

Viruses and Worms

Tom Chen

SMU

tchen@engr.smu.edu

Outline

- Introduction
- Basics of Viruses/Worms
- History: 4 Waves
- Defenses
- Why Attacks Continue
- Some Research Issues

Introduction

Can one IP packet cripple
the Internet in 10 minutes?

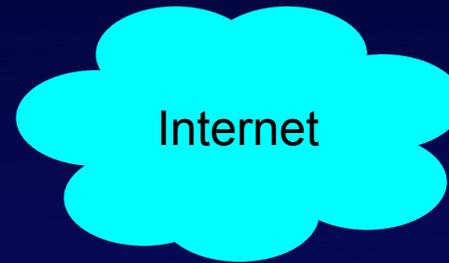
Many worry it is possible



- More than 1.2 billion dollars damage
- Widespread Internet congestion
- Attack peaked in 10 minutes
- 70% South Korea's network paralyzed
- 300,000 ISP subscribers in Portugal knocked off line
- 13,000 Bank of America machines shut down
- Continental Airline's ticketing system crippled



one packet



25 January 2003
example

➔ SQL Sapphire/Slammer
worm

Top Viruses/Worms

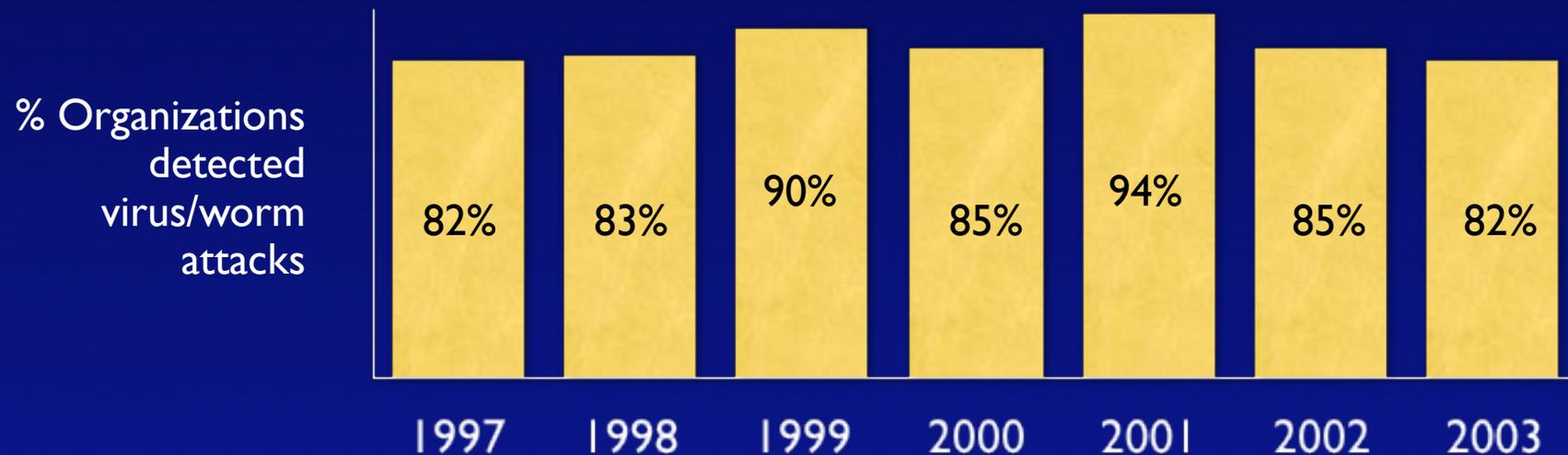
- 70,000+ viruses are known, but only hundreds “in the wild” and only a few spread well enough for major damage



