Information Systems Security (SOEN321)

Malware, Botnets, and Spam

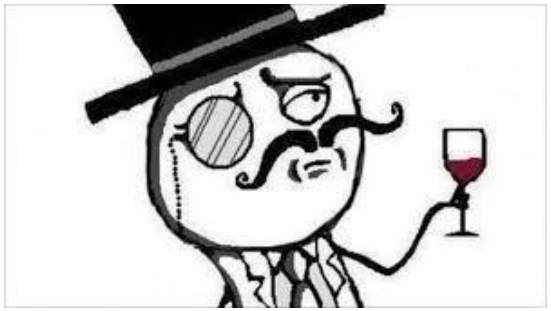
Note: Many of these slides are collected/modified from different books and online resources

Motivation

- Internet currently used for important services
  - Financial transactions, medical records
- Increasingly used for critical services
  - Surgical operations, CPSs (water/electrical system control, remote controlled drones)
- Networks more open than ever before
  - Global, ubiquitous Internet, wireless

Malicious Users

- Miscreants, e.g. LulzSec
  - In it for thrills, street cred, or just to learn
  - Defacing web pages, spreading viruses, etc.
- Hacktivists, e.g. Anonymous
  - Online political protests
  - Stealing and revealing classified information
- Organized Crime
  - Profit driven, online criminals
  - Well organized, divisions of labor, highly motivated



Network Security Problems

- Host Compromise
  - Attacker gains control of a host
  - Can then be used to try and compromise others
- Denial-of-Service
  - Attacker prevents legitimate users from gaining service
- Attack can be both
  - E.g., host compromise that provides resources for denial-of-service

Definitions

- Virus
  - Program that attaches itself to another program
- Worm
  - Replicates itself over the network
  - Usually relies on remote exploit (e.g. buffer overflow)
- Rootkit
  - Program that infects the operating system
  - Used for privilege elevation, and to hide files/processes
- Trojan horse
  - Program that opens “back doors” on an infected host
  - Gives the attacker remote access to machines
- Botnet
  - A large group of Trojaned machines, controlled en-mass
  - Used for sending spam, DDoS, click-fraud, etc.

Host Compromise

- One of earliest major Internet security incidents
  - Internet Worm (1988): compromised almost every BSD-derived machine on Internet
- Today: estimated that a single worm could compromise 10M hosts in < 5 min
- Attacker gains control of a host
  - Read data
  - Erase data
  - Compromise another host
  - Launch denial-of-service attacks on another host

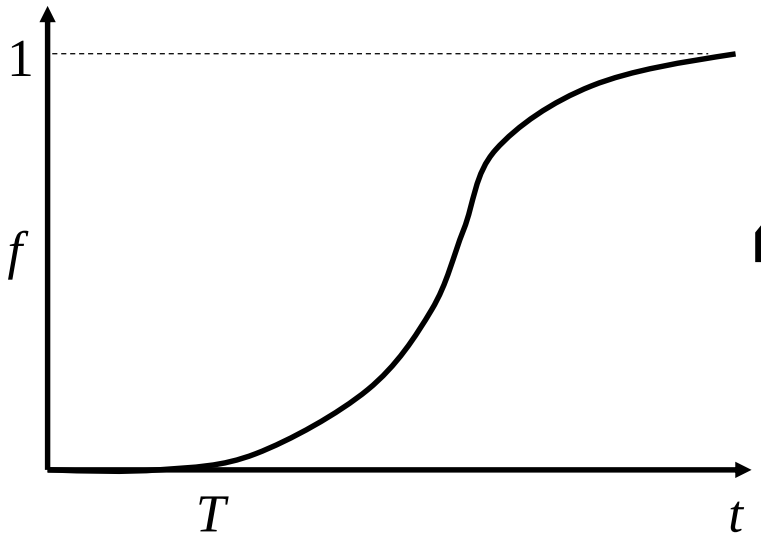
Host Compromise

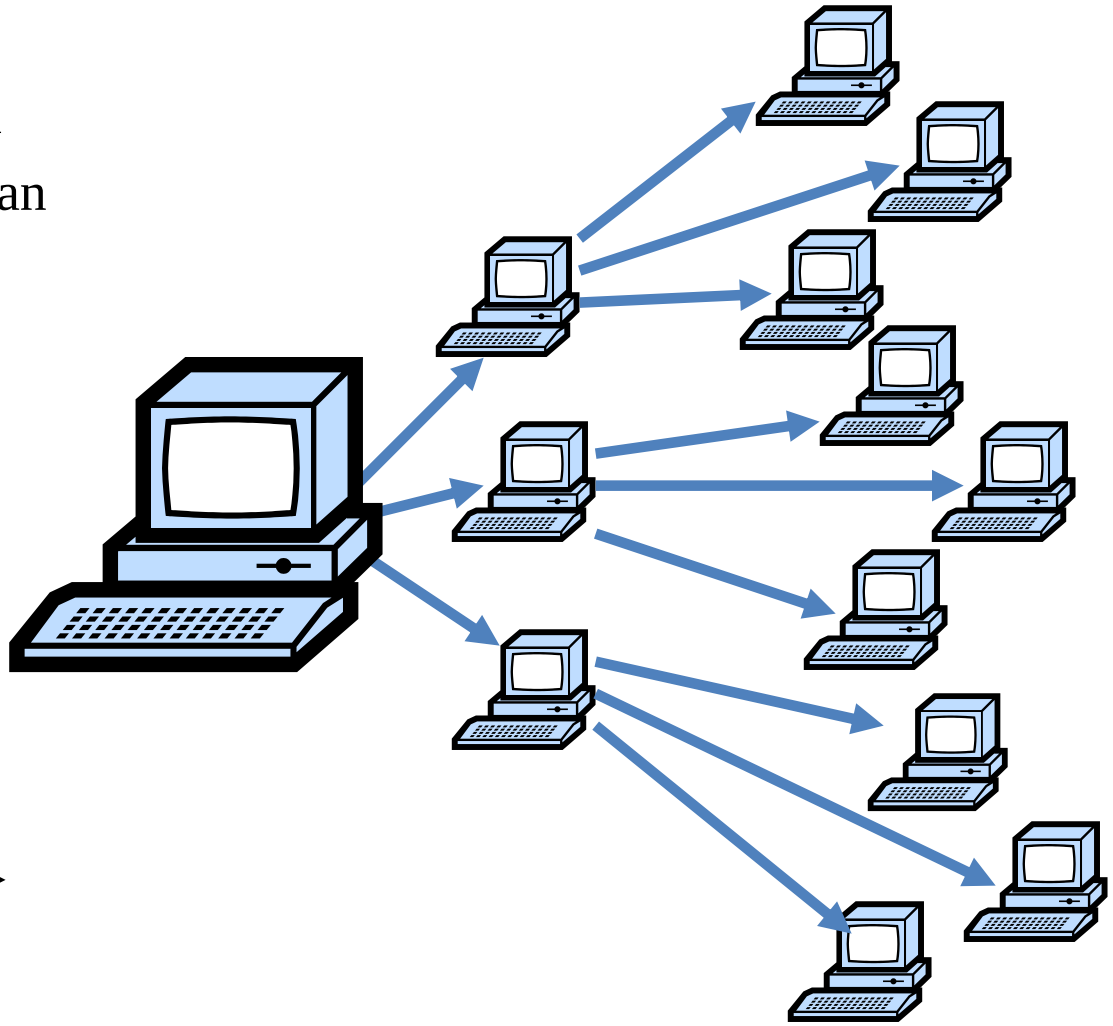
- Typical code has many bugs; those bugs are usually not triggered by common input
- Network code is vulnerable because it accepts input from the network
- Network code that runs with high privileges (i.e., as root) is especially dangerous
  - E.g., web server

Worm Spreading

$f = (e^{K(t-T)} - 1) / (1 + e^{K(t-T)})$

- f – fraction of hosts infected
- K – rate at which one host can compromise others
- T – start time of the attack





Worm (Historical Examples)

