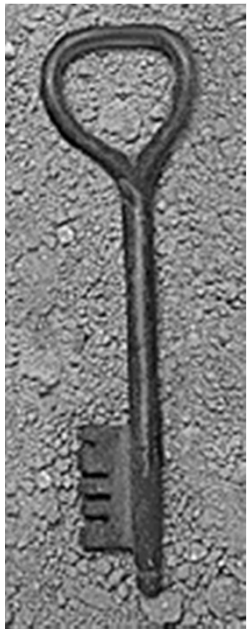
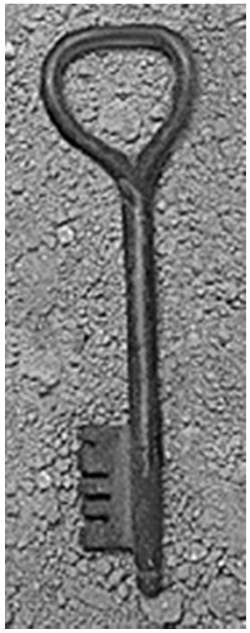
Botnets, Spam, Denial of Service

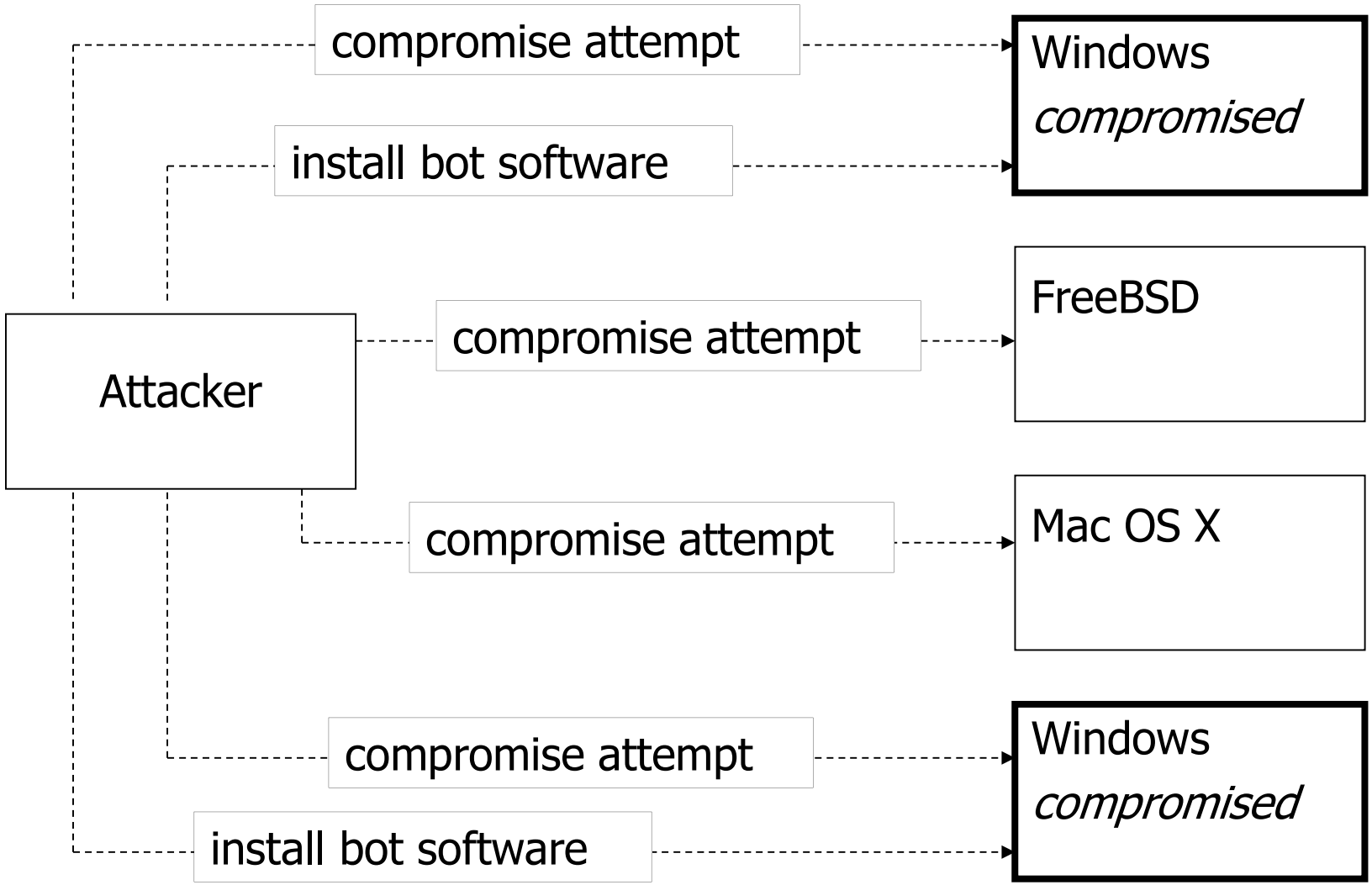


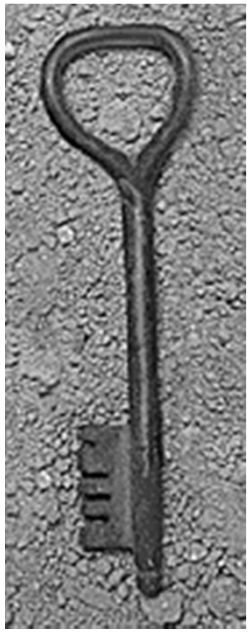
Botnets

- 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 or P2P
- Used as the platform for various attacks
  - Distributed denial of service (DDoS)
  - Spam and click fraud
  - Launching pad for new exploits/worms



Building a Botnet

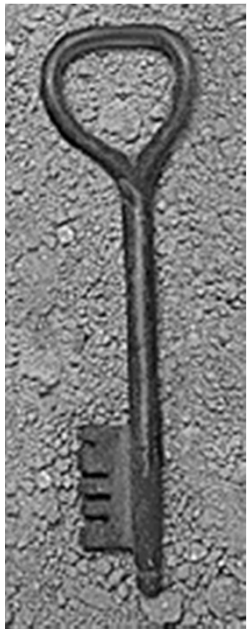




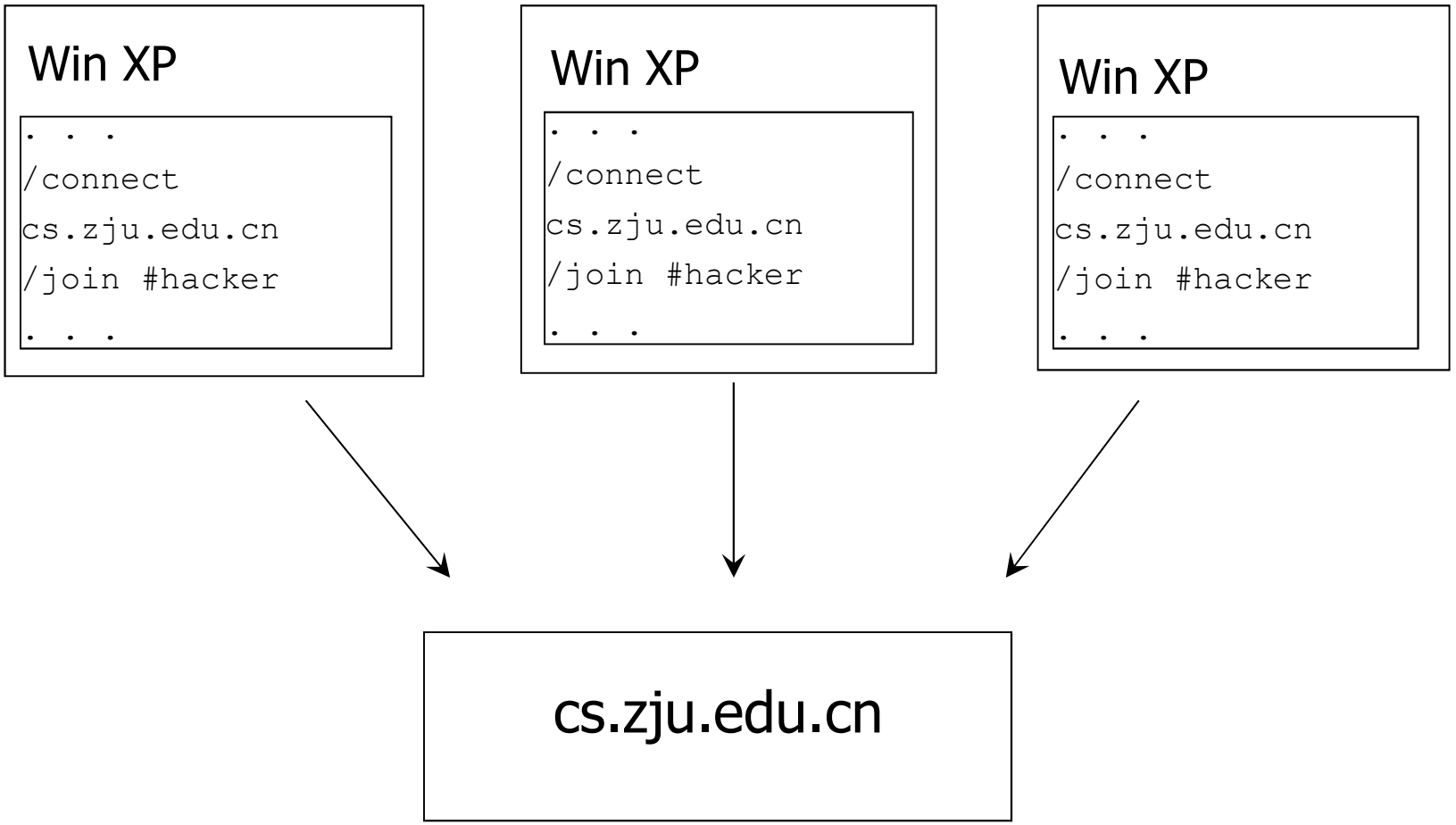
Typical Infection Path

- Exploit a vulnerability to execute a short program (shellcode) on victim's machine
  - Buffer overflows, email viruses, etc.
- Shellcode downloads and installs actual bot
