Botnets

Why to talk about Botnets...

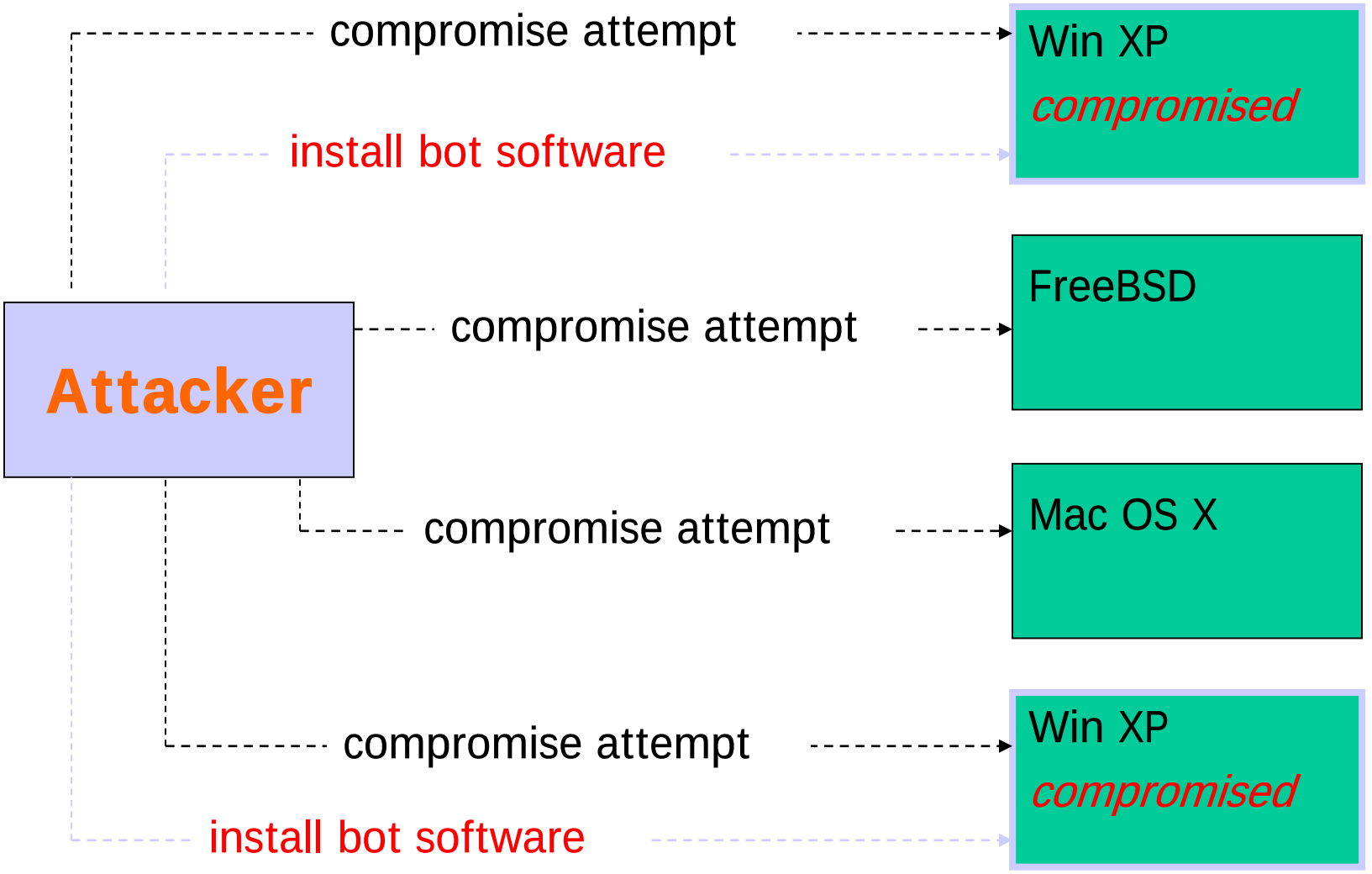
- Botnet could be a most powerful supercomputer in the world
- Recent attack on countries, e.g., Estonia
- Vehicle for cyber-terrorism and cyber crime
- Very serious security threat that could stop your national IT infrastructure

=> 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

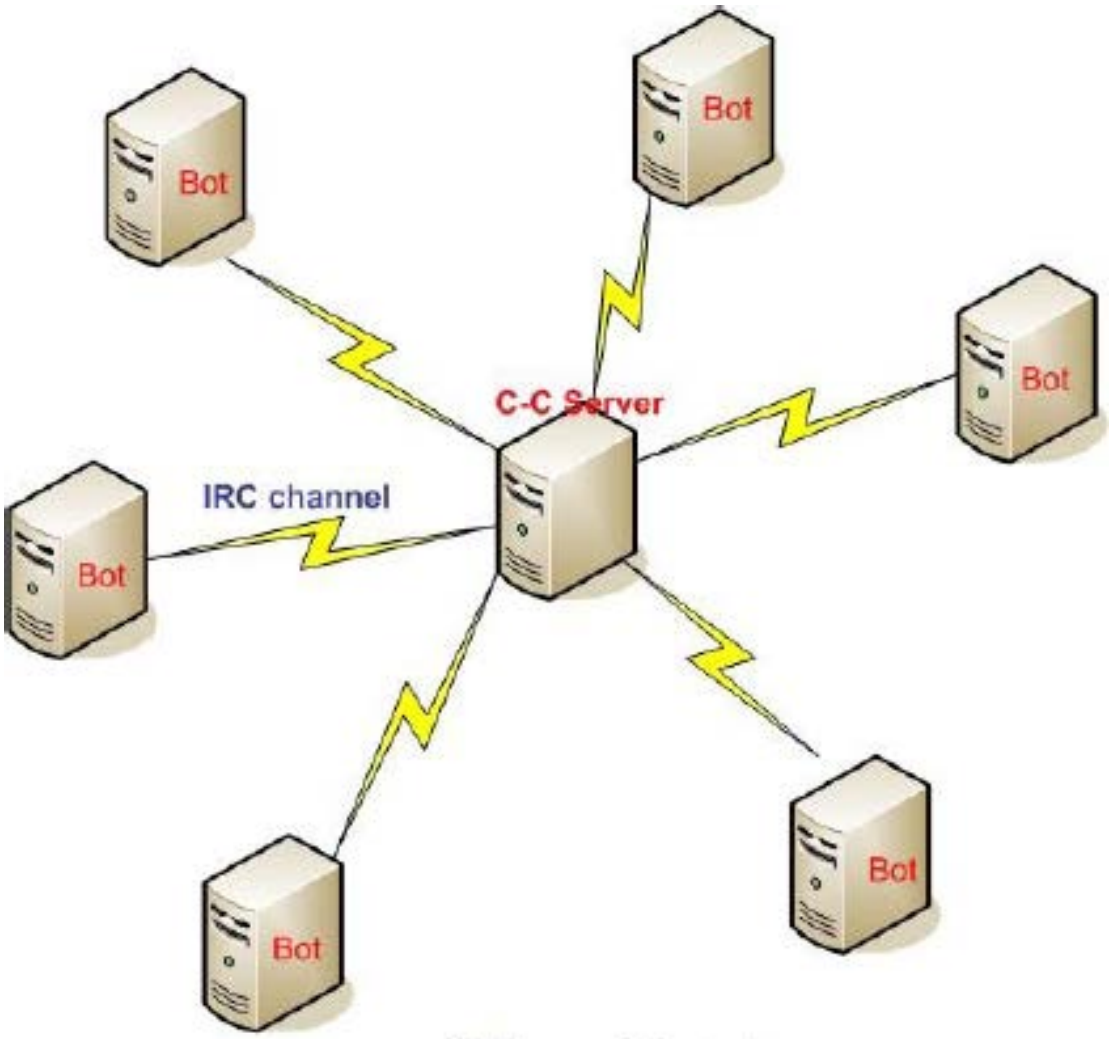
Building a Botnet



