Worms and Viruses

CS 161/194-1

Anthony D. Joseph

October 26, 2005

Outline

- What is a Worm/Virus?
- Why are they created?
- Infection Vectors and Payloads
  - How they propagate and what they do
- Worm propagation rates
- Virus/Worm detection/prevention
  - File scanners, host scanners, network scanners
  - Host monitors
- Targeted Worms and Viruses

Internet Worms and Viruses

- Self-replicating code and data
  - Worms are self-propagating (search network)
    - Typically exploit vulnerabilities in an application running on a machine or the machine's OS
  - Viruses typically require a human interaction before propagating
    - Running e-mail attachment, or click link in e-mail
    - Inserting/connecting "infected" media to a PC
- Behavioral invariant: they seek to propagate

Why Create Worms/Viruses?

- Formerly was a prestige motivation
  - Finding bugs, mass infections, …
  - 50% of viruses contain crackers'/groups' names
- Cracking for profit, including organized crime
  - Create massive botnets 10-100,000+ machines infected
    - Overloading/attacking websites, pay-per-click scams, spaming/phishing e-mail, or phishing websites…
    - More on botnets on Wednesday…
  - Corporate/personal espionage (SSN, passwords, docs, …)
- Closing security loopholes
  - Is this ethical?

Revisiting Zotab Virus (August 2005)

- Financially-driven motive
  - Infected machines and set IE security to low (enables pop-up website ads)
  - Revenue from ads that now appear
  - User may remove virus, but IE settings will likely remain set to low
  - Continued revenue from ads…
- Update (August 25th)
  - Farid Essebar was arrested in Morocco and Atilla Ekici was detained by police in

Infection Vectors and Payloads

- Two components to worms and viruses
- Infection vectors
  - How they get onto your machine and then propagate
- Payloads
  - What they do on your machine

Infection Vectors

- Network scanning for potential victims (worms)
- Local/server/P2P files (viruses/worms)
- E-mail message components (viruses)
- Web sites (worms/viruses)

Network Scanning for Potential Victims (Worms)

- How to scan the network?
  - Pick address, try to exploit protocol vulnerabilities
- How to generate addresses?
  - Use a PRG, but how to initialize the PRG?
- Same seed on each host (common flaw!)
  - Need to generate local seed…
- Generate 32-bit IP address or 4 8-bit parts?
  - Is even or uneven probing better?
  - Local hosts are likely to be same OS/patch level and have higher bandwidth
  - Also local addr space is denser

Worm Exploits

- Buffer overflow on servers/clients
  - Identify de-serializing errors, send exploit code
  - MSBlaster DCOM/RPC exploit
- Forcing protocol parsing errors
  - Identify errors in protocol handling/state machine
  - Morris worm fingerd remote code exec
- Weak passwords
  - Brute force: try name backwards, appended, …
- Out-of-the box configuration errors
  - Default ID/password
  - Debugging mode enabled (Morris worm sendmail exploit)

Infecting via Files

- Factory installed
- Removable media (viruses)
  - Floppies, CD/DVD-ROMs, USB drives/keys
- Files on shared servers and P2P networks (worms/viruses)
  - Have to convince user to click to open…
  - Or, an infected existing document
- E-mail file attachments (viruses)
  - Have to convince user to click to open…

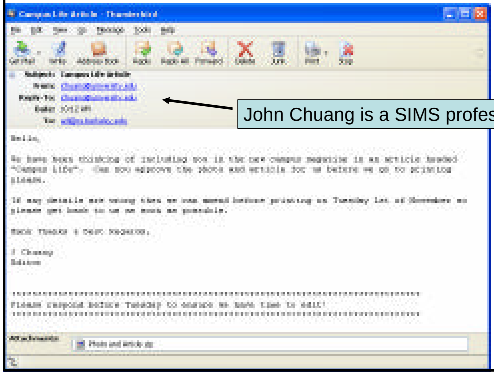
Infecting via E-mail

- E-mail attachments (viruses)
  - Files (see last slide)
  - Scripts: Windows Scripting Host
  - HTML files: browser exploits (next slide)
- HTML-formatted e-mail messages
  - Browser exploits (next slide)
  - User clicks on links (leads to browser exploits)
  - Windows Scripting Host
    - Executes simply by viewing e-mail msg (LoveLetter)
  - Embedded images (JPEG/PNG render exploits)

Why E-mail-based Infections?

