CS 194-1 (CS 161)
Computer Security

Lecture 22

Worms and Viruses; Botnets

November 20, 2006
Prof. Anthony D. Joseph
http://cs161.org/

Review: Worms vs. Viruses

- Internet Worms
  - Self-replicating, self-propagating code and data
  - Use network to find potential victims
  - Exploit vulnerabilities in running apps or OS
  - Then search the network for new victims
- Internet Viruses
  - Self-replicating code and data
  - Require human interaction before exploiting an application vulnerability
    - » Clicking on e-mail attachment or link
    - » Inserting/connecting "infected" media to a PC
  - Then search for files to infect or sends out e-mail with an infected file

Goals for Today

- Worms and Viruses – how they work
  - Infection vectors and payloads
  - Worm/virus propagation rates
  - Detection and prevention techniques
  - New threat: targeted attacks
- Botnets
  - Uses
  - The money trail…
  - Distributed Denial of Service Attacks

Infection Vectors and Payloads

- Two components to worms and viruses
- Infection vectors – how they get on your machine
  - Network scanning for potential victims (worms)
  - Local/server/P2P files (viruses/worms)
  - E-mail message components (viruses)
  - Web sites (worms/viruses)
- Payloads
  - What they do on your machine

Network Scanning for 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 address 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)

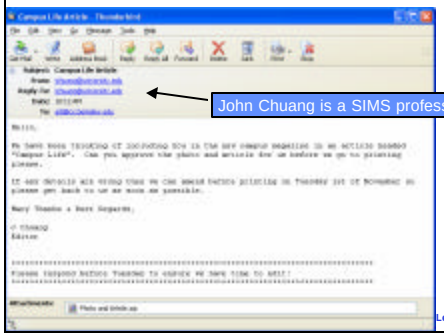
Infecting via Files

- 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
- HTML-formatted e-mail messages
  - Browser exploits or user clicks on link to exploit page
  - Windows Scripting Host (executes when viewing msg)
  - Embedded images (JPEG/PNG render exploits)
- Why use E-mail-based infections?
  - E-mail is globally ubiquitous
  - In 2004, Message Labs scanned 14.7 billion emails scanned, found >6% were viral
- Almost all virulent viruses in 2004 spread by email

Increasing Sophistication



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

Payloads (1/2)

- Sometimes payloads don't work (system crash)
- 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

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

Administrivia

Worm and Virus Side Effects

- Fast propagating worms and viruses can generate network traffic floods
  - 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!)
- Overwhelm servers (e-mail/other)
  - Denial of service (sometimes intentional)
- How fast do they propagate?

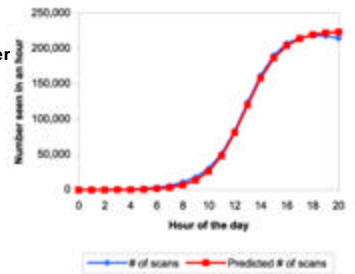
Worm Propagation Rates

- No human delays and an all-connected system
- Classic Logistic function $P(t) = a\frac{1 + me^{-t/r}}{1 + ne^{-t/r}}$
- Sigmoid function $P(t) = \frac{1}{1 + e^{-t}}$
- We have initially exponential growth in a finite system
  - Random Constant Spread (RCS) or Susceptible-Infected (S-I) model
  - Proportion of hosts that are infected (a), initial compromise rate (K), and a constant of integration that fixes the time position of the incident (T)

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

Code Red I Propagation

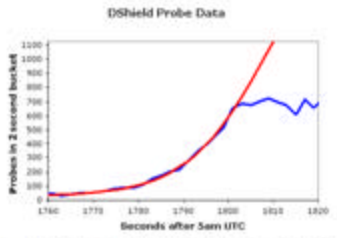
- Hard to count number of infected hosts
  - Count scans by them instead
- Theory matches observed



How to Own the Internet in Your Spare Time in Proceedings of the 11th USENIX Security Symposium (Security '02)

Propagation Rates (New Theory)

- Observed Slammer worm behavior doesn't match
  - Fast propagating worms encounter links' BW and latency constraints
  - Non-universal connectivity

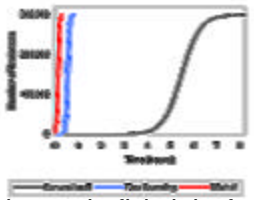


The Spread of the Sapphire/Slammer Worm, http://www.caida.org/publications/papers/2003/sapphire/sapphire.html

Other Propagation Rate Factors

- TCP (3-way handshake) 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
  - Avoid 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 mail 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

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
- Throttling

Signature Generation

- Requires human interaction – 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 (like firewall)
- 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
- Issues:
  - Scaling and reliability issues
  - May not stop worm scans of public services (web)
  - Can lead to complacency
    - » Remember, network is only one propagation method
    - » Laptops are a problem

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

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

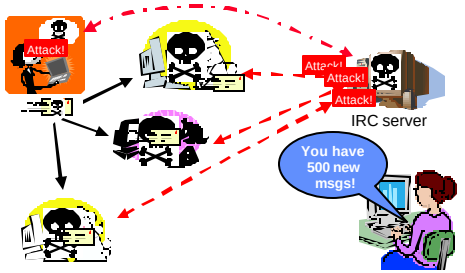
- How to profile target to identify OS, SW?
  - Send an e-mail message and examine reply!
    - » User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.0; en-US; rv:1.5) Gecko/20031007
  - More work to determine OS/SW patch levels
- Then craft an attack:
  - HTML script vulnerabilities
  - Embedded/remote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

BREAK

What is a Botnet?