Botnet construction

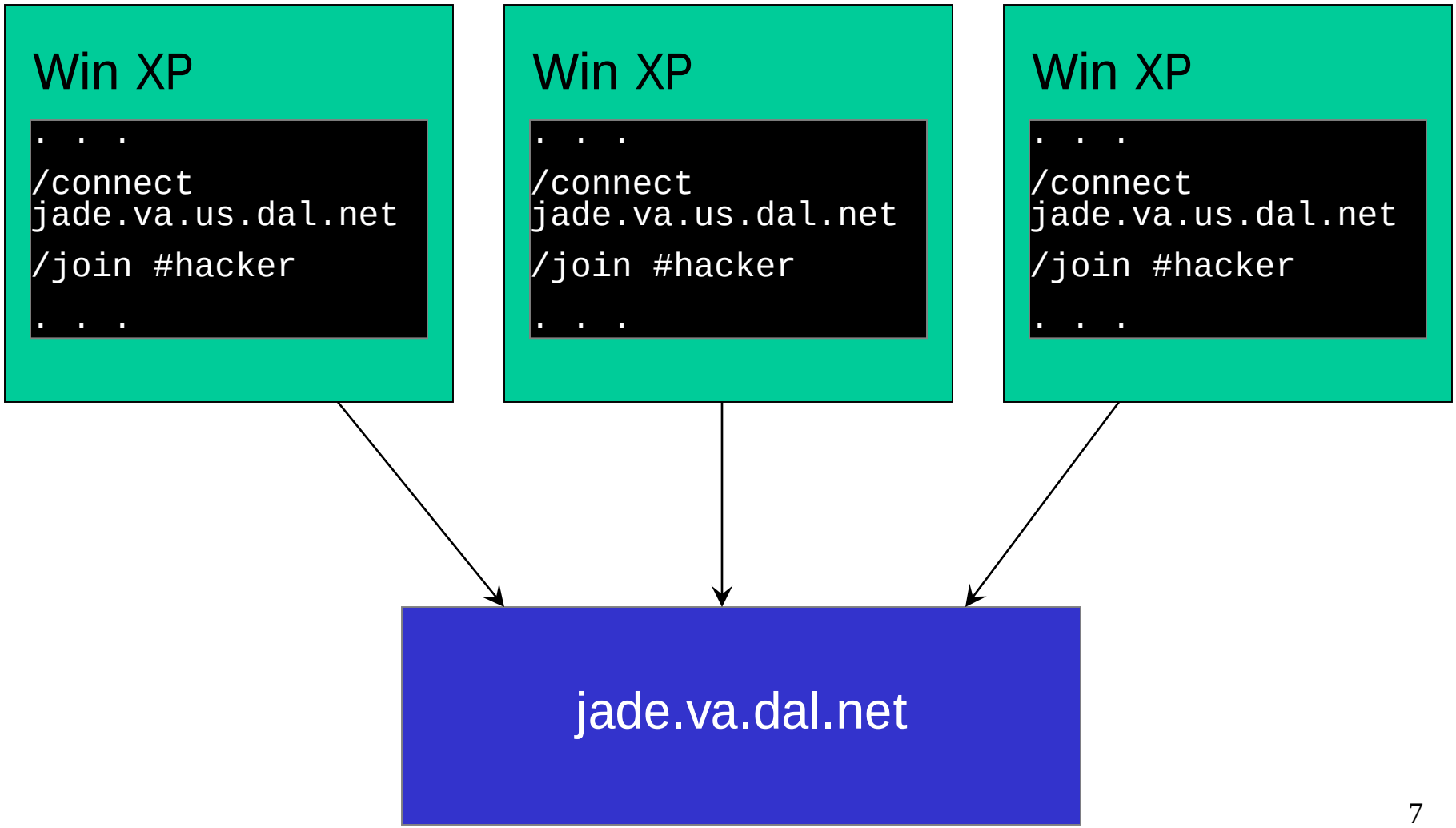
- First stage, exploit vulnerabilities (operating system's/browser's)
  - Next stage to download bot software, C&C instructions
  - Once the bot software is executed and connected to C&C server
- Bots connect to channel of C&C (IRC or HTTP) password protected channel
- Encryption layer between bot and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

IRC Botnet



IRC based Botnets