- Morris worm (1988)
- Code Red (2001)
- MS Slammer (January 2003)
- MS Blaster (August 2003)

Morris Worm (1988)

- Written by a graduate student at Cornell University, Robert Tappan Morris, and launched on November 2, 1988 from MIT.
- Infect multiple types of machines (Sun 3 and VAX)
  - Spread using a Sendmail bug
- Attack multiple security holes including
  - Buffer overflow in fingerd
  - Debugging routines in Sendmail
  - Password cracking
- Intend to be benign but it had a bug
  - number of worm on a host built up rendering the machine unusable

Code Red Worm (2001)

- Attempts to connect to TCP port 80 on a randomly chosen host
- If successful, the attacking host sends a crafted HTTP GET request to the victim, attempting to exploit a buffer overflow
- Worm “bug”: all copies of the worm use the same random seed to scanning new hosts
  - DoS attack on those hosts
  - Slow to infect new hosts
- 2nd generation of Code Red fixed the bug!
  - It spread much faster

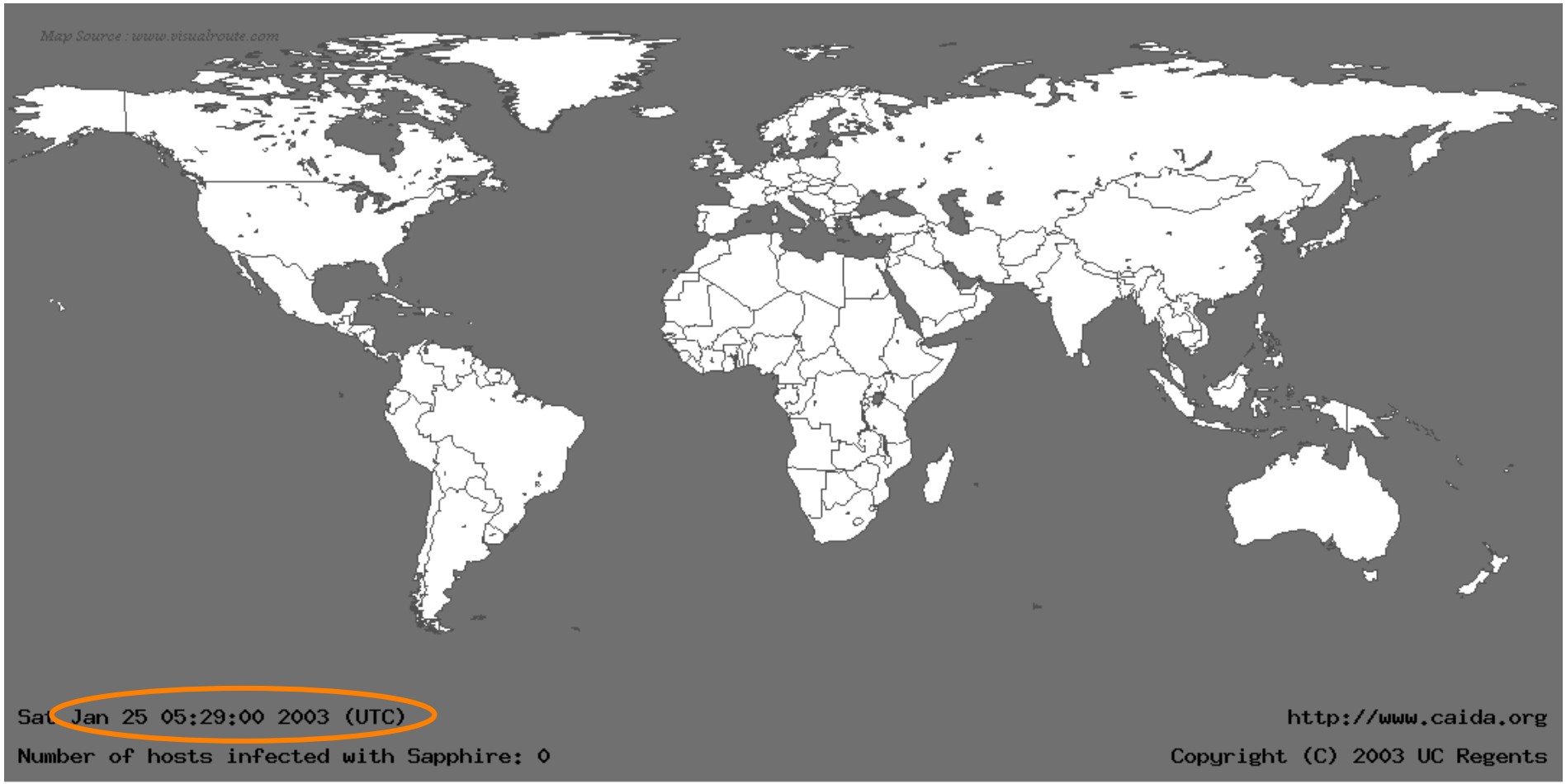
MS SQL Slammer (January 2003)

- Uses UDP port 1434 to exploit a buffer overflow in MS SQL server
  - Generate massive amounts of network packets
  - Brought down as many as 5 of the 13 internet root name servers
- Stealth Feature
  - The worm only spreads as an in-memory process: it never writes itself to the hard drive
    - Solution: close UDP port on firewall and reboot

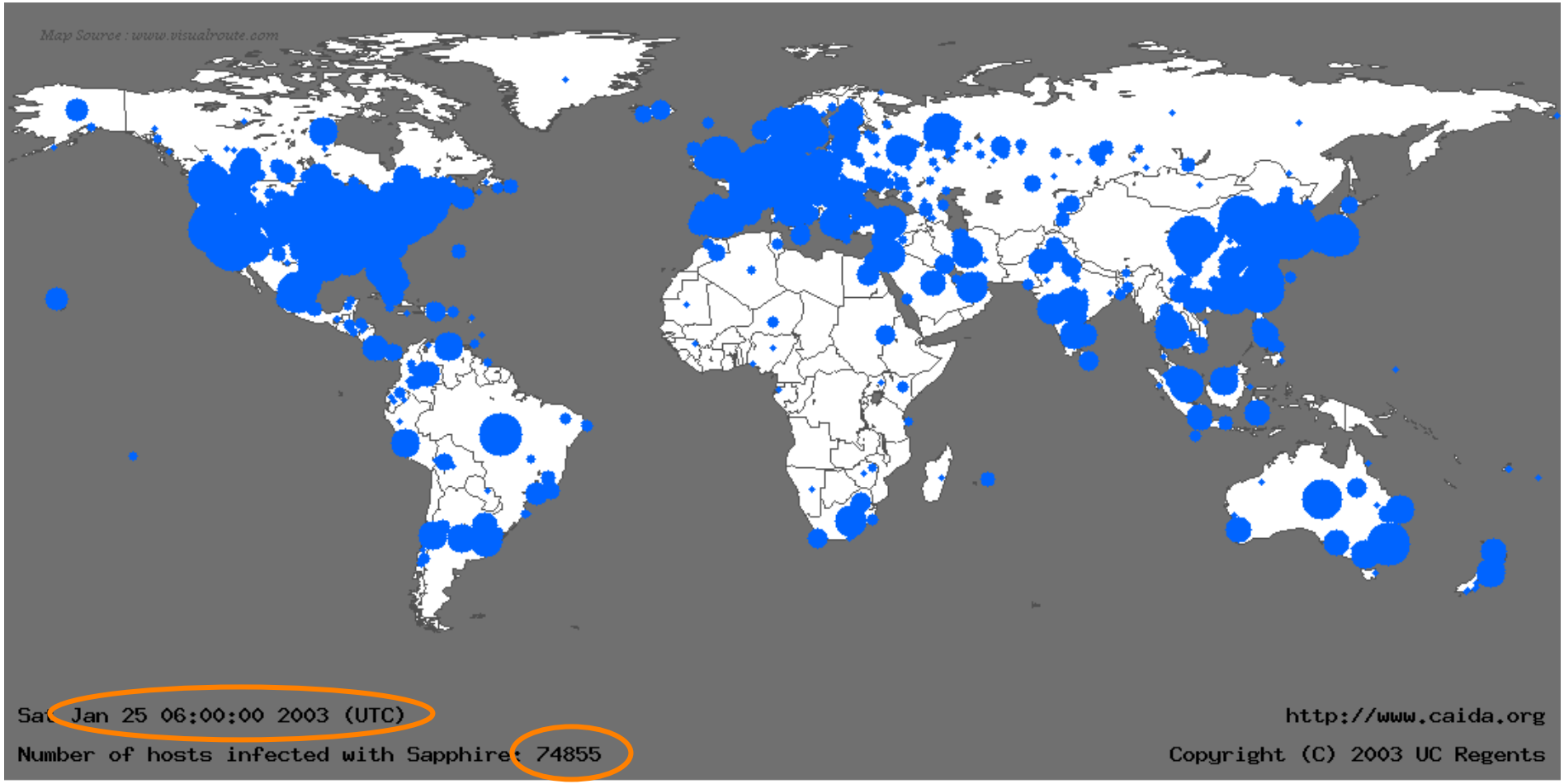
MS SQL Slammer (January 2003)