- E-mail has become globally ubiquitous
  - By 2006, e-mail traffic is expected to surge to 60 billion messages daily
- Message Labs scanned 14.7 billion emails scanned, found >6% were viral
- Nearly all of the most virulent worms of 2004 spread by email (Symantec/Sophos)

Increasing Sophistication


Campus Life Article - Thunderbird
File Edit View Go Message Tools Help
Get Mail
Write
Address Book
Reply
Reply All
Forward
Delete
Junk
Print
Stop

Subject: Campus Life Article
From: [illegible]
Reply-To: [illegible]
Date: 10:12 AM
To: [illegible]

Hello,

We have been thinking of including you in the new campus magazine in an article headed "Campus Life". Can you approve the photo and article for us before we go to printing please.

If any details are wrong then we can amend before printing on Tuesday 1st of November so please get back to us as soon as possible.

Many Thanks & best Regards,

J Chuang
Editor

****
Please respond before Tuesday to ensure we have time to edit!
****

Attachments: Photo and Article.zip

John Chuang is a SIMS professor

Web Sites (Worms/Viruses)

- Set up malicious server, or infect existing server
  - Porn, Warez/Crackz/Gamez, anti-spyware(!) sites
- Exploit bugs in browser rendering engine
  - "Drive-by-download" infection
- ActiveX exploits
  - Leverage bugs in ActiveX components
  - Enable remote script/code execution
- HTML parsing vulnerabilities
  - Redirect to malicious sites
  - Cause buffer overflow, or file download and execute

Types of Payloads

- Bootstrap loader
- Message
- Propagation engine
  - System settings/DNS changer, file installer
- Destructive actions
- Zombie software installer
- Trojans/Browser Help Objects installer
- But, sometimes payloads don't work
  - Inadvertent system crashes instead

Payloads (1/2)

- Bootstrap loader
  - Used when exploit can only send a small amount of code/script
  - Establishes TFTP connection back to infecting machine to retrieve real payload
- Message (could be null)
- Propagation engine
  - Permanently installs virus/worm by changing system settings, or replacing/infecting system files (rootkit)
  - Infect local/server/P2P documents, music, etc.
- Malicious: disk corruption, or BIOS re-flash

Payloads (2/2)

- Zombie software install
  - Password cracker
  - Spambot or Distributed Denial of Service bot
- Trojans/Browser Help Objects installer
  - Adware/spyware install
    - Typically, implemented as BHOs
  - Collect personal info, logins/passwords for financial sites, files/data and send to attacker
  - Create popups and search redirects

Fast Propagating Worm/Virus Side Effects

- Traffic floods network links
  - Slammer prevented admins from accessing servers to shut them down/patch them
  - Affected the access links
    - Border Gateway Protocol heartbeats monitor links
    - Timeouts caused links to drop, stopped worm traffic
    - Heartbeats get through, links come back up, worm traffic flows again (repeat!)
- Overwhelms servers (e-mail/other)
  - Denial of service (sometimes intentional)

Virus/Worm Toolkits

- Dozens of websites and downloadable toolkits for building worms/viruses
- Make it easy for script kiddies to create new threats
- But, most are built from common building blocks with the same polymorphic engines
  - Can create signatures for blocks and engines
- Encryption is a looming threat…

Outline

- What is a Worm/Virus?
- Why are they created?
- Infection Vectors and Payloads
  - How they propagate and what they do
- Worm propagation rates
- Virus/Worm detection/prevention
  - File scanners, host scanners, network scanners
  - Host monitors
- Targeted Worms and Viruses