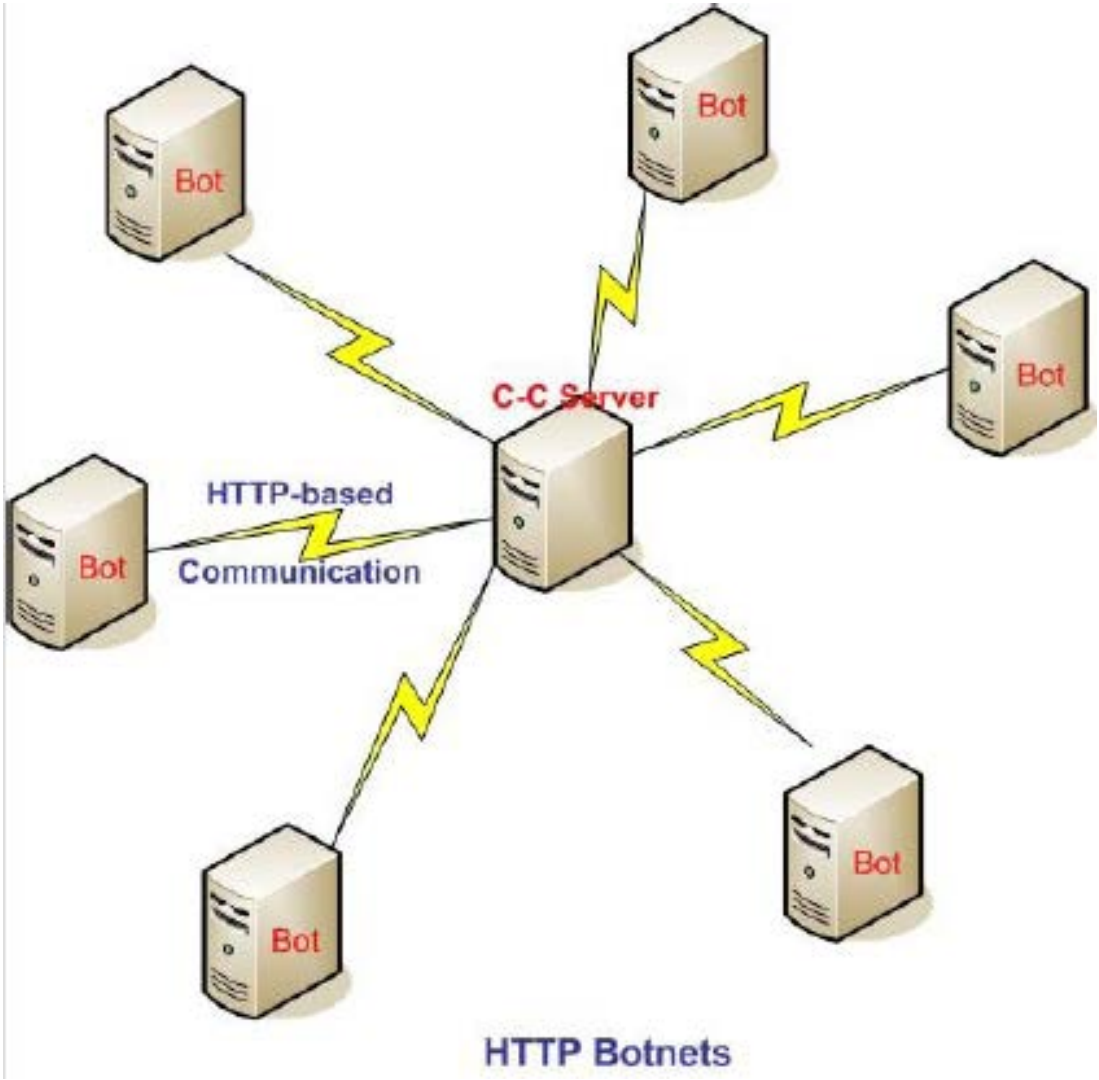
Joining the IRC Channel



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
```

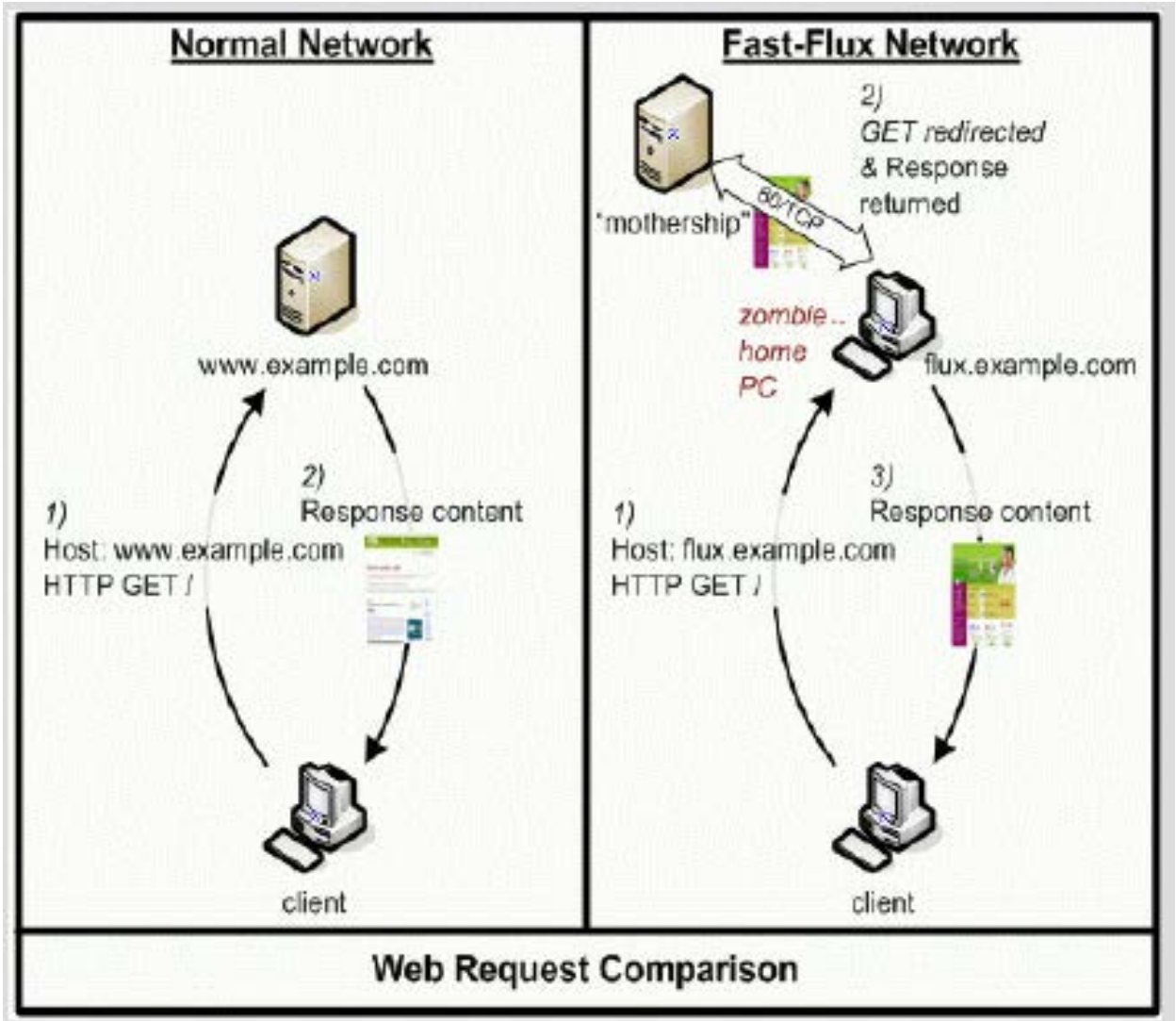
HTTP Botnet


Bot
Bot
Bot
C-C Server
Bot
HTTP-based
Communication
Bot
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
  - Detect non-responding bots, identify "superbots"

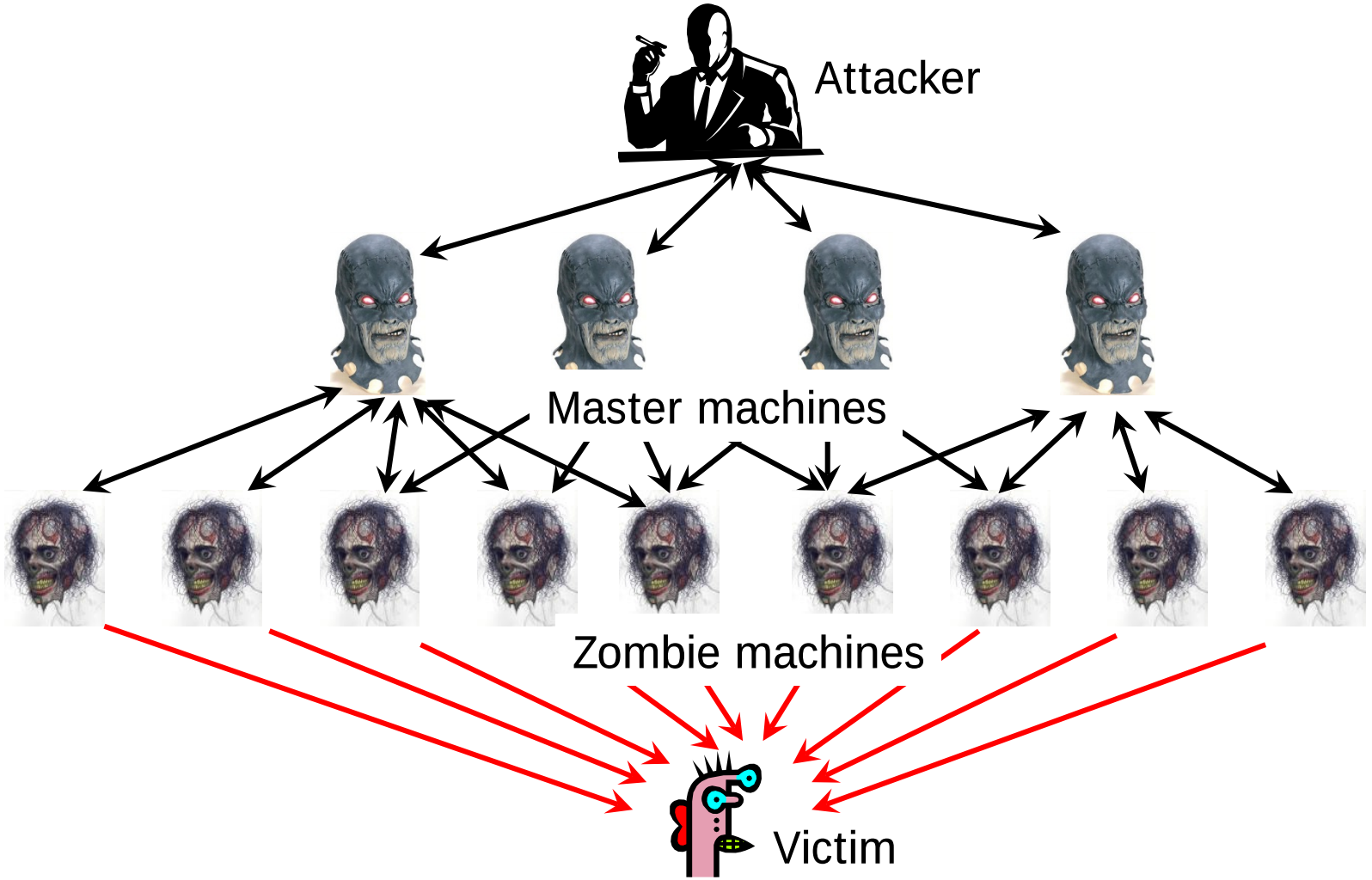
Denial of Service (DoS) Redux

