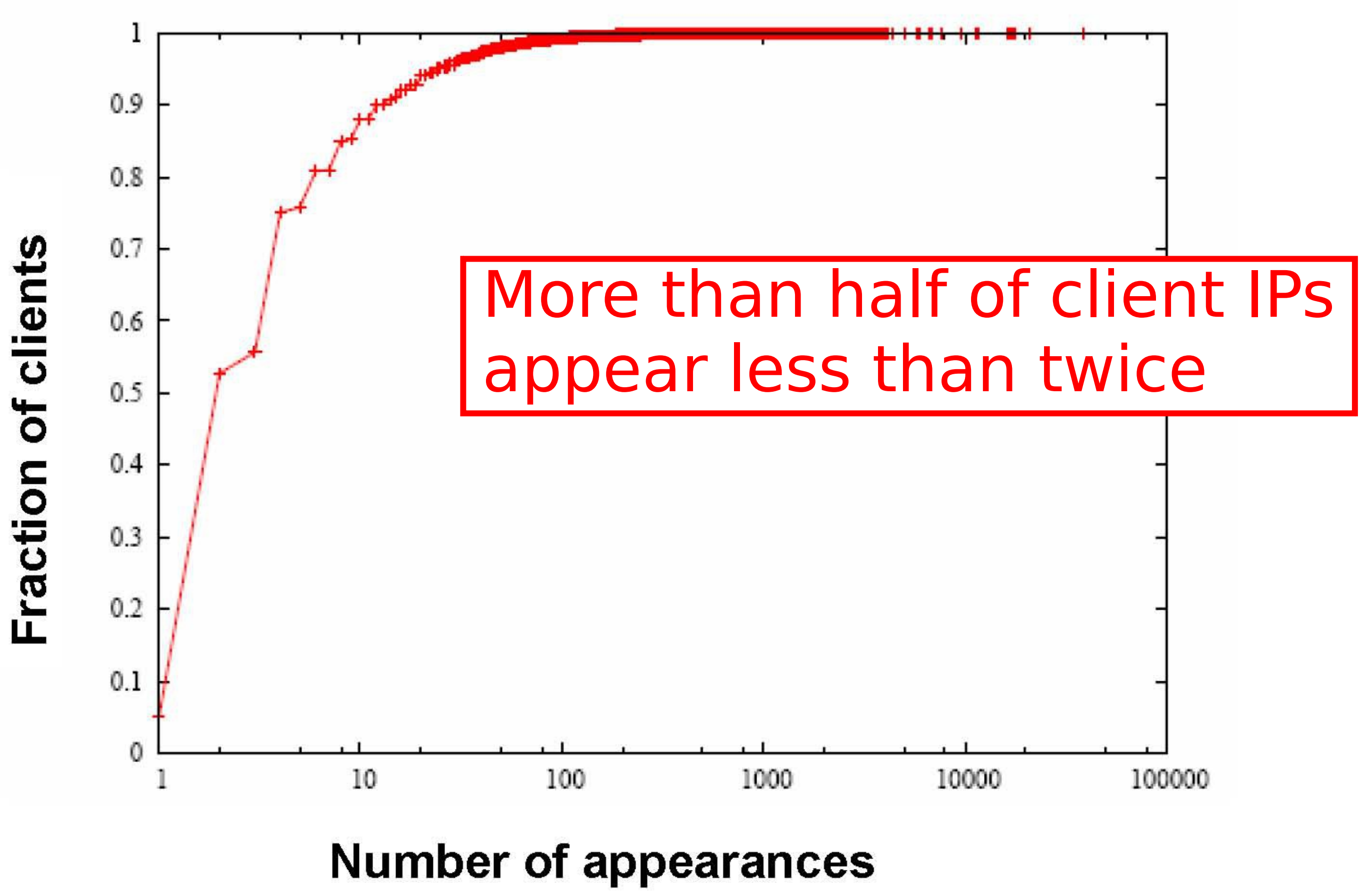
Distribution of spam sources

[Ramachandran, Feamster]