- Bot disables firewall and antivirus software
- Bot locates IRC server, connects, joins channel
  - Typically need DNS to find out server's IP address
    - Especially if server's original IP address has been blacklisted
  - Authentication password often stored in bot binary
- Botmaster issues authenticated commands

Like an Army!

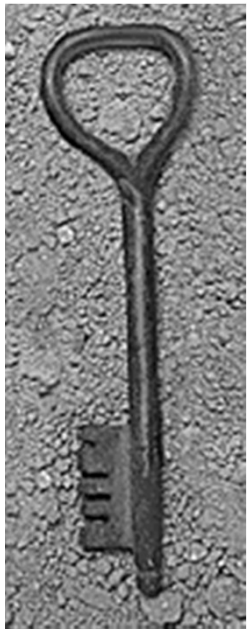


Joining the IRC Channel



Command and Control

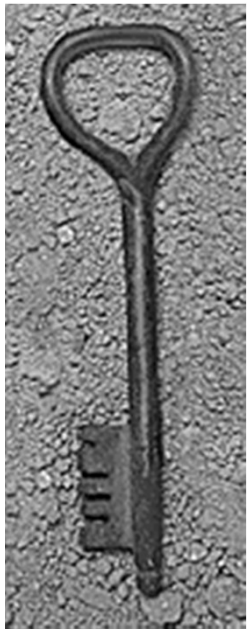
```
(12:59:27pm) -- A9-pcgbdv (A9-pcgbdv@140.134.36.124) has
joined (#owned) Users : 1646

(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 DOMAIN

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



Botnet Propagation

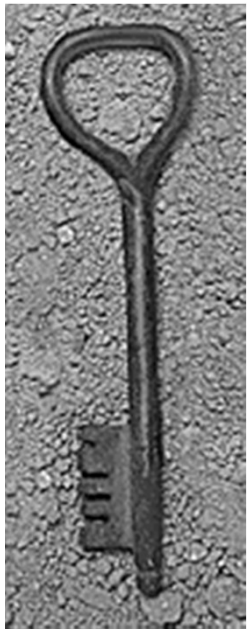
[Abu Rajab et al.]