- 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



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 someone connects when master is already authenticated
- August of 1999: a network of 227 Trin00 zombies took U. of Minnesota offline for 3 days

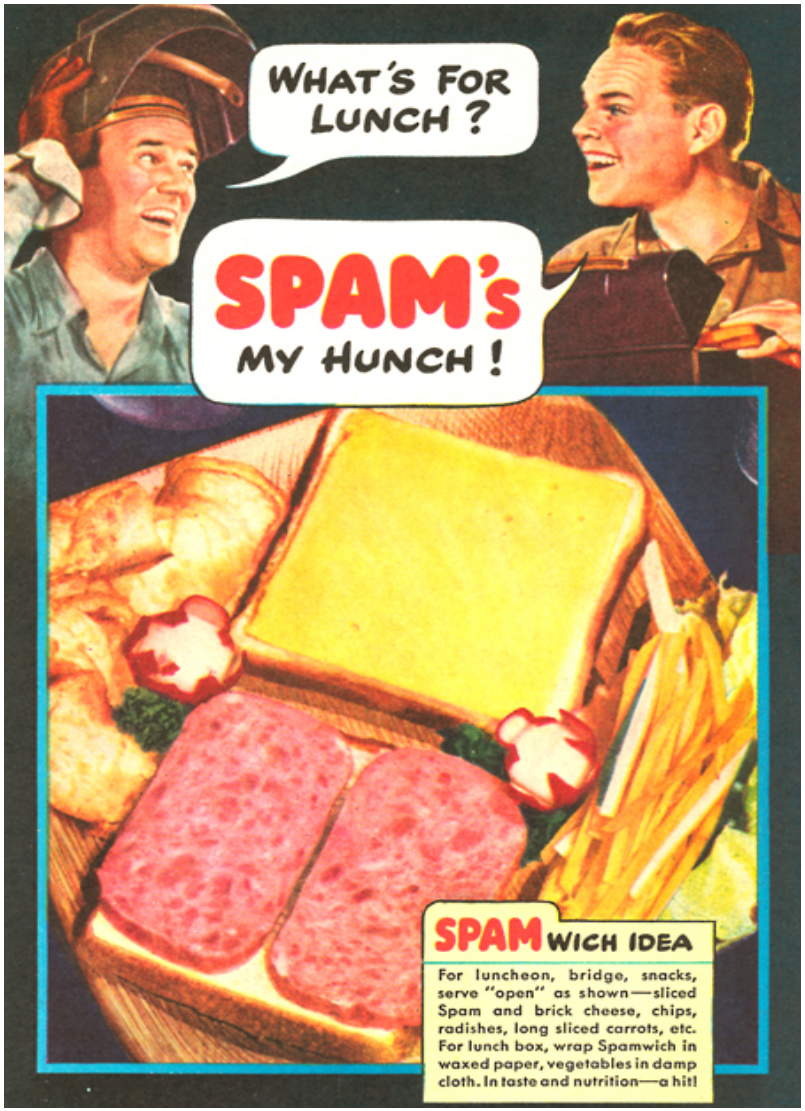
DDoS Tools: Tribal Flood Network

- 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 scripts
  - Protects identities of zombies if master is discovered