IP blacklisting not enough

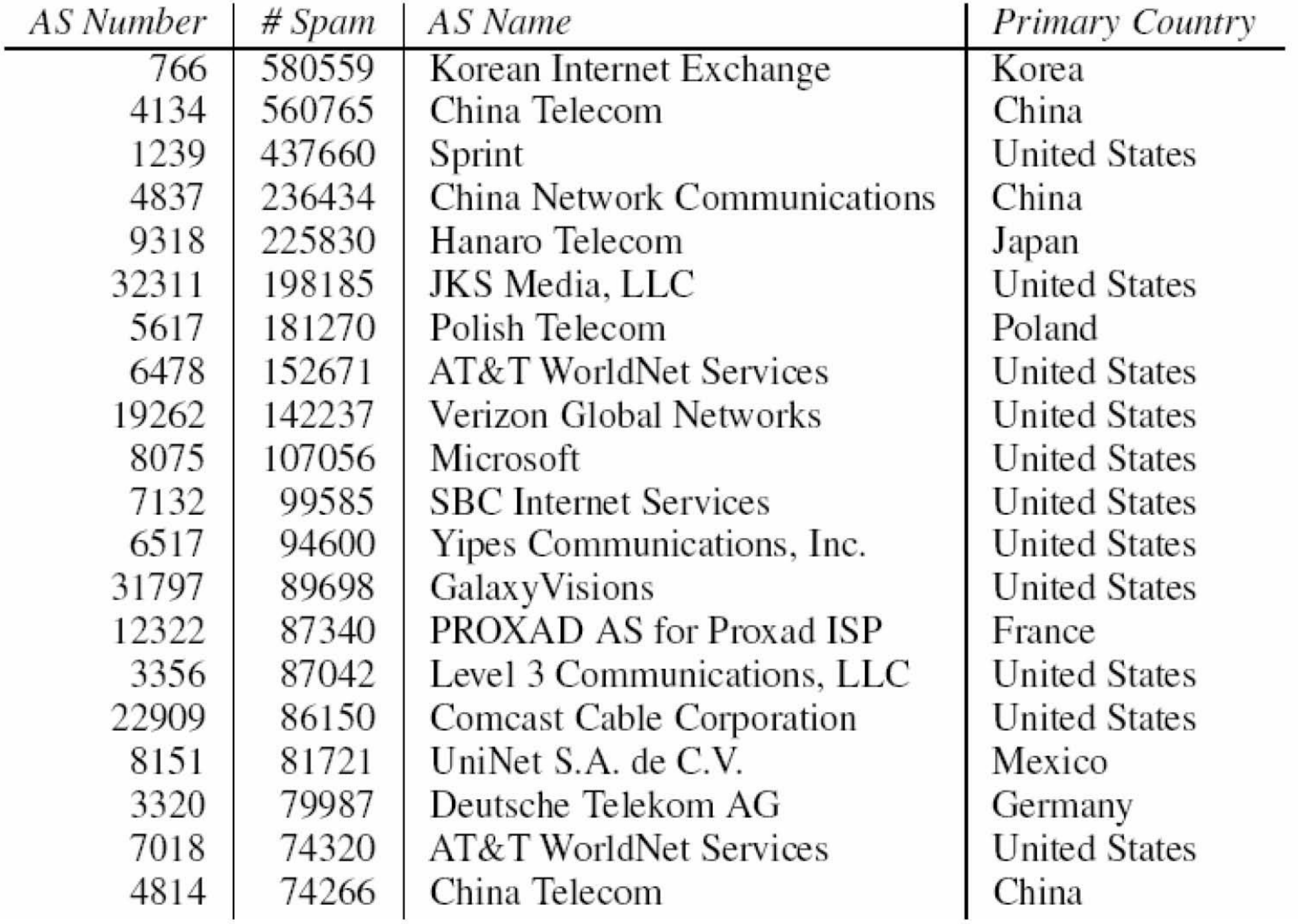
[Ramachandran, Feamster]



More than half of client IPs appear less than twice

Distribution across domains

[Ramachandran, Feamster]