- Slammer exploited a connectionless UDP service, rather than connection-oriented TCP.
  - Entire worm fit in a single packet!
- Worm infected 75,000+ hosts in 10 minutes (despite broken random number generator).
  - At its peak, doubled every 8.5 seconds
- Progress limited by the Internet's carrying capacity!

Life Just Before Slammer



Life Just After Slammer



Spreading Faster

- Idea 1: *Reduce Redundant Scanning*
  - Construct permutation of address space.
  - Each new worm instance starts at random point
  - Worm instance that "encounters" another instance re-randomizes
- Idea 2: *Reduce Slow Startup Phase*
  - Construct a "hit-list" of vulnerable servers in advance
  - Assume 1M vulnerable hosts, 10K hit-list, 100 scans/worm/sec, 1 sec to infect
    - 99% infection rate in 5 minutes

Spreading Even Faster — Flash Worms

- Idea: use an *Internet-sized* hit list.
  - Initial copy of the worm has the entire hit list
  - Each generation…
    - Infect *n* hosts from the list
    - Give each new infection 1/*n* of the list
  - ~10 seconds to infect the whole Internet

Incidental Damage … Today

- Worms have significant real-world impact:
  - Code Red disrupted routing
  - Slammer disrupted root DNS, elections, ATMs, airlines, operations at an off-line nuclear power plant …
  - Blaster possibly contributed to Great Blackout of Aug. 2003 … ?
  - Plus major clean-up costs
- But most worms are amateurish

Next-Generation Worm Authors

- Military (e.g. Stuxnet)
  - Worm spread in 2010 (believed to be developed by US/Israel)
  - Targets Siemens industrial (SCADA) systems
  - Target: Iranian uranium enrichment infrastructure
- Crooks:
  - Very worrisome onset of blended threats
    - Worms + viruses + spamming + phishing + DOS-for-hire + botnets + spyware
  - Money on the table → **arms race**
    - (market price for spam proxies: 3-10¢/host/week)

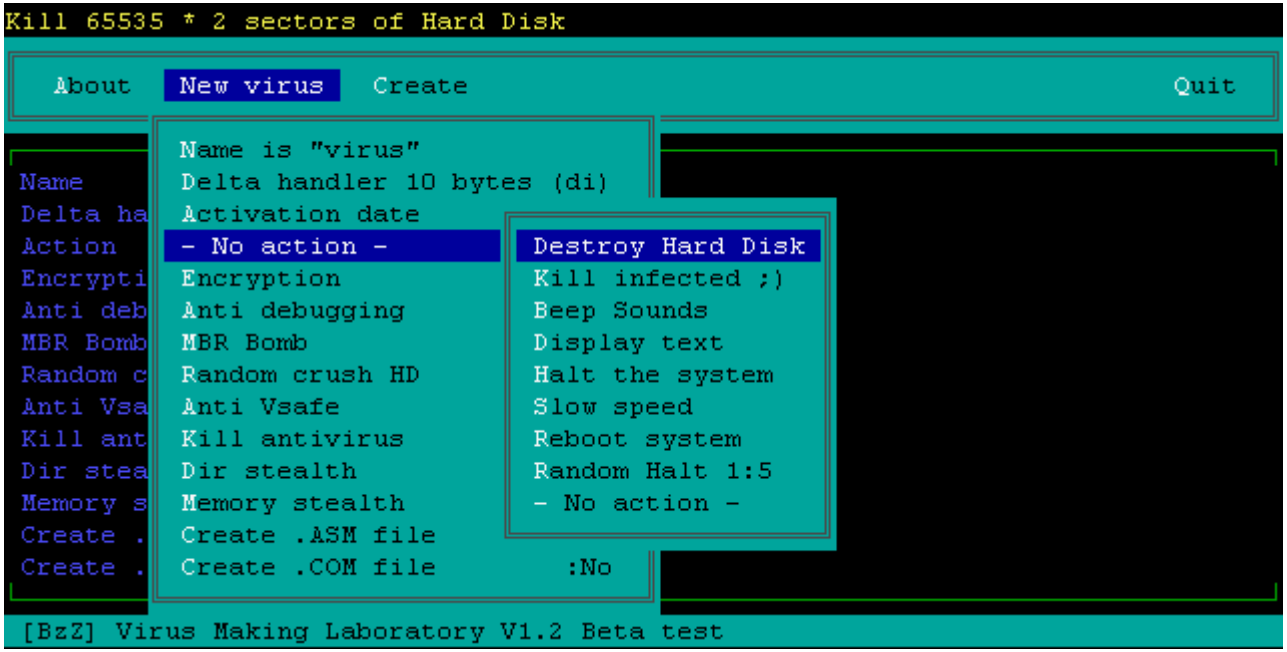
Shamoon

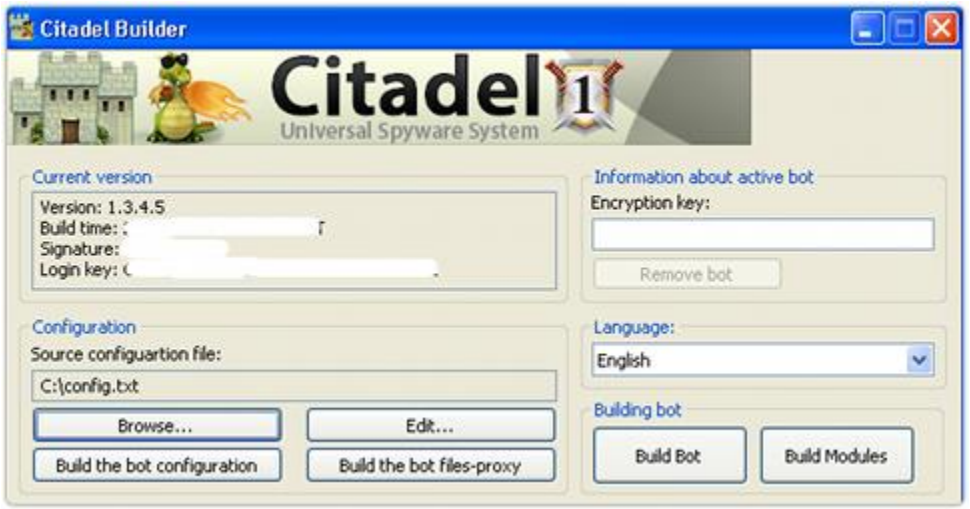
- Found August 16, 2012
- Targeted computers from Saudi Aramco
  - Largest company/oil producer in the world
- Infected 30,000 desktop machines
  - Took one week to clean and restore
- Could have been much worse
  - Attack was not stealthy
    - Stolen data slowly over time
    - Slowly corrupt random disk blocks, spreadsheets, etc.
  - Did not target SCADA or production control systems