- Each bot can scan IP space for new victims
  - Automatically
  - On-command: target specific /8 or /16 prefixes
    - Botmasters share information about prefixes to avoid
- Active botnet management
  - Detect non-responding bots, identify "superbots"
- Evidence of botnet-on-botnet warfare
  - DoS server by multiple IRC connections ("cloning")
  - N-to-N architecture, see the architecture in DDoS



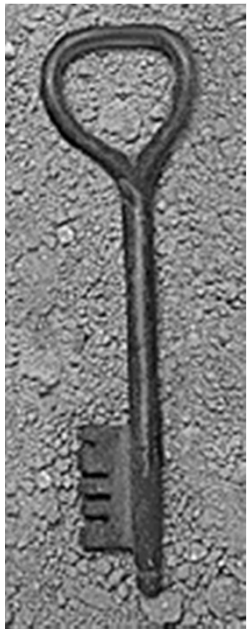
Denial of Service (DoS) Redux

- 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

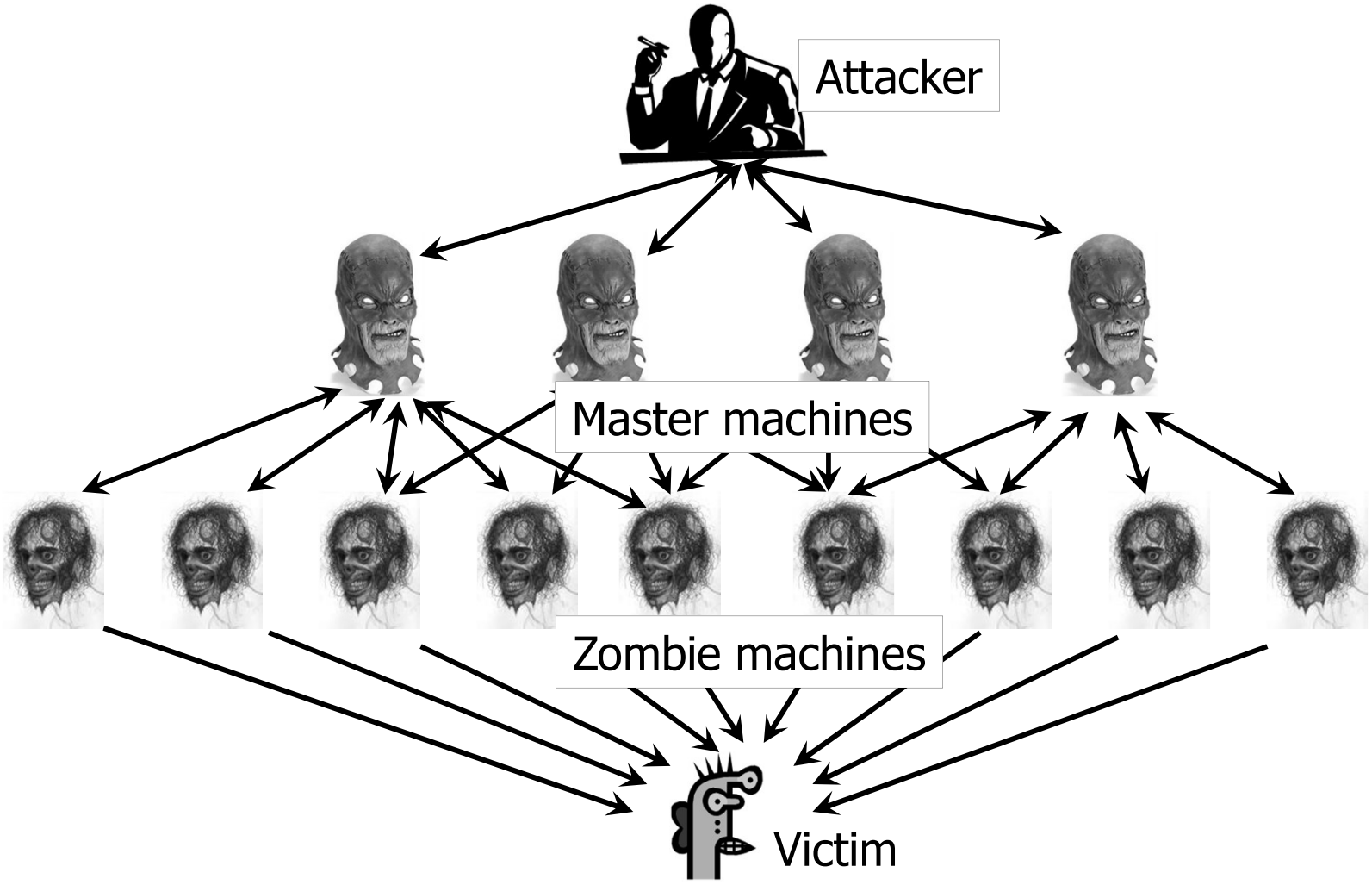


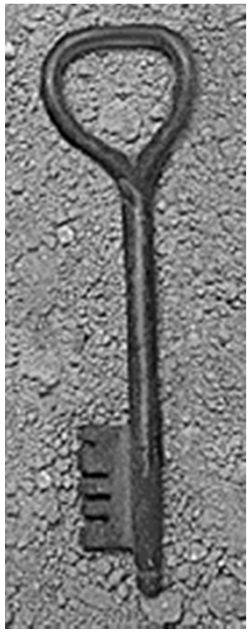
Distributed Denial of Service (DDoS)

- 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



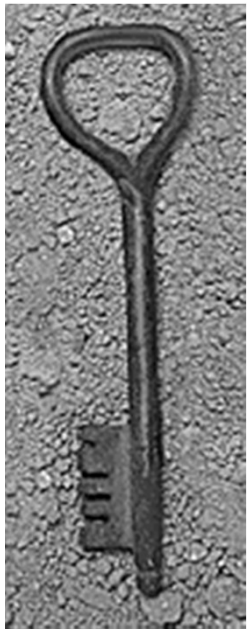
DDoS Architecture





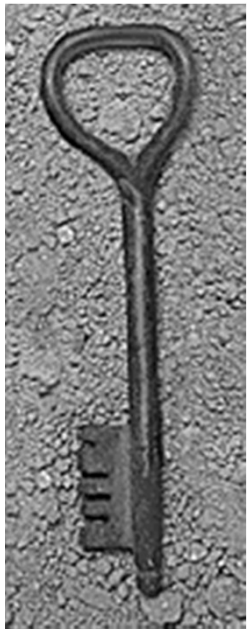
DDoS Tools: Trin00

- 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