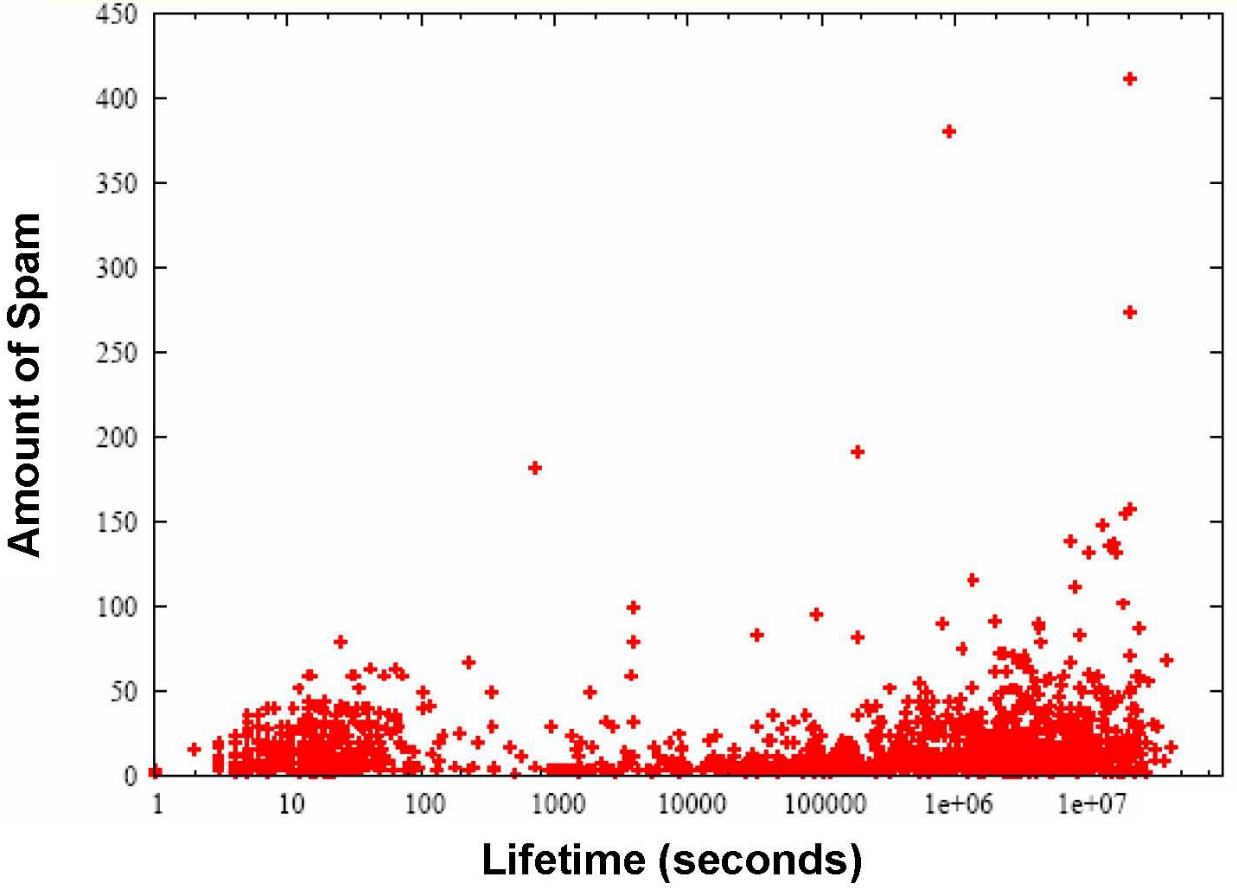


AS Number	*# Spam*	*AS Name*	*Primary Country*
766	580559	Korean Internet Exchange	Korea
4134	560765	China Telecom	China
1239	437660	Sprint	United States
4837	236434	China Network Communications	China
9318	225830	Hanaro Telecom	Japan
32311	198185	JKS Media, LLC	United States
5617	181270	Polish Telecom	Poland
6478	152671	AT&T WorldNet Services	United States
19262	142237	Verizon Global Networks	United States
8075	107056	Microsoft	United States
7132	99585	SBC Internet Services	United States
6517	94600	Yipes Communications, Inc.	United States
31797	89698	GalaxyVisions	United States
12322	87340	PROXAD AS for Proxad ISP	France
3356	87042	Level 3 Communications, LLC	United States
22909	86150	Comcast Cable Corporation	United States
8151	81721	UniNet S.A. de C.V.	Mexico
3320	79987	Deutsche Telekom AG	Germany
7018	74320	AT&T WorldNet Services	United States
4814	74266	China Telecom	China

Most bots send little spam

[Ramachandran, Feamster]

Most bot IP addresses send very little spam, regardless of how long they have been spamming…



Where does spam come from?

[Ramachandran, Feamster]

- IP addresses of spam sources are widely distributed across the Internet
  - In tracking experiments, most IP addresses appear once or twice; 60-80% not reachable by traceroute
- Vast majority of spam originates from a small fraction of IP address space
  - Same fraction that most legitimate email comes from
- Spammers exploit routing infrastructure
  - Create short-lived connection to mail relay, then disappear
  - Hijack large blocks of unallocated “dark”

Spambot behavior

[Ramachandran, Feamster]

- Strong correlation with Bobax infections
- Most are active for a very short time
  - 65% of Bobax victims send spam once; 3 out of 4 are active for less than 2 minutes
- 99% of bots send fewer than 100 messages regardless of their lifetime
- 95% of bots already in one or more blacklists
  - Cooperative detection works, but …
  - Problem: False positives!
  - Problem: Short-lived hijacks of dark address space