Threat Detection

- Both defense and deterrence are predicated on getting *good intelligence*
  - Need to detect, characterize and analyze new malware threats
  - Need to be do it quickly across a very large number of events
- Classes of monitors
  - Network-based
  - Host/Endpoint-based
- Monitoring environments
  - In-situ: real activity as it happens
    - Network/host IDS
  - Ex-situ: “canary in the coal mine”
    - HoneyNets/Honeypots

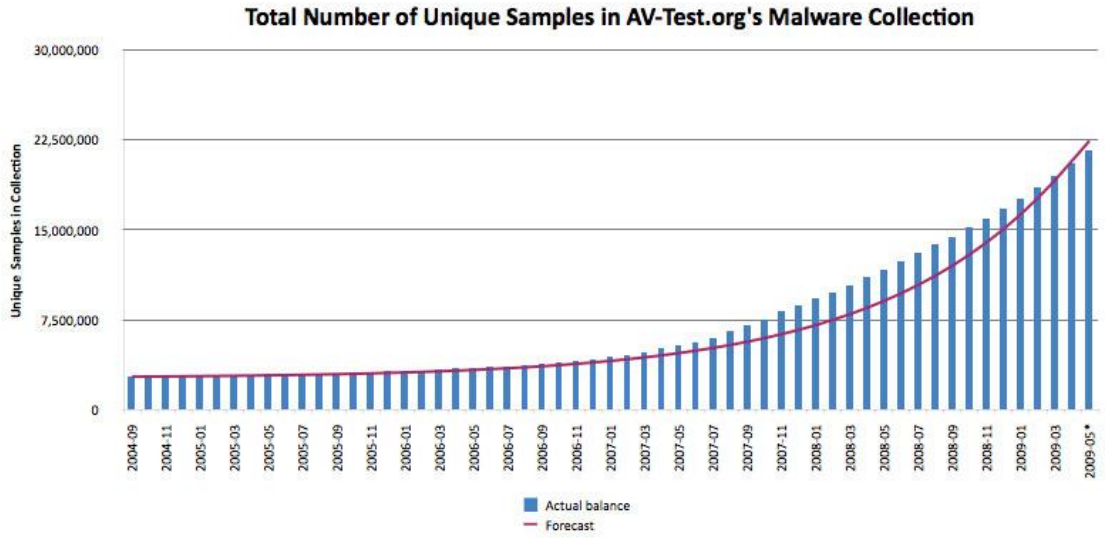
Challenges (Malware Automation)

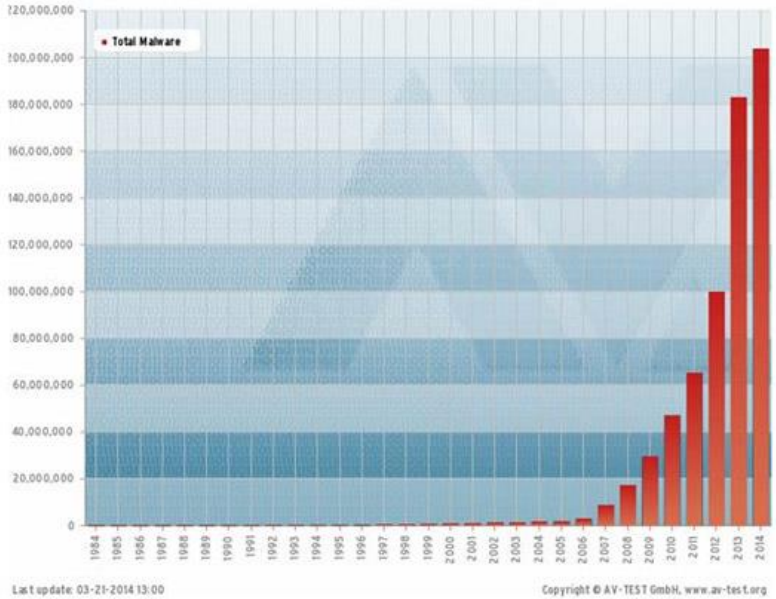


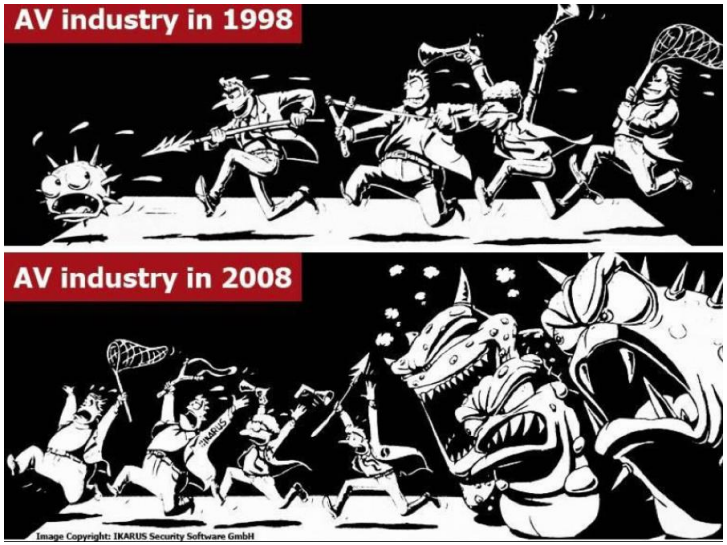


"Quality assurance"
Is achieved through a suit of MultiAV scan Tools (e.g., Virustotal, novirusthanks) after subjecting the automatically generated samples to ***Armoring* tools** (these tools also provides the malware with
-Anti-debugging
- Anti-Sandboxing)

Challenges (Malware Automation)







Static versus Dynamic Analysis

Static approaches

+ Complete analysis

- Difficult to extract semantics

- Obfuscation / packing

Dynamic approaches

+ Easy to see “behaviors”

+ Malware unpacks itself

- “Dormant” code

More Defensive Strategies

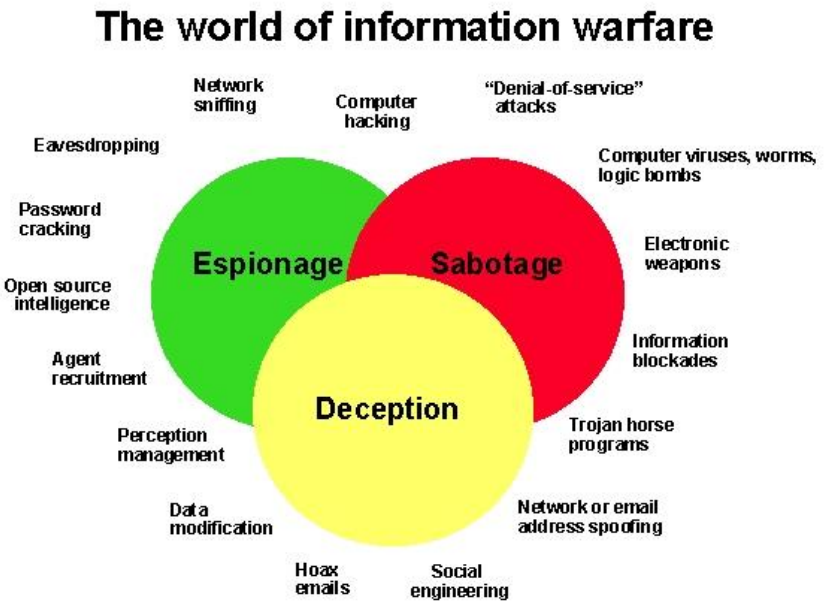
- Host-based security
  - Tools for hardening software
    - Static and dynamic analysis, taint tracking
    - Address space layout randomization
    - Sandboxing and virtualization

Worms to Botnets

- Ultimate goal of most Internet worms
  - Compromise machine, install rootkit, then trojan
  - One of many in army of remote controlled machines
- Used by online criminals to make money
  - Extortion
    - "Pay use $100K or we will DDoS your website"
  - Spam and click-fraud
  - Phishing and theft of personal information
    - Credit card numbers, bank login information, etc.