Propagation Rates

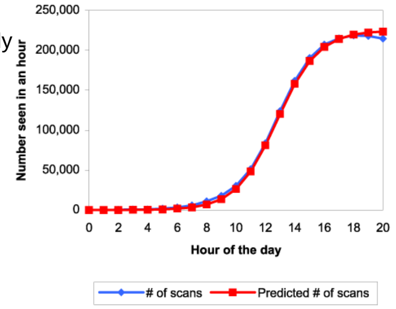
- Classic theory
  - Function of # vulnerable hosts (N), initial compromise rate (K), start time (T)
- Logisitics equation:

$$a = \frac{e^{K(t-T)}}{1 + e^{K(t-T)}}$$

- *a* is number of infected hosts

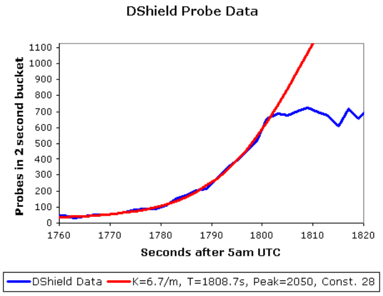
Code Red I Propagation

- Can't easily count infected hosts
  - Count scans instead
- Theory matches observed



Propagation Rates (New Theory)

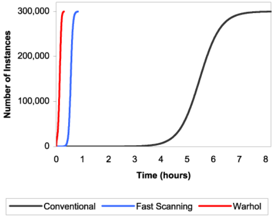
- Slammer
- Doesn't apply to fast propagating worms
  - Links have bandwidth / latency constraints
  - No universal connectivity



Other Factors

- TCP (3-way) versus UDP
  - Latency between attacker and victim has major impact for TCP
  - Timeout delay when scanning
- Also, function of scan algorithm
  - PRN quality
    - Broken algorithms mean missed hosts
  - Seed computation
  - Scan distribution (even or local bias?)

Propagation Behavior



- More efficient scanning finds victims faster (< 1hr)
- Even faster propagation is possible if you cheat
  - Wasted effort scanning non-existent or non-vulnerable hosts
  - Warhol: seed worm with a “hit list” of vulnerable hosts (15 mins)

Virus Propagation Rates

- How to determine virus propagation rates?
  - Don’t have universal connectivity
    - Small worlds effect: 6-degrees of separation
  - Have to account for queuing delays
  - Limited (delayed) by human interaction rate
  - Very hard to model analytically
- E-mail viruses tend to appear first in Asia, then Europe, finally North/South America
  - Follows business day/timezones

Outline

- What is a Worm/Virus?
- Why are they created?
- Infection Vectors and Payloads
  - How they propagate and what they do
- Worm propagation rates
- Virus/Worm detection/prevention
  - File scanners, host scanners, network scanners
  - Host monitors
- Targeted Worms and Viruses

Detection/Prevention Techniques

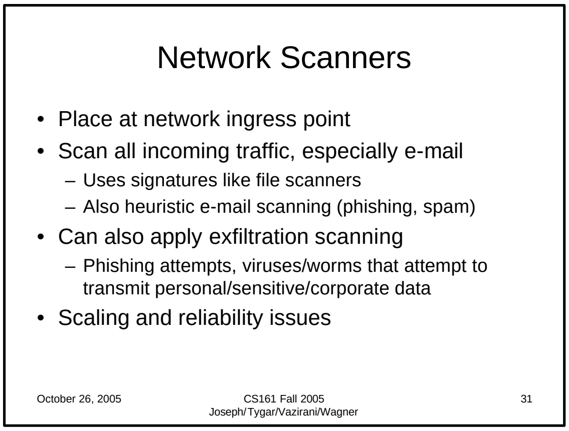
- File and host scanners and monitors
  - Signature-based scanners
    - Have “zero” false negatives/positives
    - Significant human delay (hours to days)
  - Heuristic-based scanners
    - Non-zero false negative/positive rates
- Network scanners
- Firewalls
- Throttling