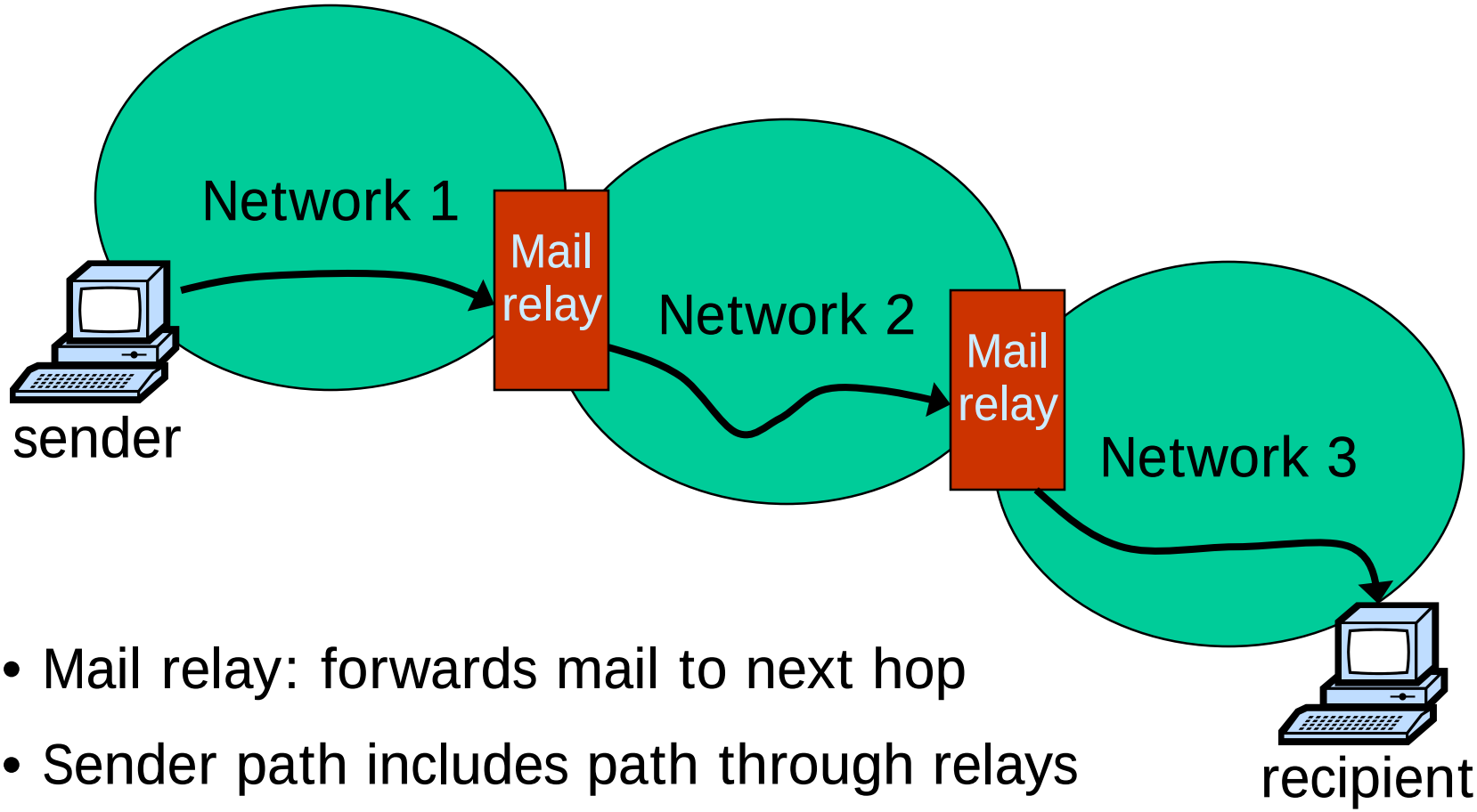
DDoS Tools: Stacheldraht

- 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


WHAT'S FOR LUNCH ?
SPAM's MY HUNCH !
SPAM WICH IDEA
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

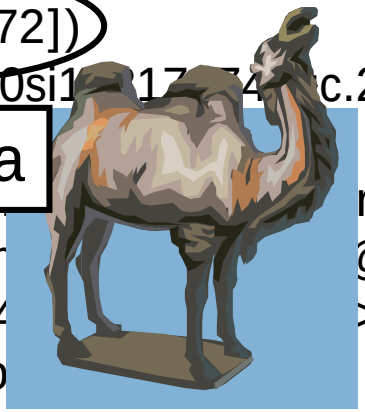
Inserted by relays

Received: by 10.78.68.6 [illegible] hua;
Mon, 12 Feb 2007 06:43:30 -0800 (PST)
Received: by 10 [illegible] MTP id l18mr17307116agc.1171291410432;
Mon [illegible] 43:30 -0800 (PST)
Return-Path: <[illegible]>
Received: from onelinkpr.net ([203.169.49.172])
by mx.google.com with ESMTP id 30si1[illegible]c.2007.02.12.06.43.18;
[illegible]
Rec[illegible] r permitted nor
[illegible]oy best guess record for dor[illegible]@aviva.ro)
Mes[illegible]0050057765.stank.203.169.4[illegible]>
From: "Barclay Morales" <wvnlwee@aviva.ro
To: <raykwatts@gmail.com>
Subject: You can order both Viagra and Cialis.