Botnet Attacks

- Truly effective as an online weapon for terrorism
  - i.e. perform targeted attacks on governments and infrastructure
- Recent events: massive DoS on Estonia
  - April 27, 2007 – Mid-May, 2007
  - Closed off most government and business websites
  - Attack hosts from US, Canada, Brazil, Vietnam, …
  - Web posts indicate attacks controlled by Russians
  - All because Estonia moved a memorial of WWII soldier
- Is this a glimpse of the future?
  - information warfare

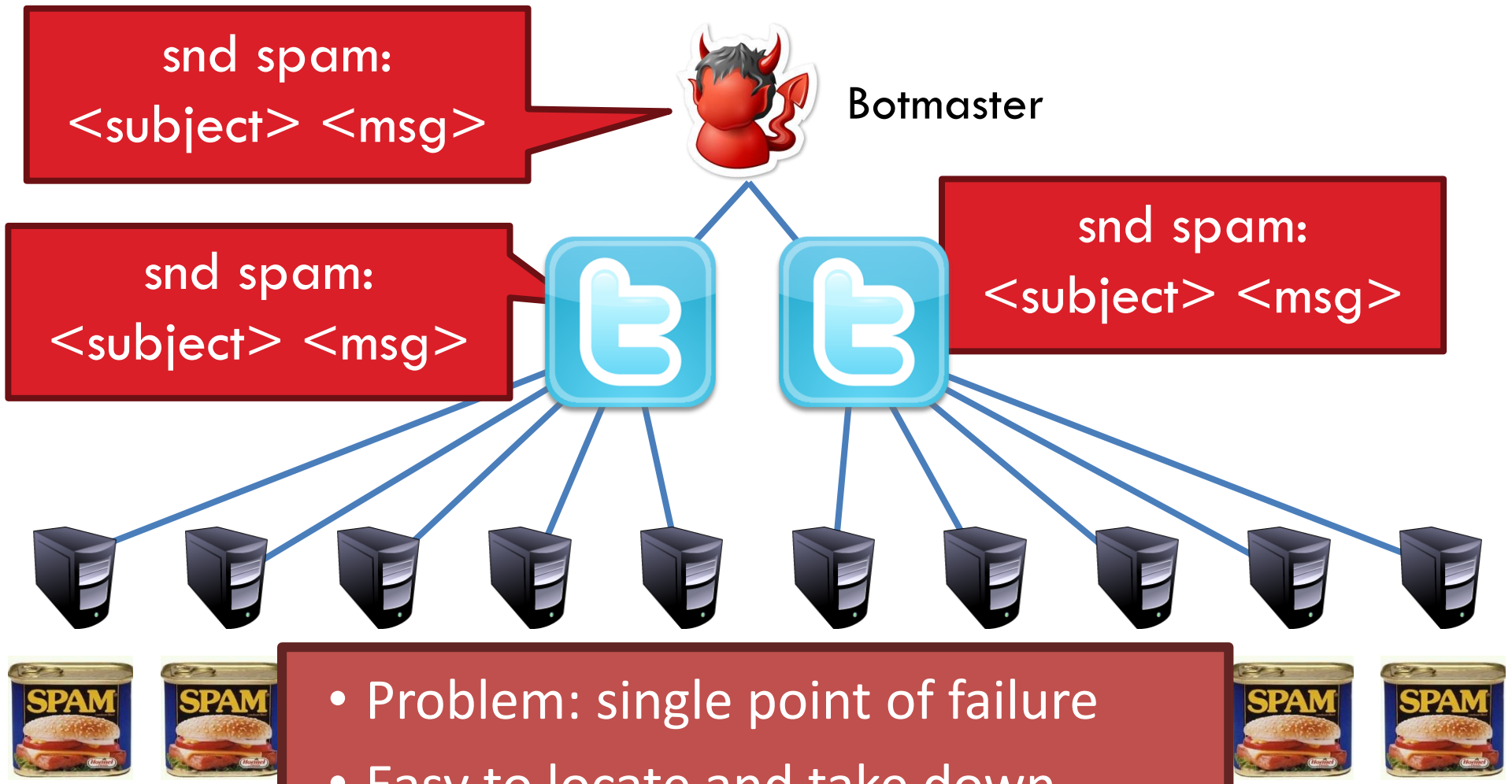



1
2
OK
3
$
4

Detecting / Deterring Botnets

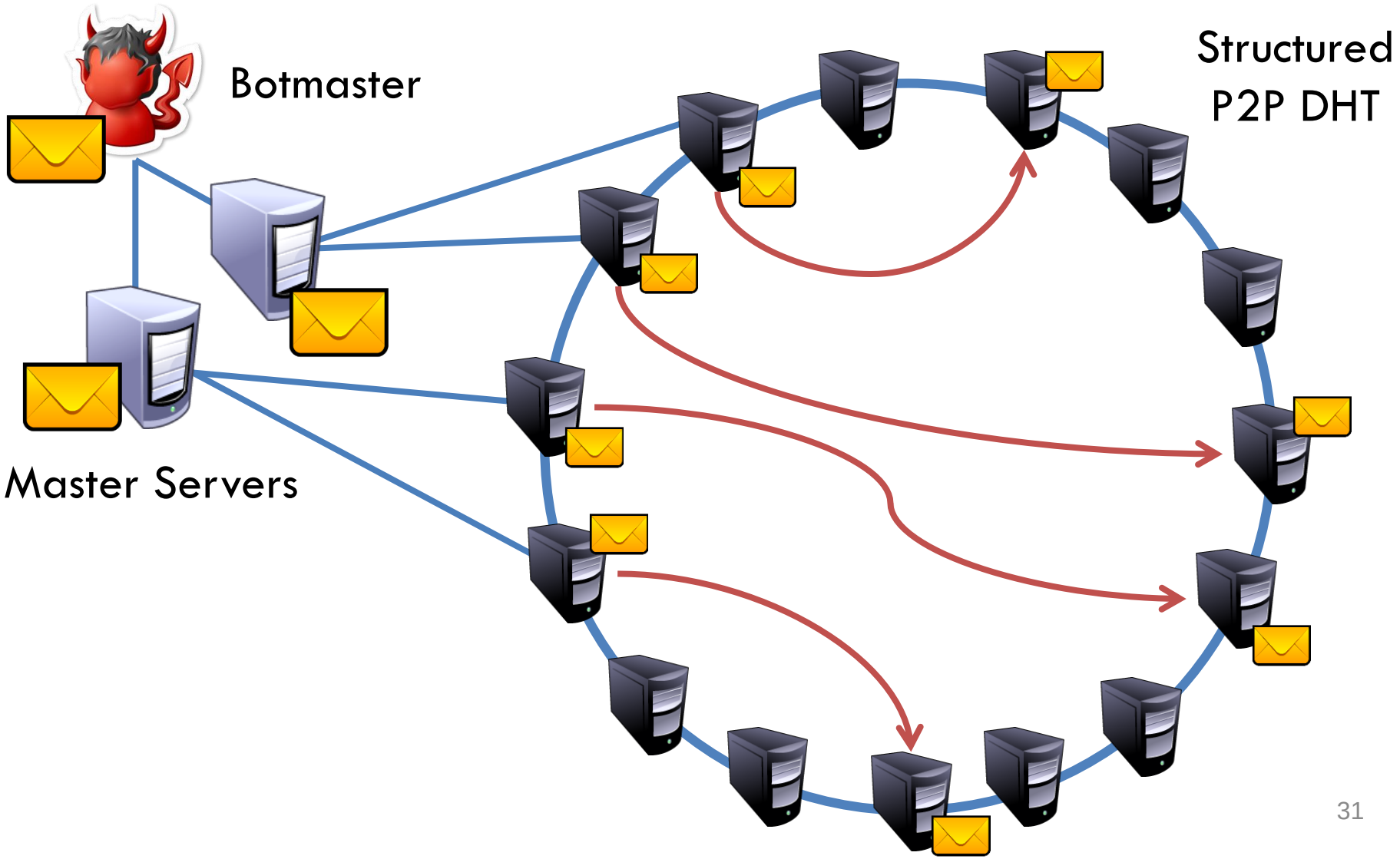
- Bots controlled via C&C channels
  - Potential weakness to disrupt botnet operation
  - Traditionally relied on IRC channels run by ephemeral servers (Now mostly use HTTP instead of IRC)
    - Can rotate single DNS name to different IPs on minute-basis
  - Can be found by mimicing bots (using honeypots)
- Bots also identified via DNS blacklist requests
- A constant cat and mouse game
  - Attackers evolving to decentralized C&C structures
  - Peer to peer model, encrypted traffic
  - Storm botnet, estimated 1-50 million members in 9/2007
- Utilizes 3 network resources Domains (Can be one or separate)
  - C&C
  - Domain Drop Zone
  - Malware serving domains (updates)