- http://staff.washington.edu/dittrich/misc/trinoo.analysis



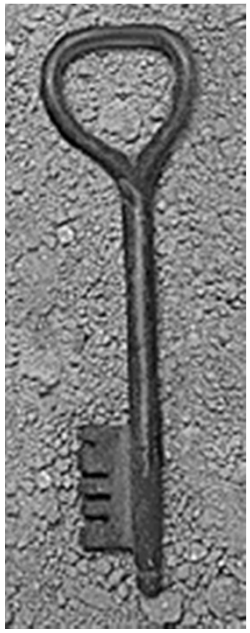
DDoS Tools: Tribal Flood Network

- 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
- http://staff.washington.edu/dittrich/misc/tfn.analysis

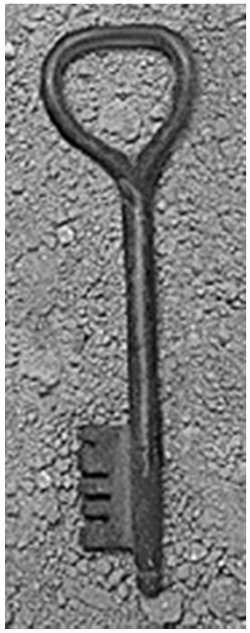


DDoS Tools: Stacheldraht

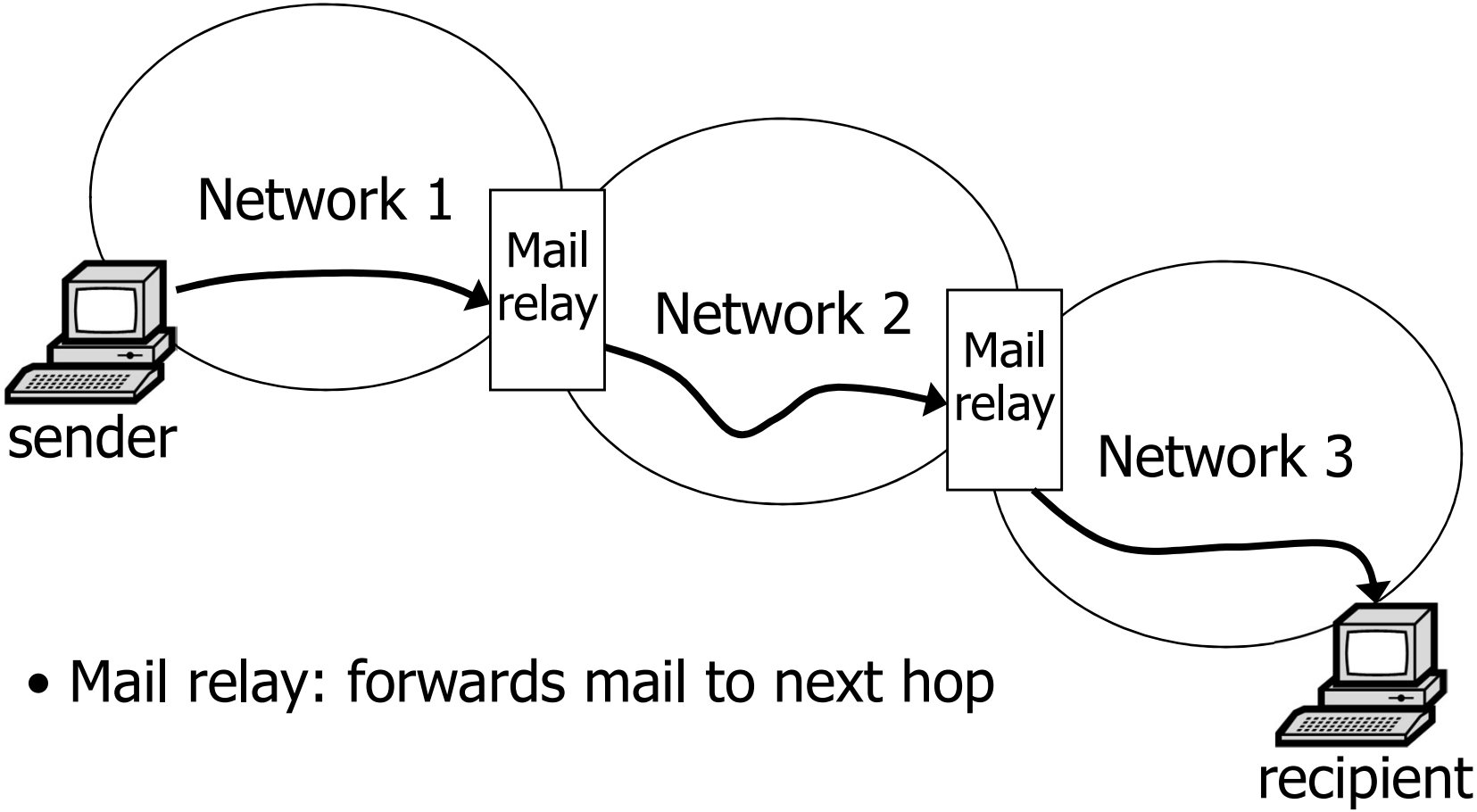
- Combines "best" features of Trin00 and TFN
  - Multiple attack types (like TFN)
- Symmetric encryption for attacker-master connections
- Master daemons can be upgraded on demand
- February 2000: crippled Yahoo, eBay, Amazon, Schwab, E*Trade, CNN, Buy.com, ZDNet
  - Smurf-like attack on Yahoo consumed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



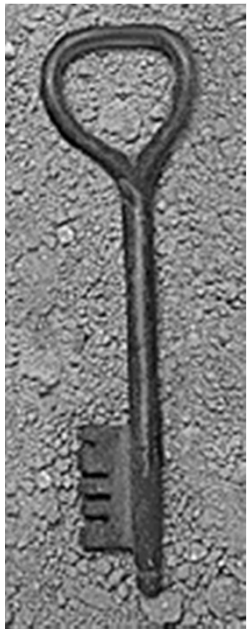
Spam



Email in the Early 1980s

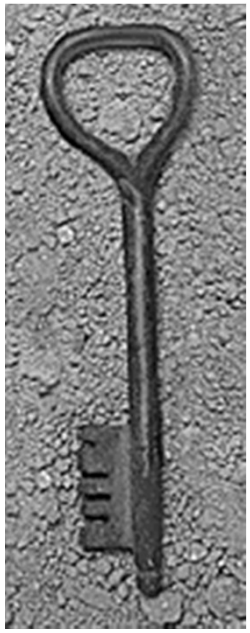


- Mail relay: forwards mail to next hop