Detecting Botnets

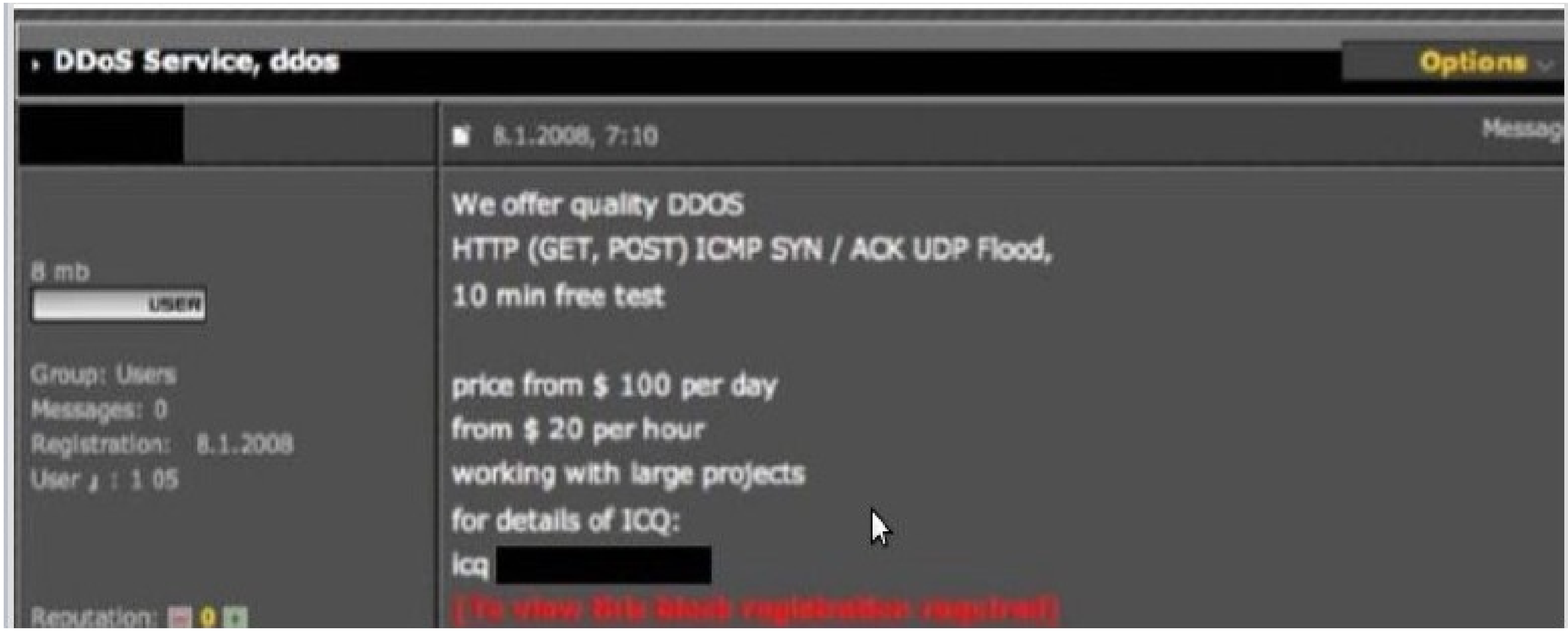
- Today's bots are controlled via IRC and DNS
  - IRC used to issue commands to zombies
  - DNS used by zombies to find the master, and by the master to find if a zombie has been blacklisted
- IRC/DNS activity is very visible in the network
  - Look for hosts performing scans, and for IRC channels with a high percentage of such hosts
    - Used with success at Portland State University
  - Look for hosts who ask many DNS queries, but receive few queries about themselves

Bot usage

- DDoS attacks
- ID theft
- Phishing
- Spamming
- Privacy Issues- installing keylogger, spywares
- Renting web proxies for illegal purposes
- …many more

In short – “ **TO EARN MONEY”**

Bot economics



DDoS Service, ddos

[redacted]

8.1.2008, 7:10

8 mb

Group: Users
Messages: 0
Registration: 8.1.2008
User ♪ : 1 05

Reputation: 0

We offer quality DDOS
HTTP (GET, POST) ICMP SYN / ACK UDP Flood,
10 min free test

price from $ 100 per day
from $ 20 per hour
working with large projects
for details of ICQ:
icq [redacted]
[To view this block registration required]

Bot economics (2.)

- A paper from VB conference 2006 by Lovet
- A credit card business
  - Buying 40 valid CC - $200
  - Hiring 10 drops to collect purchased things- $800 ($20 per package)
  - Drops to cyber criminal delivery - $800
  - Selling on eBay - $17,800 (like Laptop,mobiles,clothes)
- Total cost, monthly- $1800
- Total profit - $17,800
- Net profit: $16,000
- Productivity index (Profit/Costs): 8.9

Protecting against Botnets

- For individual users:
  - Use updated OS and legal software
  - Anti virus software
  - Firewall
  - Don't open Spam e-mails
  - Check your logs
- For corporate networks:
  - Use strict firewall rules
  - Deploy honeypots and set-up DNS redirection to to it
  - Sniff outbound connection by using keywords used by bot herders