- A network of compromised machines
  - Typically rented to "users" at costs depending on metrics ("bragging rights")
    - » Number of machines (1,000's – 100,000's)
    - » Aggregate bandwidth (gigabits – terabits)
  - Can be rented for campaign or for time
- Zombies connect to server(s)
  - Typically one or more IRC servers running on zombies
  - Some botnets use custom encrypted protocols
- Zombies await commands or perform pre-determined actions (e.g., send spam)
  - Some botnets require authenticated commands
  - Commands can be scripts or executables

Creating and Using a Botnet



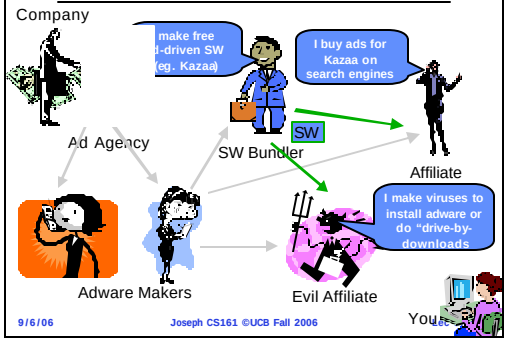
Uses for Botnets

- Send spam, spyware, adware, and phishing e-mail
  - Also, hosting phishing websites
- Click-for-pay fraud
- Distributed programming
  - Example: password cracking
  - Distributed servers to control the botnet
- Distributed Denial of Service (DDoS) attacks
  - Overwhelm server and/or network links
  - Political msgs, fame/bragging
  - Extortion ("pay or your site and business die")

The Adware / Spyware Money Trail…

- Popup ads start appearing on Joe's PC
  - For well-known brands (Chrysler, Expedia, Microsoft, Priceline, and Travelocity)
  - Each has border saying it is from "Aurora"
- Aurora is adware from Direct Revenue
  - But, Joe doesn't remember installing it…
- The adware industry has a $200 million to $2 billion a year revenue stream
- How does the ad go from Priceline to Joe?

Following the Money



Malicious Affiliates

- Most adware/spyware vendors claim they prohibit drive-by-download and virus-based installs
- But, there's a strong profit incentive, since they get paid based on the number of "eyeballs"…
- Some even sue adware/spyware detection companies for labeling them as such!!
- Adware/spyware may also recruit the machine into a botnet …

DDoS Attacks

- Overwhelm server and/or network links
  - Typical target is web server(s)
  - Try to consume all resources (BW, disk space, CPU)
- Simple: same req. for large images/complex action
  - Might be able to create packet filter to block
  - Might also be able to block source subnets
  - Have to put filters into the network (at upstream ISPs)
- Complex: Vary requests, rate, zombie set
  - Harder to create packet filter (esp. if requests look "real")
  - Rotating set makes source subnet blocks hard
  - Only choice may be to add more and more HW and BW

Toxbot Trojan (Oct 10, 2005)

- Three Dutch crackers (19, 22, and 27)
- Used Toxbot Trojan (aka Codbot) to infect machines
  - Installed adware and spyware on user' machines
  - Conducted DDoS attack against a US company for extortion (pay or crash your site)
  - Conducted phishing attacks to hijack PaPal and eBay accounts, then bought goods with accounts
- Estimated network size of 100K
- Investigators later discovered true size (>1.5M!)

Microsoft Decoy Zombie

- Intentionally infected a machine with zombie code
- Within 20 days:
  - PC received > 5 million connections!
  - Tried to send 18 million spam e-mails containing ads for 13,000 unique domains!
- October 27, 2005: filed 13 "John Doe" lawsuits against spammers
  - Enables them to subpoena ISPs and domain registrars for identities

Worm/Virus Summary

- Worms are a critical threat
  - More than 100 companies hit by the Zotob Windows 2000 worm in August 2005
  - Arms race between creators and protectors
  - Existing signature approaches are limited
  - Financial motive poses growing threat
  - High risk from Warhol worms
- Viruses are a critical threat
  - FBI survey of 269 companies in 2004 found that viruses caused ~$55 million in damages
  - DIY toolkits proliferate on Internet
- Botnets
  - Growing in size and threat
  - Recruited via adware, spyware, worms, viruses, …