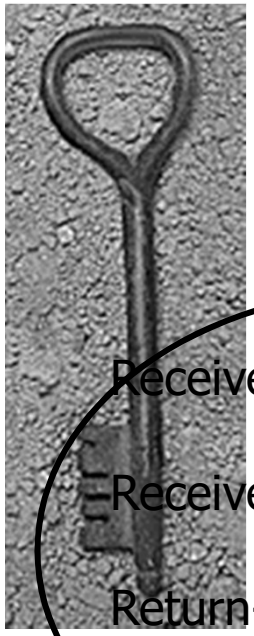
Email Spoofing

- 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

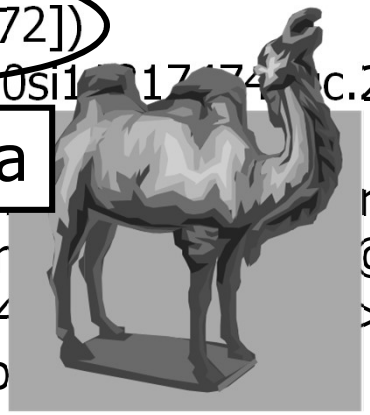
Inserted by relays

Bogus!

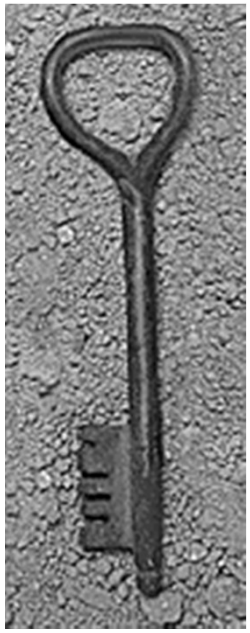
Received: by 10.78.68.6 [illegible] hua;
Mon, 12 Feb 2007 06:43:30 -0800 (PST)
Received: by 10 [illegible] MTP id l18mr17307116agc.1171291410432;
Mon [illegible] 43:30 -0800 (PST)
Return-Path: <[illegible]>
Received: from onelinkpr.net ([203.169.49.172])
by mx.google.com with ESMTP id 30si1[illegible]c.2007.02.12.06.43.18;
[illegible]

Puerto Rico

Mongolia

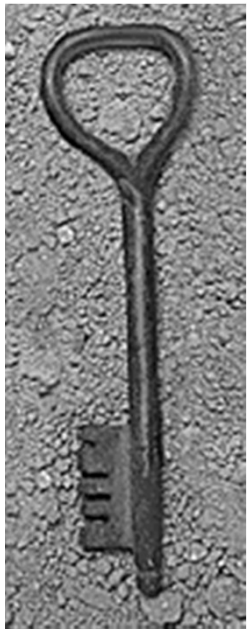


Rec[illegible]r permitted nor
[illegible]by best guess record for dor[illegible]@aviva.ro)
Mes[illegible]0050057765.stank.203.169.4[illegible]>
From: "Barclay Morales" <wvnlwee@aviva.ro
To: <raykwatts@gmail.com>
Subject: You can order both Viagra and Cialis.