*estimated by Computer Economics 2001

Prevalence

- Viruses/worms are consistently among most common attacks



*2003 CSI/FBI Computer Crime and Security Survey

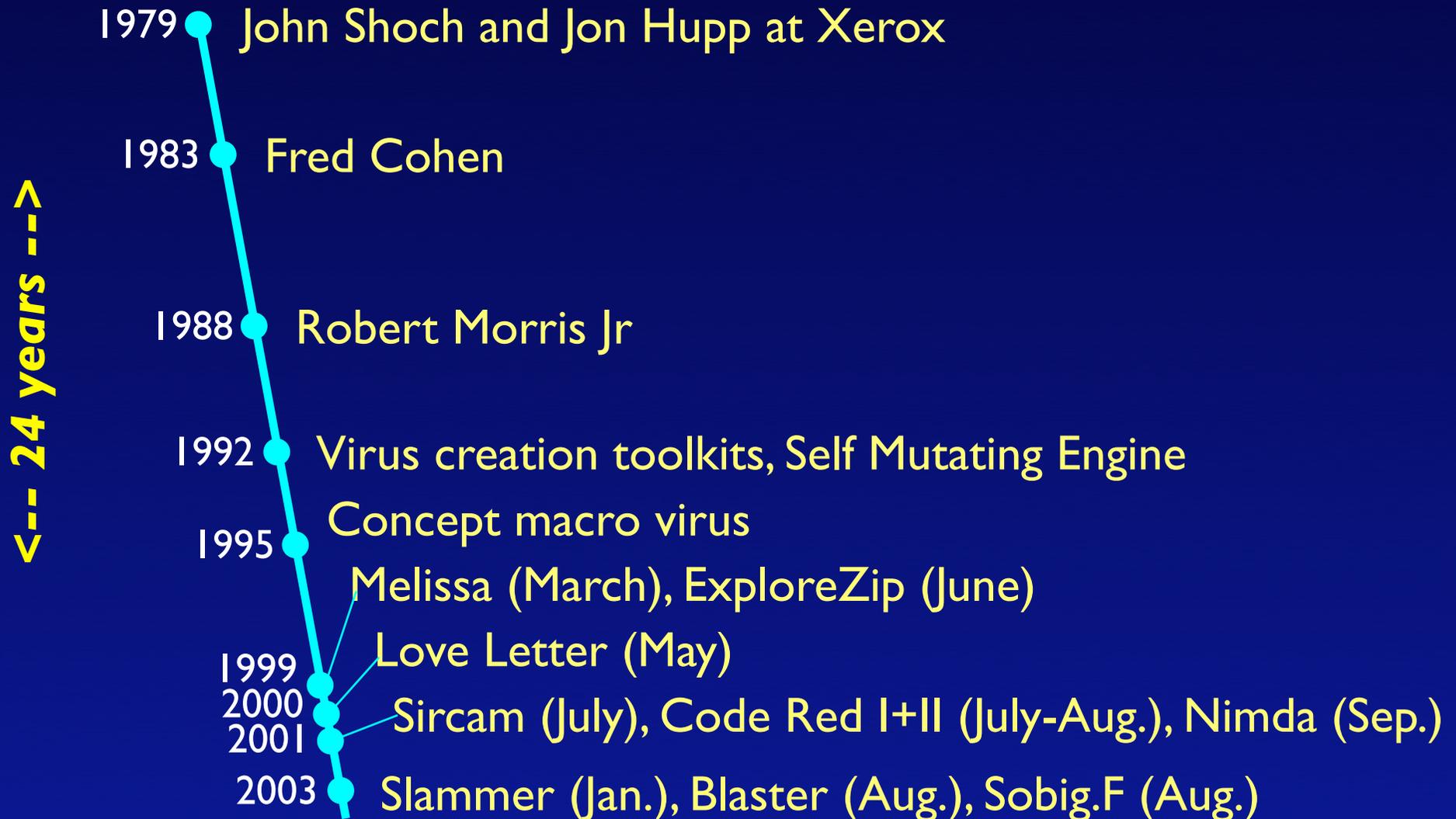
Damages

- Third most costly security attack (after theft of proprietary info and DoS)



*2003 CSI/FBI Computer Crime and Security Survey

Virus/Worm Highlights



Recent Cases (cont)

- July 18 Bagle.AI worm spread as attachment in email message from fake sender and subject line “Re:”
- Carries list of 288 antivirus and firewall software products -- disables these processes to avoid detection
- Attempts to contact several German Web sites to report addresses of infected machines

Recent Cases (cont)

- July 18 MyDoom.N also spread as email attachment
- Fake message from “Postmaster” or “Mailer-daemon”, appears to be a rejected message from mail server
 - Tries to trick user to open attachment

Recent Cases (cont)

- July 26 latest MyDoom.O worm added capability to search for email addresses using a search engine
 - When worm finds an email address on infected PC, it searches for other addresses in same domain using Google or Lycos
 - Sends copy of itself to these addresses

Basics of Viruses and Worms

What are Viruses

- Key characteristic: ability to self-replicate by modifying (infecting) a normal program/file with a copy of itself
 - Execution of the host program/file results in execution of the virus (and replication)
 - Usually needs human action to execute infected program

Cohen's Viruses

- Nov. 1983 Fred Cohen (“father” of computer virus) thought of the idea of computer viruses as a graduate student at USC
 - “Virus” named after biological virus
- Cohen wrote the first documented virus and demonstrated on the USC campus network

Cohen's Viruses (cont)

- Mathematically proved that perfect detection of viruses is impossible
- Always argued that viruses could have useful applications (like Shoch and Hupp wrote useful worms at Xerox)
 - Example: viruses for automatic program updating
 - But today viruses are malicious

Cohen's Viruses (cont)