Bogus!

Puerto Rico

Mongolia

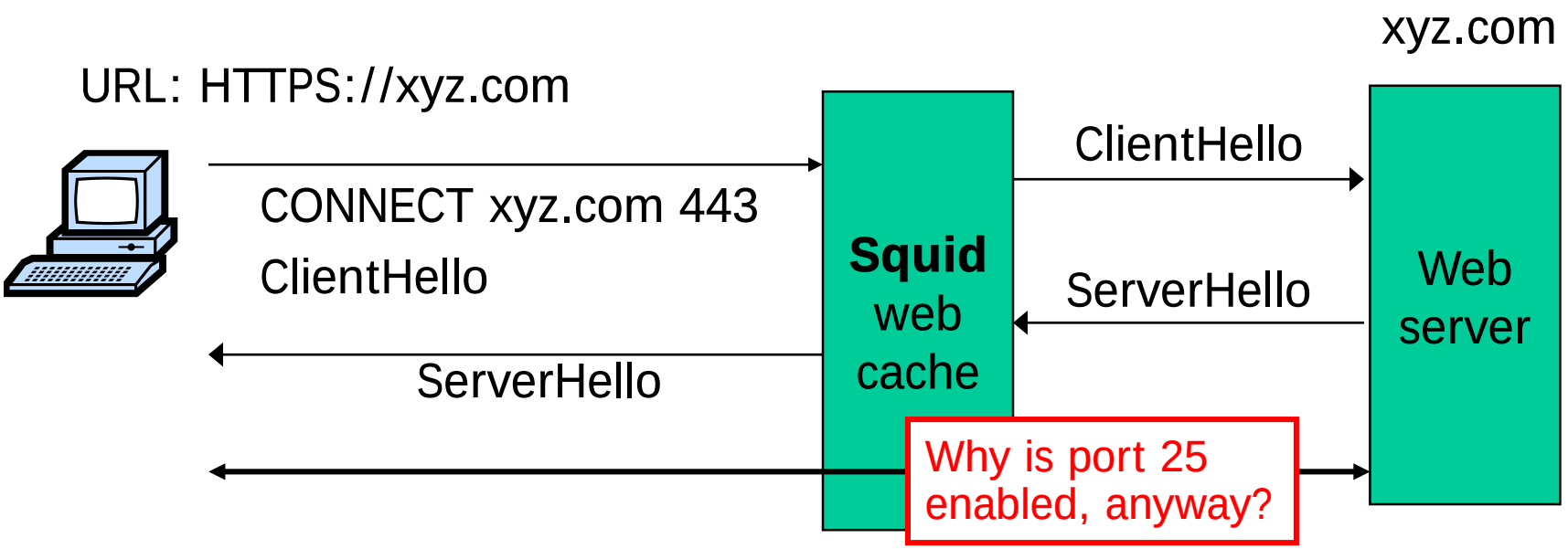


Why hide sources of spam?

- 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!

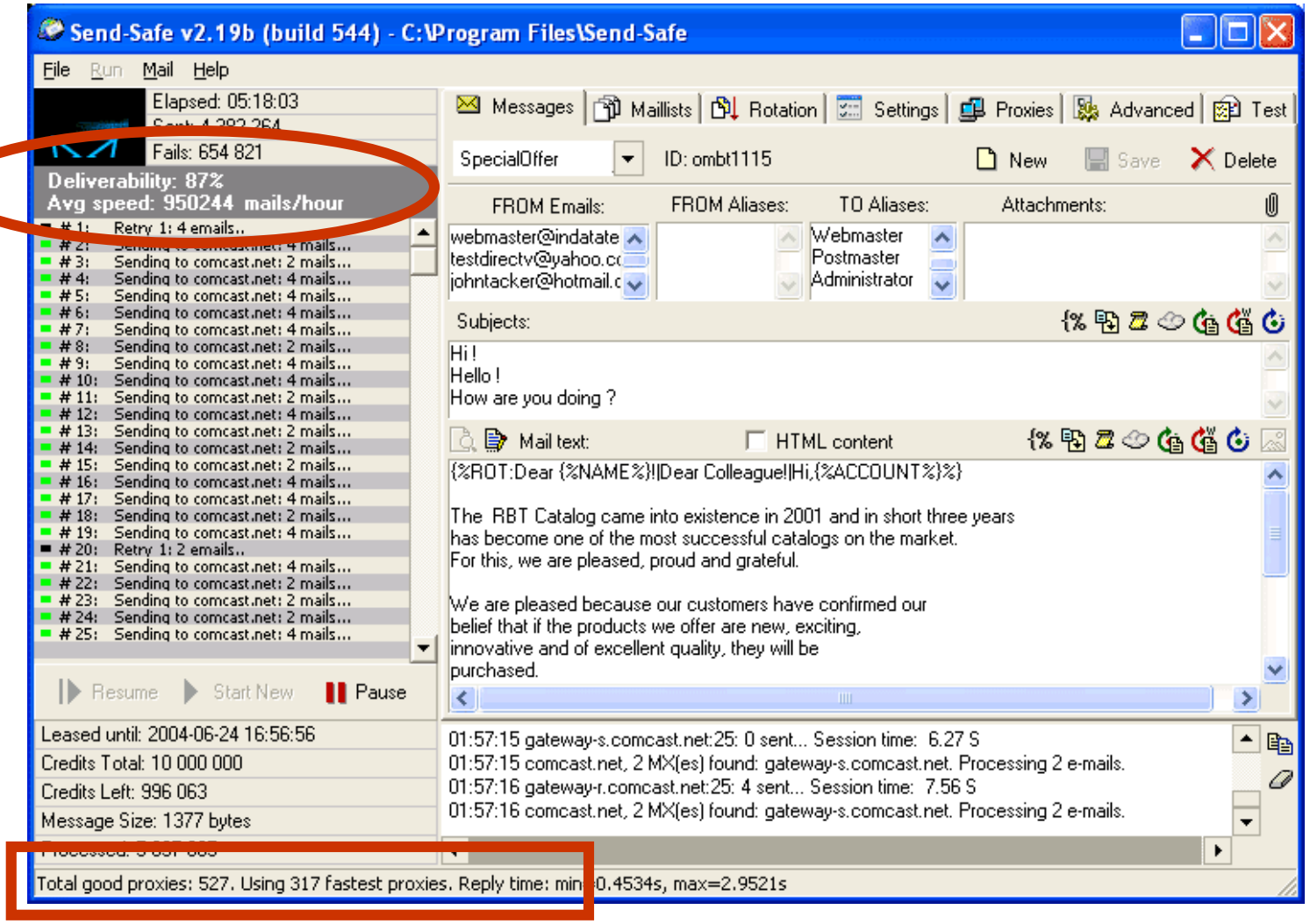
Open HTTP proxies

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



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

Send-safe spam tool



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)

Detecting Botnets

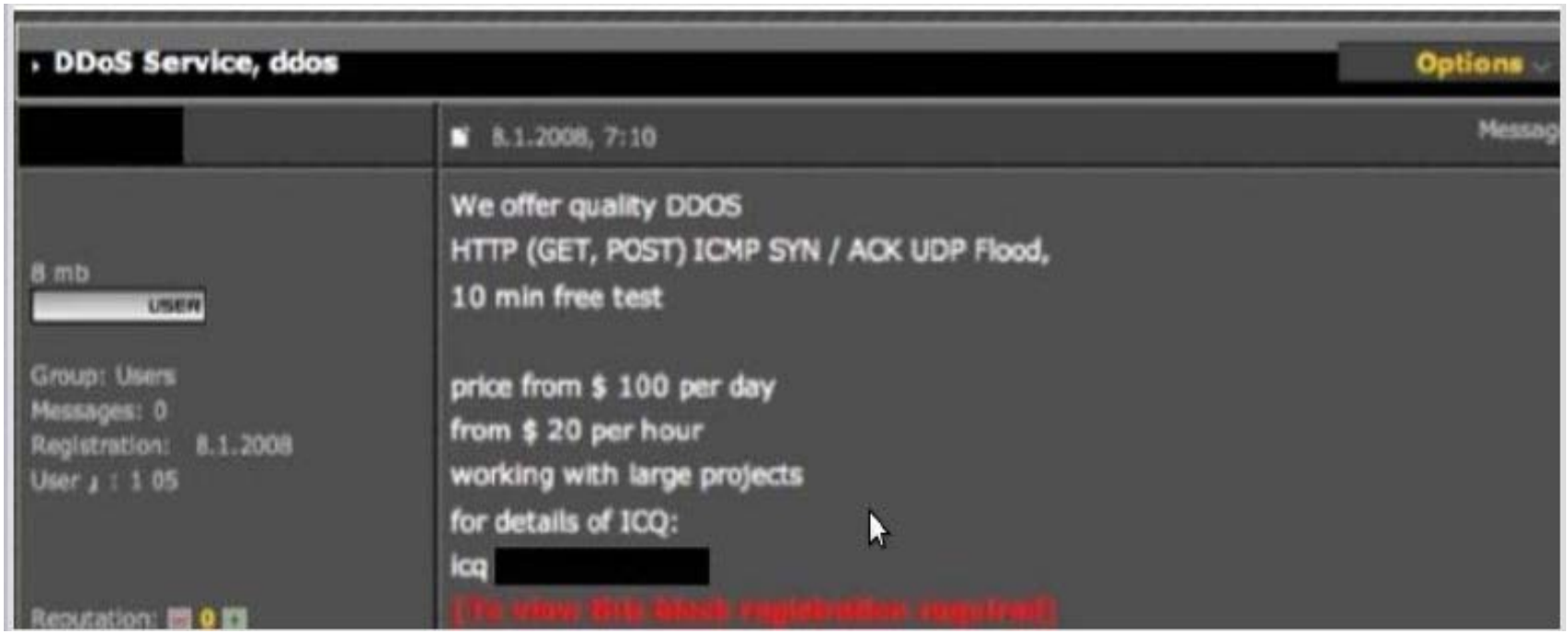
- Today's bots are controlled via IRC and DNS
  - IRC used to issue commands to zombies
  - DNS used by zombies to find the master, and by the master to find if a zombie has been blacklisted
- IRC/DNS activity is very visible in the network
  - Look for hosts performing scans, and for IRC channels with 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
- Easily evaded by using encryption and P2P ☹

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



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