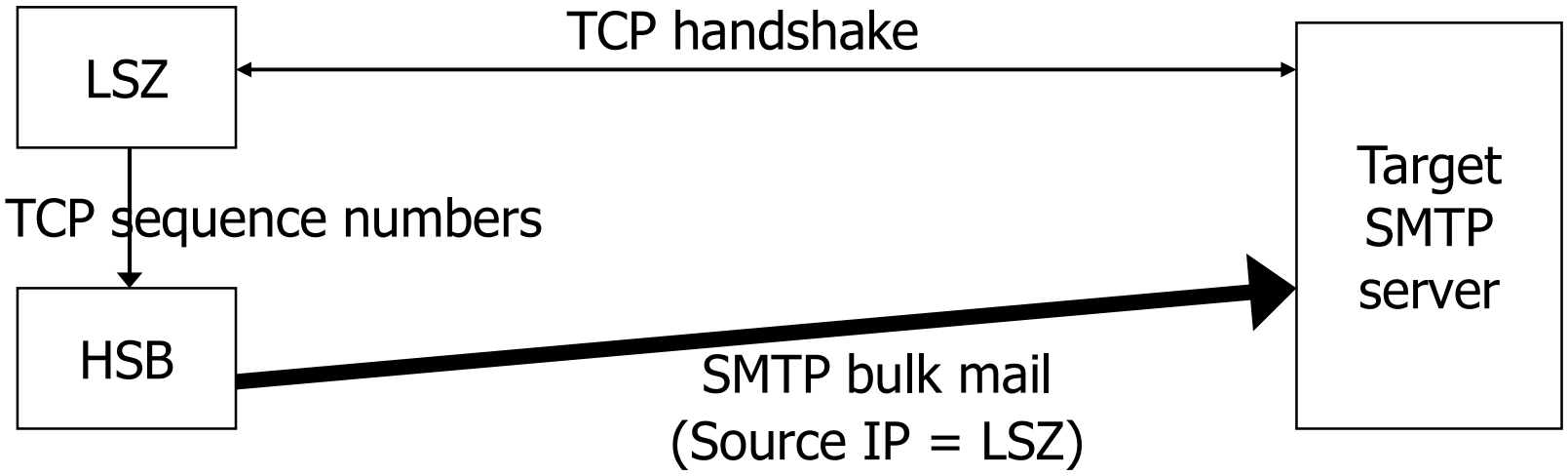
Why Hide Sources of Spam?

- Many email providers blacklist servers and ISPs that generate a lot of spam
  - Use info from spamhaus.org, spamcop.net
- Real-time blacklists stop 15-25% of spam at SMTP connection time
  - 85% after message body URI checks
- Spammers′ objective: evade blacklists
  - Botnets come very handy!

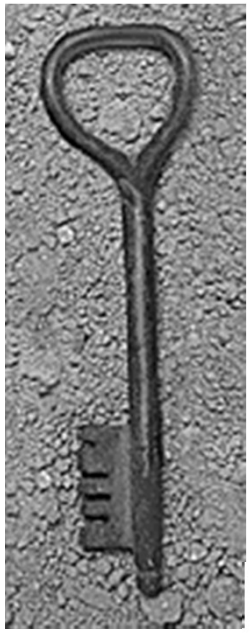


Thin Pipe / Thick Pipe

- Spam source has high-speed broadband machine (HSB) and controls a low-speed zombie (LSZ)

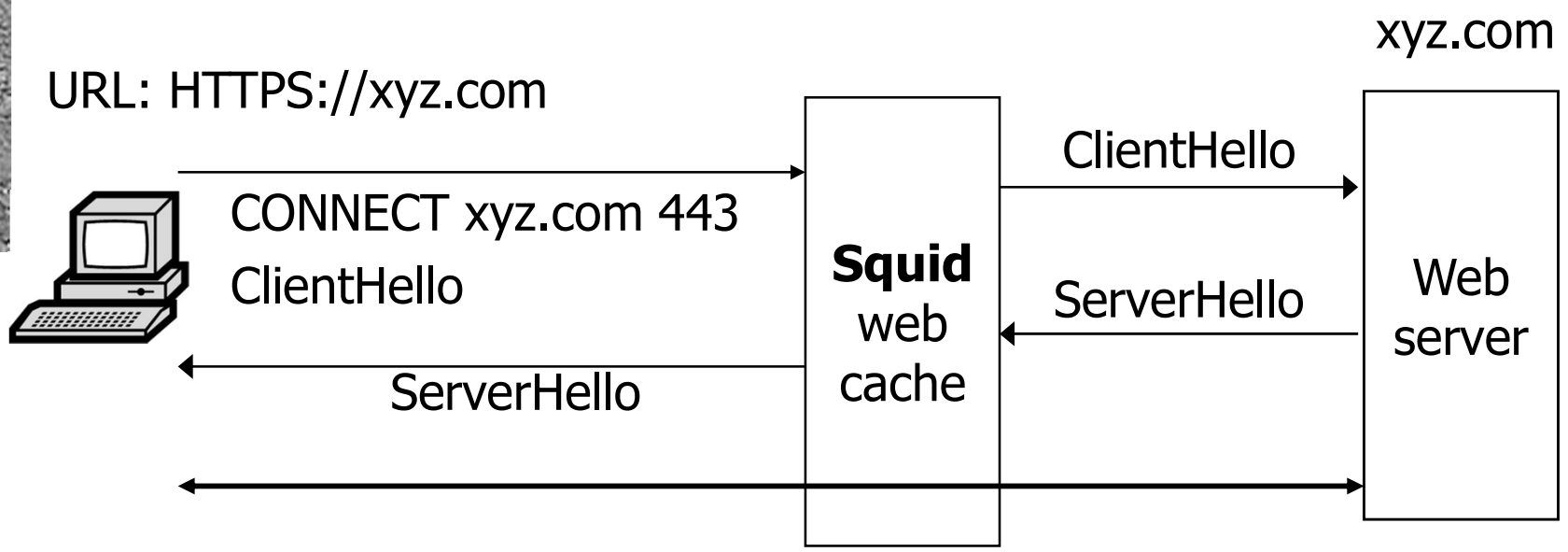


- Hides IP address of HSB; LSZ is blacklisted



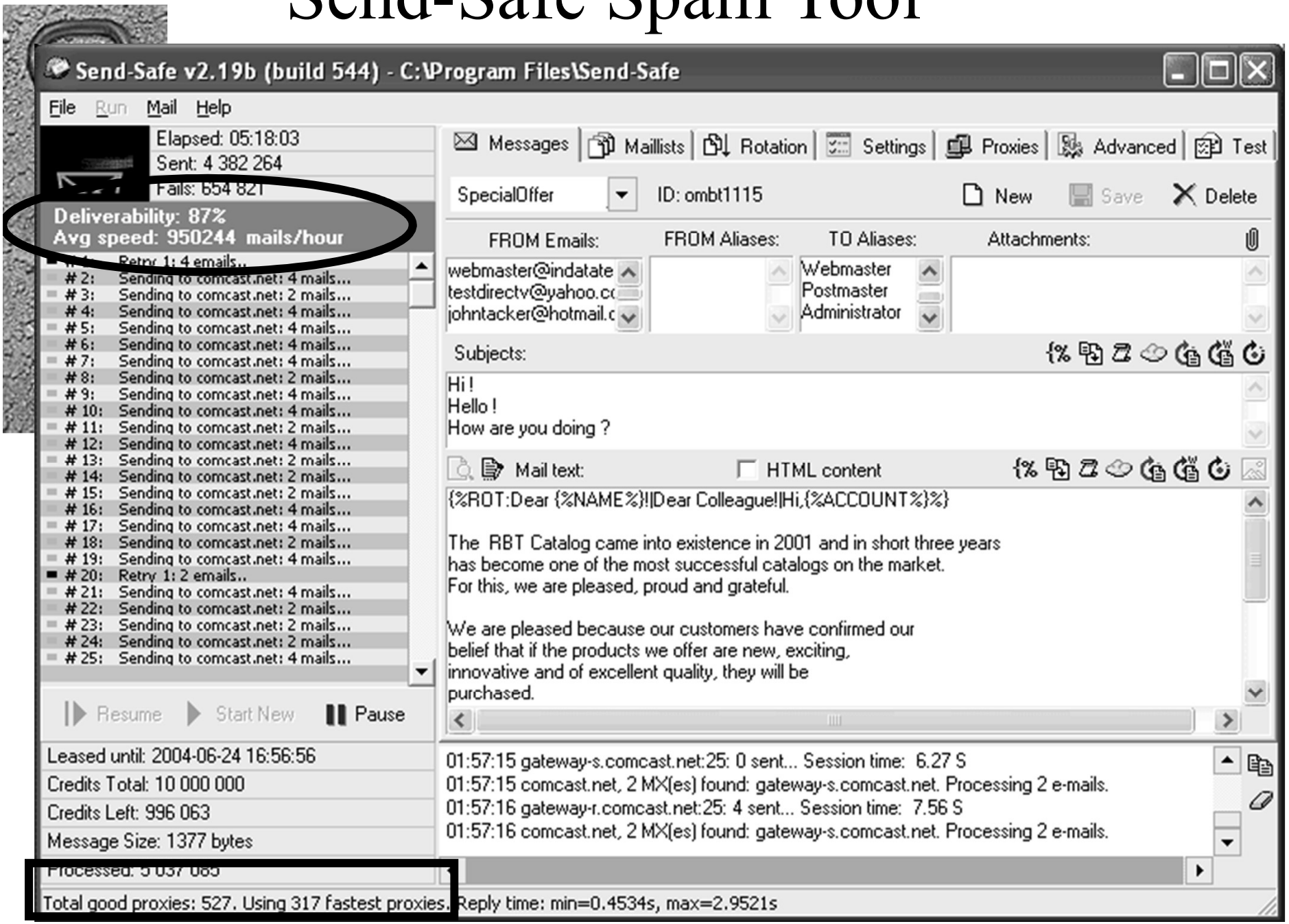
Open HTTP Proxies

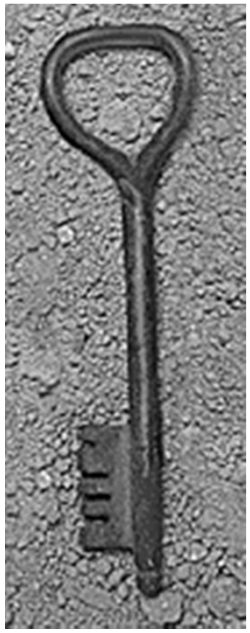
- Web cache (HTTP/HTTPS proxy), e.g., squid



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