Old-School C&C: IRC Channels

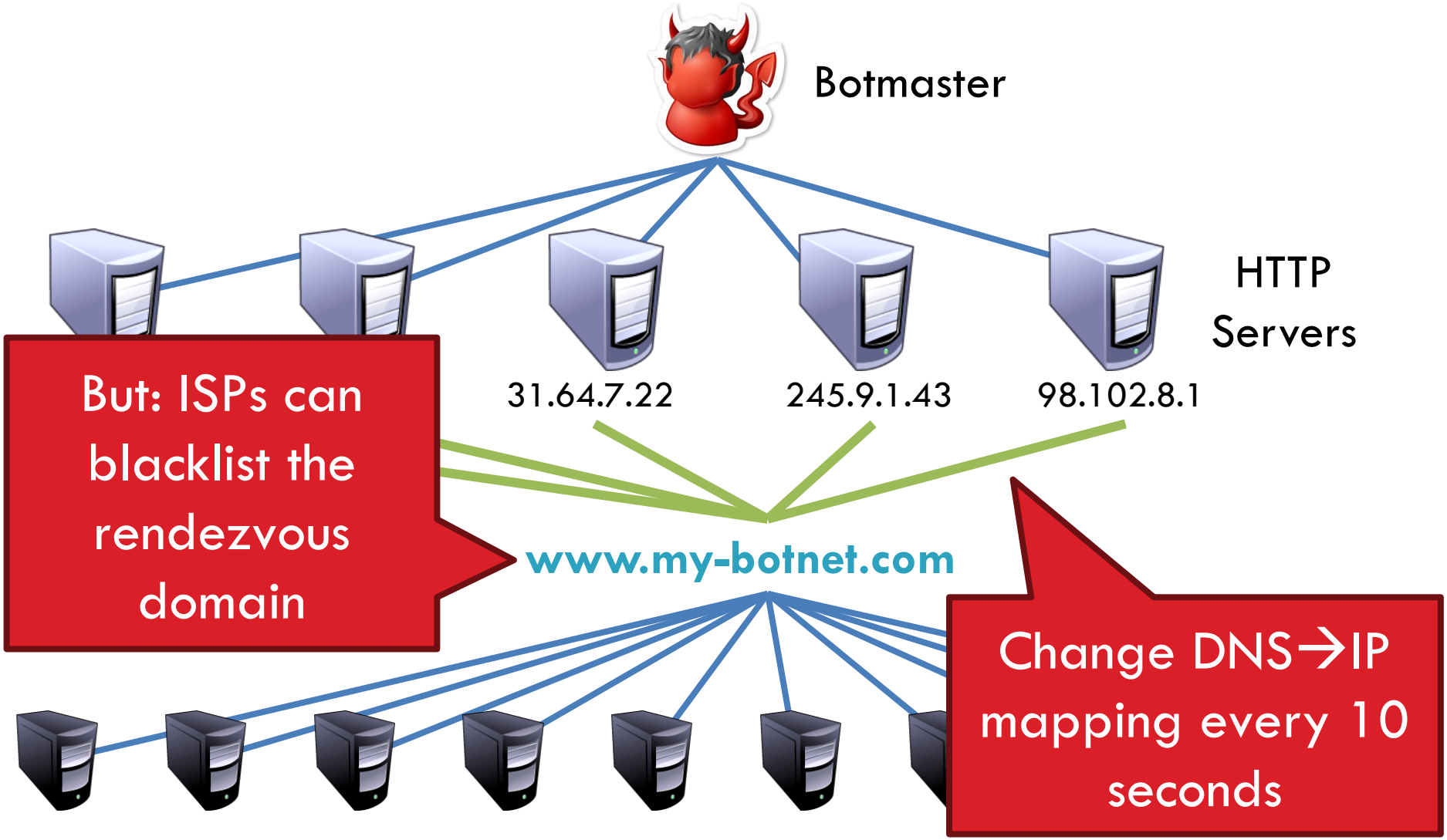


- Problem: single point of failure
- Easy to locate and take down

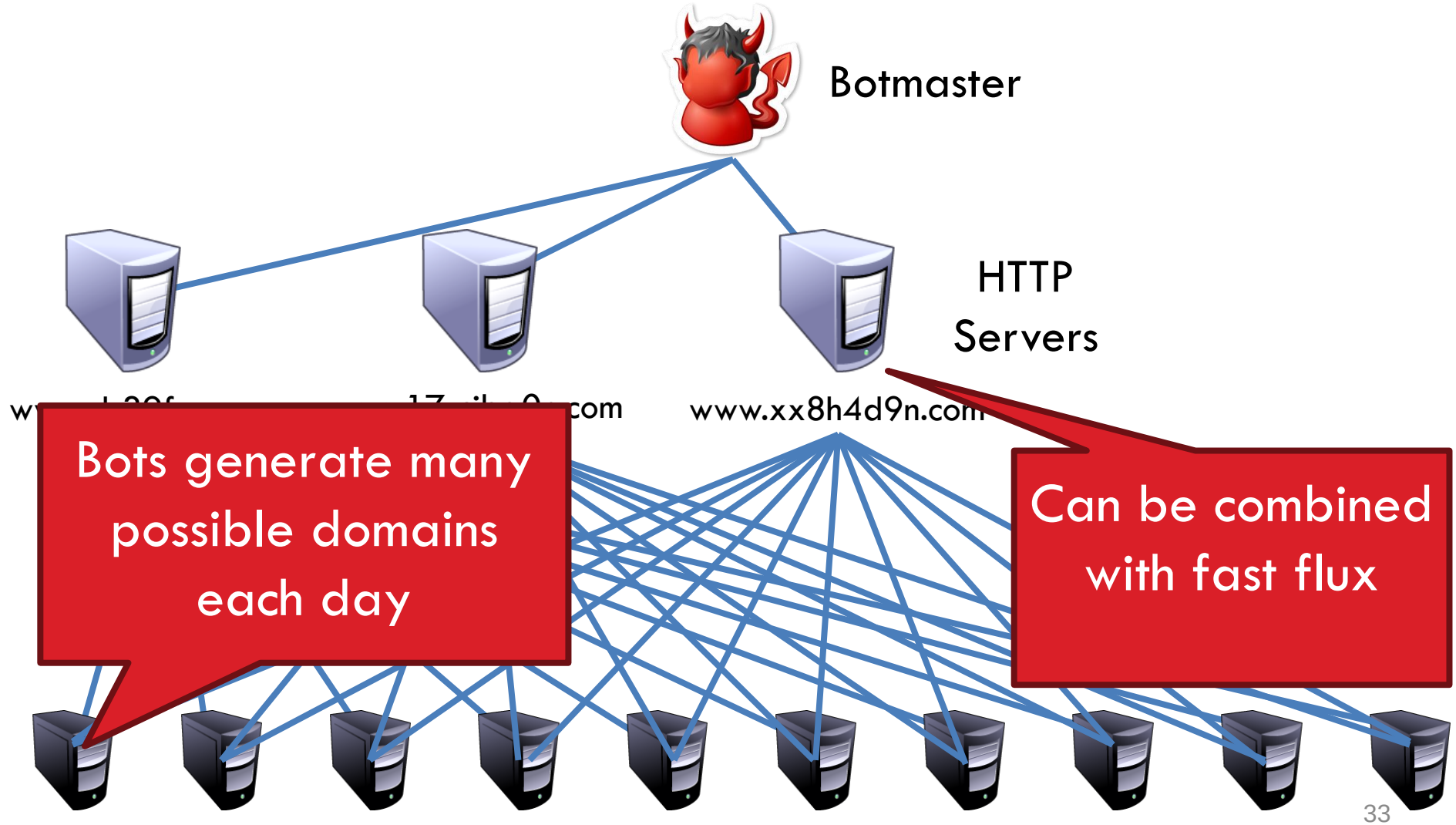
P2P Botnets



Fast Flux DNS



Random Domain Generation



“Your Botnet is My Botnet”