Signature Generation Requires Human Intervention

- Human element slows reaction times
  - Malcode collection can take hours
  - Signature generation can take hours to days
  - Signature distribution can take hours to days
  - Novel malcode propagates faster than signatures
- Signature methods are mired in an arms race
  - MyDoom.m and Netsky.b slipped through EECS mail scanners
  - Malcode: polymorphic today, encrypted in future
  - Signature-based approach alone is insufficient

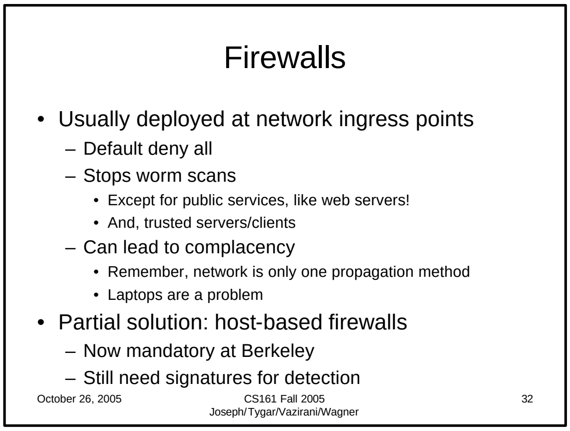
File/Host Scanners and Monitors

- File
  - One-time/periodic “scan” or continuous real-time monitor
  - Scan all files on read/write
  - Heuristic: look for code similarities (e.g., propagation engines), not identical matches
- Host scanner
  - One-time/periodic “scan” or continuous real-time monitor
  - Scan active processes, bios, registry, … for infections
  - Heuristic: examine process memory, look for anomalous registry entries, …



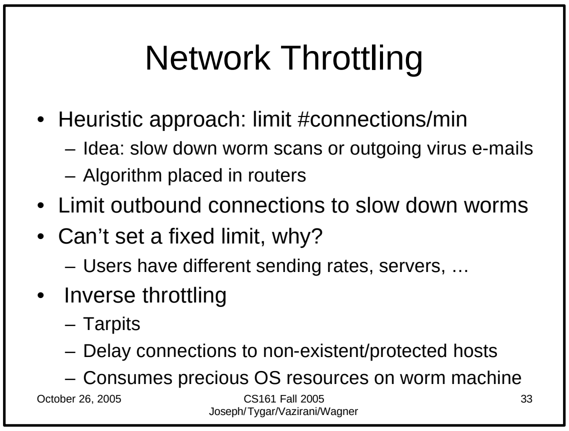
Network Scanners

- Place at network ingress point
- Scan all incoming traffic, especially e-mail
  - Uses signatures like file scanners
  - Also heuristic e-mail scanning (phishing, spam)
- Can also apply exfiltration scanning
  - Phishing attempts, viruses/worms that attempt to transmit personal/sensitive/corporate data
- Scaling and reliability issues



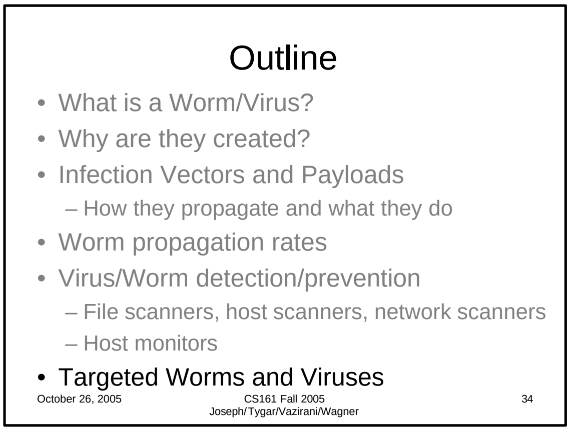
Firewalls

- Usually deployed at network ingress points
  - Default deny all
  - Stops worm scans
    - Except for public services, like web servers!
    - And, trusted servers/clients
  - Can lead to complacency
    - Remember, network is only one propagation method
    - Laptops are a problem
- Partial solution: host-based firewalls
  - Now mandatory at Berkeley
  - Still need signatures for detection