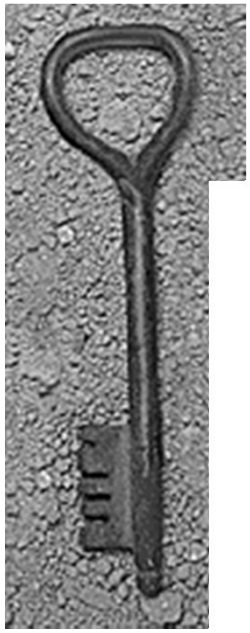
Send-Safe Spam Tool





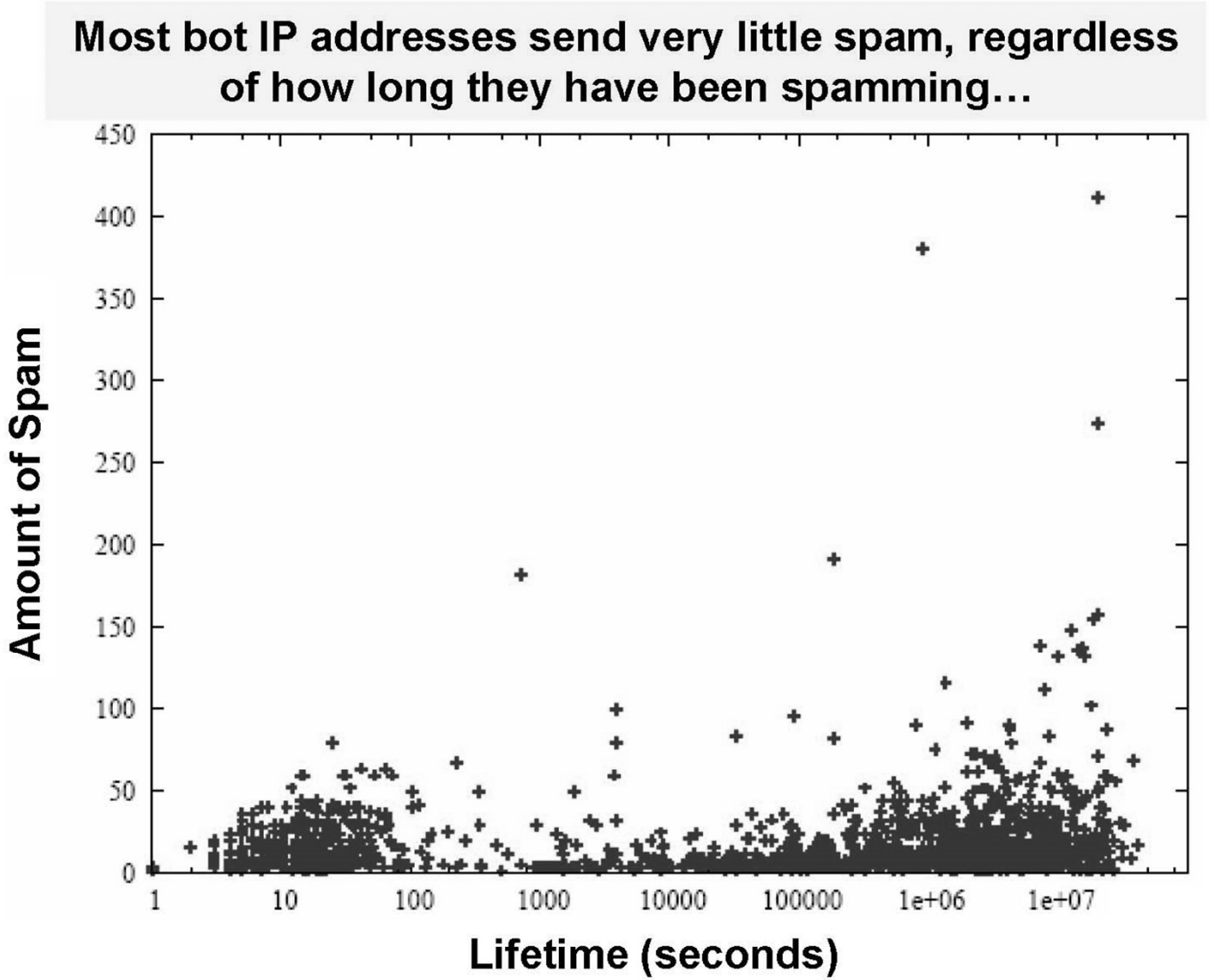
Bobax Worm

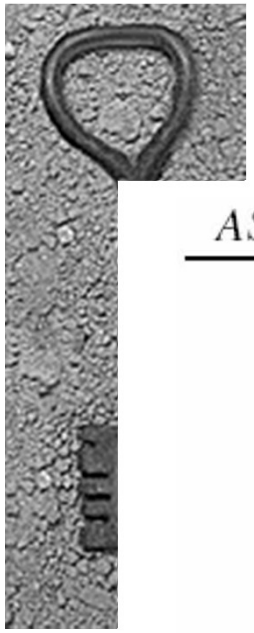
- Infects machines with high bandwidth
  - Exploits MS LSASS.exe buffer overflow vulnerability
- Slow spreading (and thus hard to detect)
  - On manual command from operator, randomly scans for vulnerable machines
- Installs hacked open relay on infected zombie
  - Once spam zombie added to blacklist,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



Most Bots Send Little Spam

[Ramachandran, Feamster]

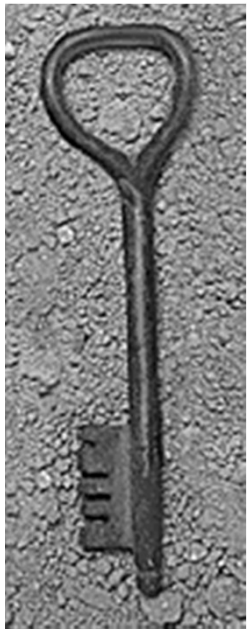




Distribution Across Domains

[Ramachandran, Feamster]

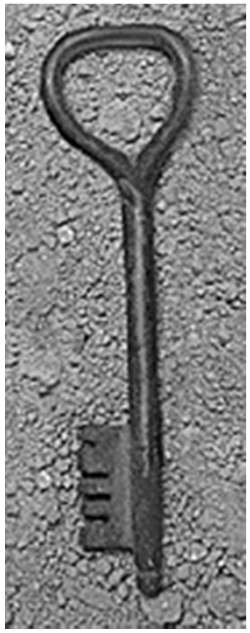
AS Number	*# Spam*	*AS Name*	*Primary Country*
766	580559	Korean Internet Exchange	Korea
4134	560765	China Telecom	China
1239	437660	Sprint	United States
4837	236434	China Network Communications	China
9318	225830	Hanaro Telecom	Japan
32311	198185	JKS Media, LLC	United States
5617	181270	Polish Telecom	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



Where Does Spam Come From?

[Ramachandran, Feamster]

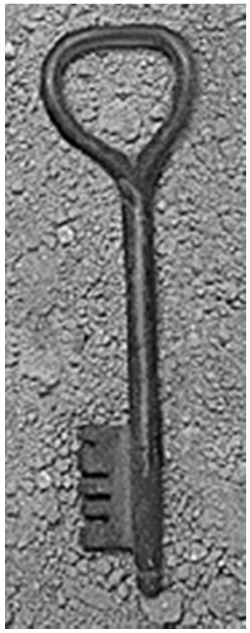
- IP addresses of spam sources are widely distributed across the Internet
  - In tracking experiments, most IP addresses appear once or twice; 60-80% not reachable by traceroute
- Vast majority of spam originates from a small fraction of IP address space
  - Same fraction that most legitimate email comes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



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
- Easily evaded by using encryption and P2P ☹