- Takeover of the Torpig botnet
  - Random domain generation + fast flux
  - Team reverse engineered domain generation algorithm
  - Registered 30 days of domains before the botmaster!
  - Full control of the botnet for 10 days
- Goal of the botnet: theft and phishing
  - Steals credit card numbers, bank accounts, etc.
  - Researchers gathered all this data
- Other novel point: accurate estimation of botnet size

Stolen Information

- Data gathered from Jan 25-Feb 4 2009

User Accounts

Data Type	Data Items (#)
Mailbox account	54,090
Email	1,258,862
Form data	11,966,532
HTTP account	411,039
FTP account	12,307
POP account	415,206
SMTP account	100,472
Windows password	1,235,122

Banks Accounts

Country	Institutions (#)	Accounts (#)
US	60	4,287
IT	34	1,459
DE	122	641
ES	18	228
PL	14	102
Other	162	1,593
Total	410	8,310

- How much is this data worth?
  - Credit cards: $0.10-$25 Banks accounts: $10-$1000
  - $83K-$8.3M

E-Crime

Spam, phishing, scams

- Spam
  - unsolicited bulk emails
  - 2006: 80% of emails on web, 85 billion messages a day
  - 2009: 95% of emails blocked as spam (100s of billions)
- Scam spam
  - Nigerian emails (advanced fee fraud / confidence trick)
- Phishing
  - trick users into downloading malware, submitting CC info to attacker, etc.
  - Spear phishing: targeted on individuals (used in high-profile intrusions)

Hi Dear,

I am Mrs. Zarina Al-Usman, I have been diagnosed with Esophageal cancer .It has defied all forms of medical treatment, and Right now, I have only about a few months to live and I want you to Distribute my funds worth Twelve Million Five Hundred Thousand US Dollars to charities homes in your country.

I have set aside 40% for you and your family so keep this as a secret to yourself because this will be my last wish.
Yours Truly,

Mrs. Zarina Al-Usman

WebMail FDV - MG
Faculdade Viçosa

This is an automatic notification of your current disk space usage on the CSE mail server:

Your account status:

Current utilization: 95.33%

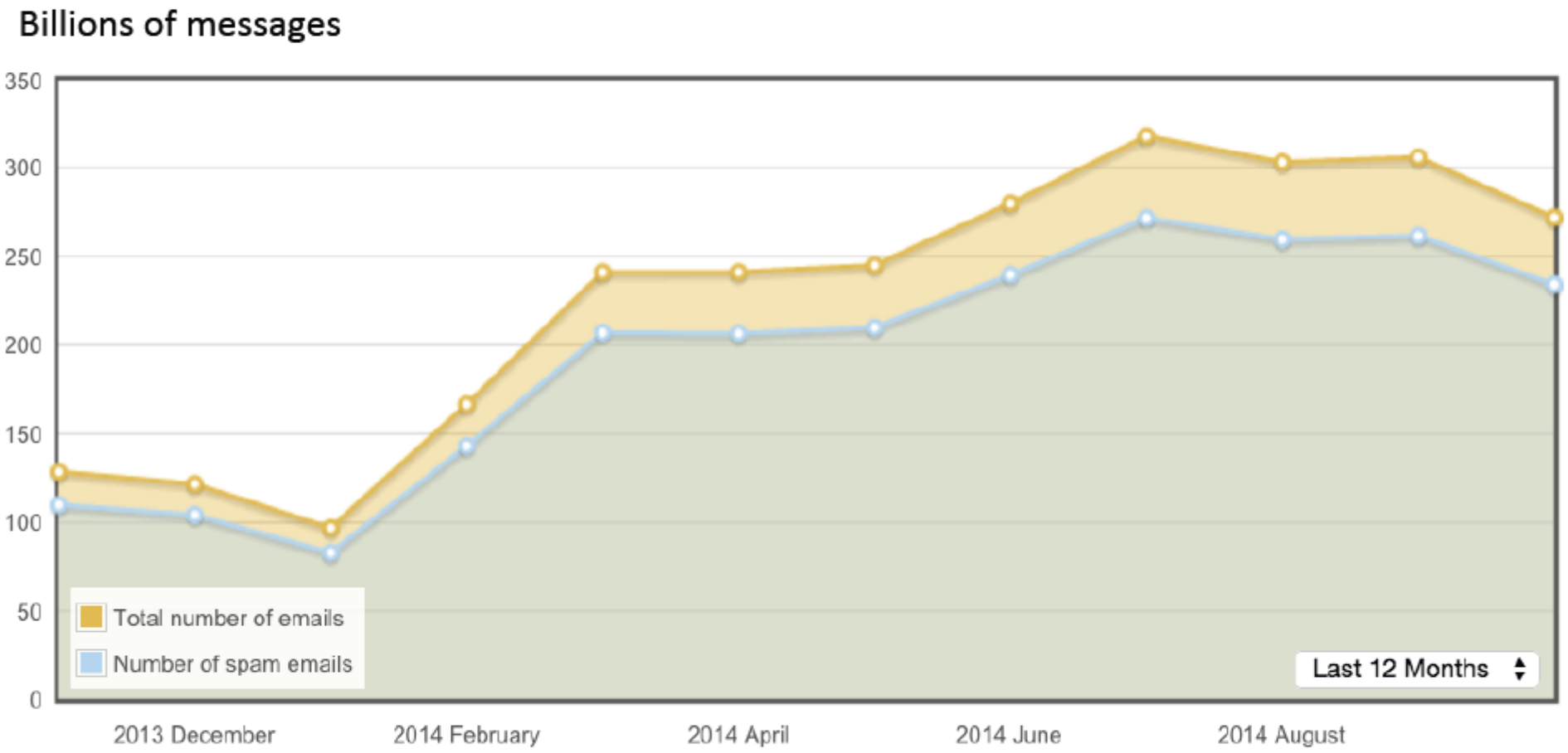
Space used:	976 MB
Available space:	47 MB
Account limit:	1024 MB

Once your quota has been reached, mail will no longer be delivered to your account, and will be returned to the sender as undeliverable.

If you are not sure where to look for mail that can likely be deleted to clear space in your account, you may likely have large amounts of mail in your Trash and/or Junk folders. Also, you may have a large amount of mail accumulating in your Sent folder over time, if you have configured your mail client to automatically save sent messages.

Your account limit may be increased for an additional charge, as per the CSE Recharge Policy. Please contact CSEHelp regarding quota increases.

Spam volume



http://www.senderbase.org/static/spam/#tab=1

Spam

- The frontend (email recipients)
  - Filtering, classification
  - Psychology
- The backend (email generation)
  - Open email relays
  - Botnets
  - Social structure
    - Affiliates
    - Criminal organizations

Spam Classifiers

Spam / Ham

This classifier will be trained from a large corpus of labeled data

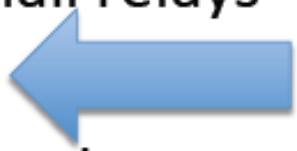
...

Spam classifiers

- Real classifiers more complex than this
  - Other features: Who is sender? How many links embedded? Is it from an open mail relay?
  - Can update in real-time given labelings by user
  - For larger orgs, can leverage wide view across many email recipients
- Nowadays some companies do pretty good job of making sure spam doesn't hit your inbox
  - 95% of email gets filtered as spam (2009, ENISA Spam Survey)

Spam

- The frontend (email recipients)
  - Filtering, classification
  - Psychology, usability
- The backend (email generation)
  - Open email relays
  - Botnets
  - Social structure
    - Affiliates
    - Criminal organizations



How to make money off a botnet?