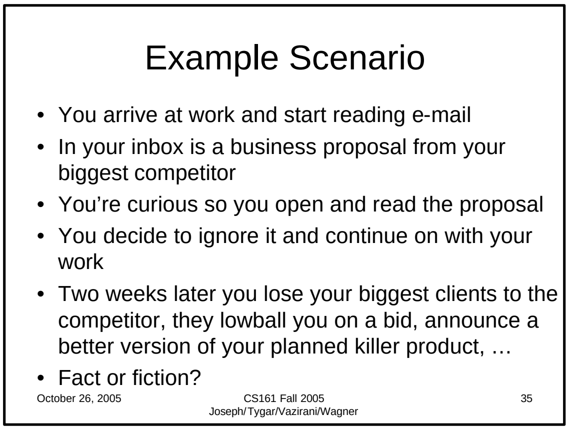
Network Throttling

- Heuristic approach: limit #connections/min
  - Idea: slow down worm scans or outgoing virus e-mails
  - Algorithm placed in routers
- Limit outbound connections to slow down worms
- Can't set a fixed limit, why?
  - Users have different sending rates, servers, …
- Inverse throttling
  - Tarpits
  - Delay connections to non-existent/protected hosts
  - Consumes precious OS resources on worm machine



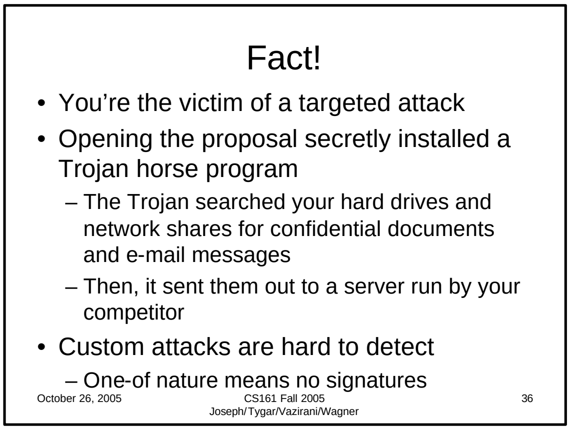
Outline

- What is a Worm/Virus?
- Why are they created?
- Infection Vectors and Payloads
  - How they propagate and what they do
- Worm propagation rates
- Virus/Worm detection/prevention
  - File scanners, host scanners, network scanners
  - Host monitors
- Targeted Worms and Viruses



Example Scenario

- You arrive at work and start reading e-mail
- In your inbox is a business proposal from your biggest competitor
- You're curious so you open and read the proposal
- You decide to ignore it and continue on with your work
- Two weeks later you lose your biggest clients to the competitor, they lowball you on a bid, announce a better version of your planned killer product, …
- Fact or fiction?



Fact!

- You're the victim of a targeted attack
- Opening the proposal secretly installed a Trojan horse program
  - The Trojan searched your hard drives and network shares for confidential documents and e-mail messages
  - Then, it sent them out to a server run by your competitor
- Custom attacks are hard to detect
  - One-of nature means no signatures

Targeted Attacks

- Israel (May 19, 2005)
  - 7 businessmen and 11 private detectives arrested for using Trojan horse for cyber industrial espionage
    - Satellite TV, cell phone, auto import business
- Trojan designed by husband-wife pair in Britain
  - Named Rona (variant of Hotword Trojan)
- Caught because husband installed it on father-in-law's computer and it posted copies of a private manuscript online

Designing a Targeted Attack

- How to profile target to identify OS, SW?
  - Send an e-mail message and examine reply!
    - User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.0; en-US; rv:1.5) Gecko/20031007
  - More work to determine OS/SW patch levels
- Then craft an attack:
  - HTML script vulnerabilities
  - Embedded/remote images
  - Web site exploits
  - Office documents (macros, scripts, …)
  - Other document types (PDF, PS, …)

Worm/Virus Summary

- Arms race between creators and protectors
- Existing signature approaches are limited
- Financial motive poses growing threat
- High risk from Warhol worms
- Viruses are still a critical threat
  - FBI survey of 269 companies in 2004 found that viruses caused ~$55 million in damages