- Rental
  - "Pay me money, and I'll let you use my botnet… no questions asked"
- DDoS extortion
  - "Pay me or I take your legitimate business off web"
- Bulk traffic selling
  - "Pay me to direct bots to websites to boost visit counts"
- Click fraud, SEO
  - "Simulate clicks on advertised links to generate revenue"
  - Cloaking, link farms, etc.
- Theft of monetizable data (eg., financial accounts)
- Data ransom
  - "I've encrypted your harddrive, now pay me money to unencrypt it"
- Advertise products

How to make money off financial credentials?

- Money mules
  - Deposits into mules' account from the victim's
  - Mule purchases items using stolen CCN, sells them online
  - Mule withdraws cash from ATMs using victim credentials
- Wires money to (frequently) former Soviet Union

> Organized cyber criminals stole almost $11 million in two highly coordinated ATM heists in the final days of 2012, KrebsOnSecurity has learned. The events prompted Visa to warn U.S. payment card issuers to be on high-alert for additional ATM cash-out fraud schemes in the New Year.

Dear Student,

I would like to offer you a new interesting and respectable job!
We are looking for people to work as professional distance-based typists. No experience is needed!
If you're eager to use your skills to make some additional cash, then you might want to consider a home typing position!

All data entry operators work from home and are independent contractors.
You typically set your own hours and work from home on projects that are enjoyable!
Average monthly earnings start from $1000 to $3000 or more.

Requirements:
-Computer with Internet access.
-Good Typing Skills.
-Basic Internet knowledge.
-Basic Computer and Typing Skills.

You will not have to devote full time hours. These assignments can be done on your time.
They may be done in Internet cafes or where ever you can get Internet access!
If you are interested just reply to my email!

Best Regards,

Richard Hill
Local Recruitment Manager

Botnet countermeasures?

- Infection prevention
- Infection detection
- C&C take-down
- Undermine the economics
  - Banking take-down

C&C takedowns

Microsoft Seizes ZeuS Servers in Anti-Botnet Rampage

BY KIM ZETTER 03.26.12 2:45 PM

It's not the first time Microsoft has attempted to take down botnets. The company previously attacked three other botnets — Waledac, Rustock and Kelihos — through similar civil suits that allowed the company to seize web addresses and associated computers. The gains from such takedowns, however, are generally short-lived. After Waledac was targeted, the criminals behind it simply altered their software to thwart easy detection and launched a new botnet.

http://www.wired.com/threatlevel/2012/03/microsoft-botnet-takedown/

Anti-Botnet Efforts Still Nascent, But Groups Hopeful

Seven months after a government-industry coalition announced recommendations for ISPs to fight botnets, success is still a long way off

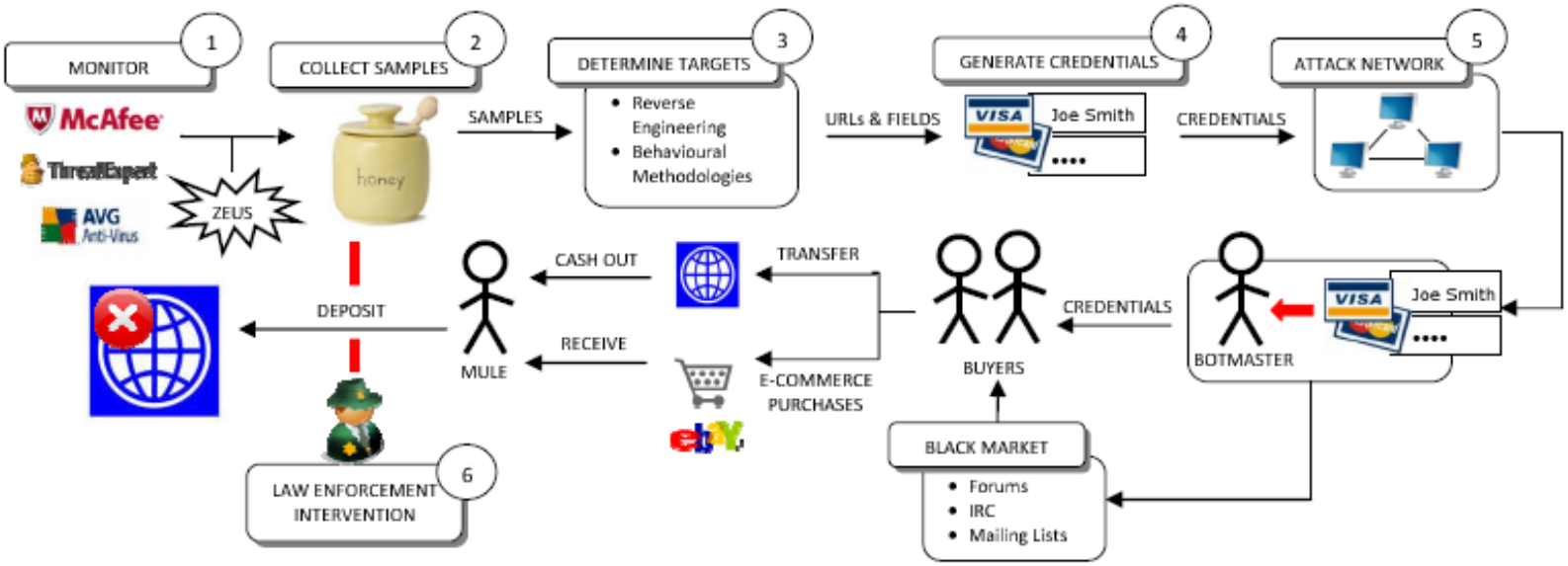
Botnet countermeasures?

- Infection prevention
- Infection detection
- C&C take-down
- Undermine the economics
  - Banking take-down

First Variant

- **Dilute the stolen identity information from a botnet with false credentials**
- Monitor current botnet toolkit trends and select the leading toolkit used for identity theft as our target.
- Acquire as many samples of botnet binaries as possible from honeynets, antivirus companies, financial institutions and security forums
- Determine targeted web sites and targeted fields by analyzing malware samples.
- Generate false identity information.
- Submit identity information to the botmasters through the framework.

Botnet toolkit defamation process



Second Variant

- The second variant of our framework is an extension of the first one.
- The intent is to discredit the security for the end-users of the stolen information. This approach contains one additional step that occurs after the credentials propagate through the Internet black market:
- **Monitor account usage and make arrests when funds withdrawn and purchases received**
- Coordination between law enforcement and the various financial institutions is paramount for this approach to succeed.
- The criminals must be convinced that the accounts are valid and the transactions are working.
- Law enforcement's role is to monitor these accounts and attempt to arrest individuals as they try to extract the funds.

Traditional examples of Online Scams

- **Check fraud**
  - Money order for an online deal is far larger than sale price
    - “Oversight” by buyer
  - Buyer needs check for the difference
  - Original money order is forged
- **Bump & Dump**
  - Scammer invests in penny stock
  - Sends messages hyping the stock
  - People invest
    - Value goes up
    - Scammer “dumps” the stock

More examples

- **419 Scam (“Nigerian Scam”)**
  - The number "419" refers to the section of the Nigerian Criminal Code dealing with fraud, the charges and penalties for offenders
  - Businessman needs to launder money
  - Make you rich
  - Requires upfront fees
  - Often perpetrated from Nigeria
    - Though now from all over the world
- **Romance Scam**
  - Usually scammers post profiles, using stolen photographs of attractive people
  - In some cases, online dating services are themselves engaged in misrepresentation

Vishing

- Vishing – another threat vector.
- E.g.: Caller ID shows it's your bank calling.
- People trust the telephone system more than they trust the internet
- People have come to expect non-human telephone operators and directories
- Elderly are easily reachable this way
- Smart targeting victims **using technology**
  - Examples include: Asterisk http://www.asterisk.org/
- Can be combined with Phishing

E-crime is a complex ecosystem

- Lots of moving parts
- Economics important
  - Fascinating measurement studies
- Technical mechanisms often don't measure up