Biological virus

Consists of DNA or RNA strand surrounded by protein shell to bond to host cell

No life outside of host cell

Replicates by taking over host's metabolic machinery with its own DNA/RNA

Copies infect other cells

Computer virus

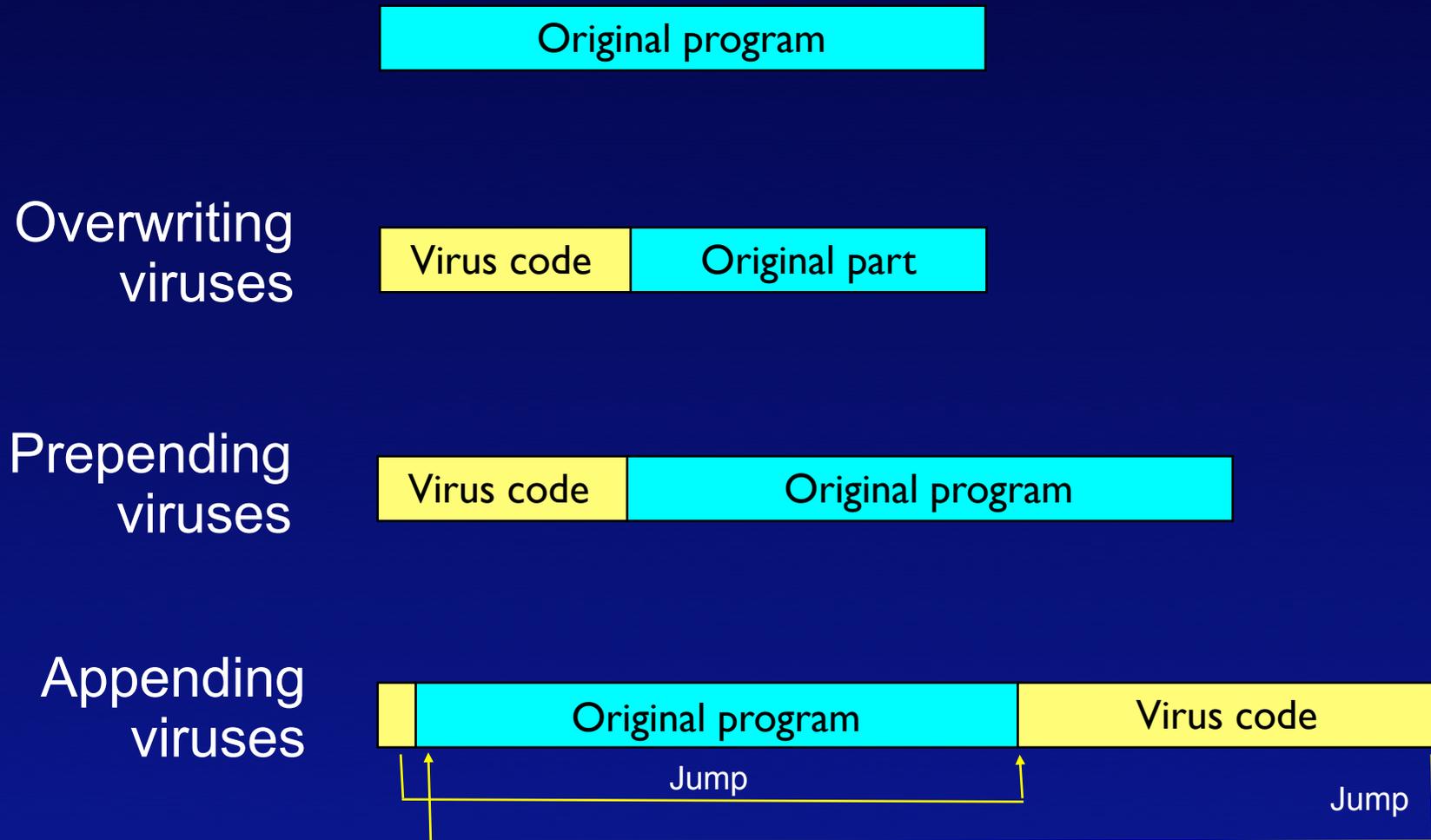
Consists of set of instructions stored in host program

Active only when host program executed

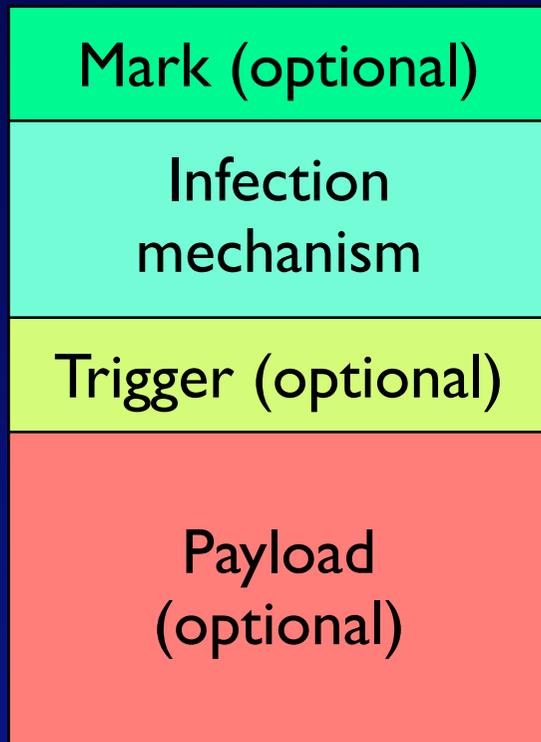
Replicates when host program is executed or host file is opened

Copies infect (attach to) other host programs

Virus Examples

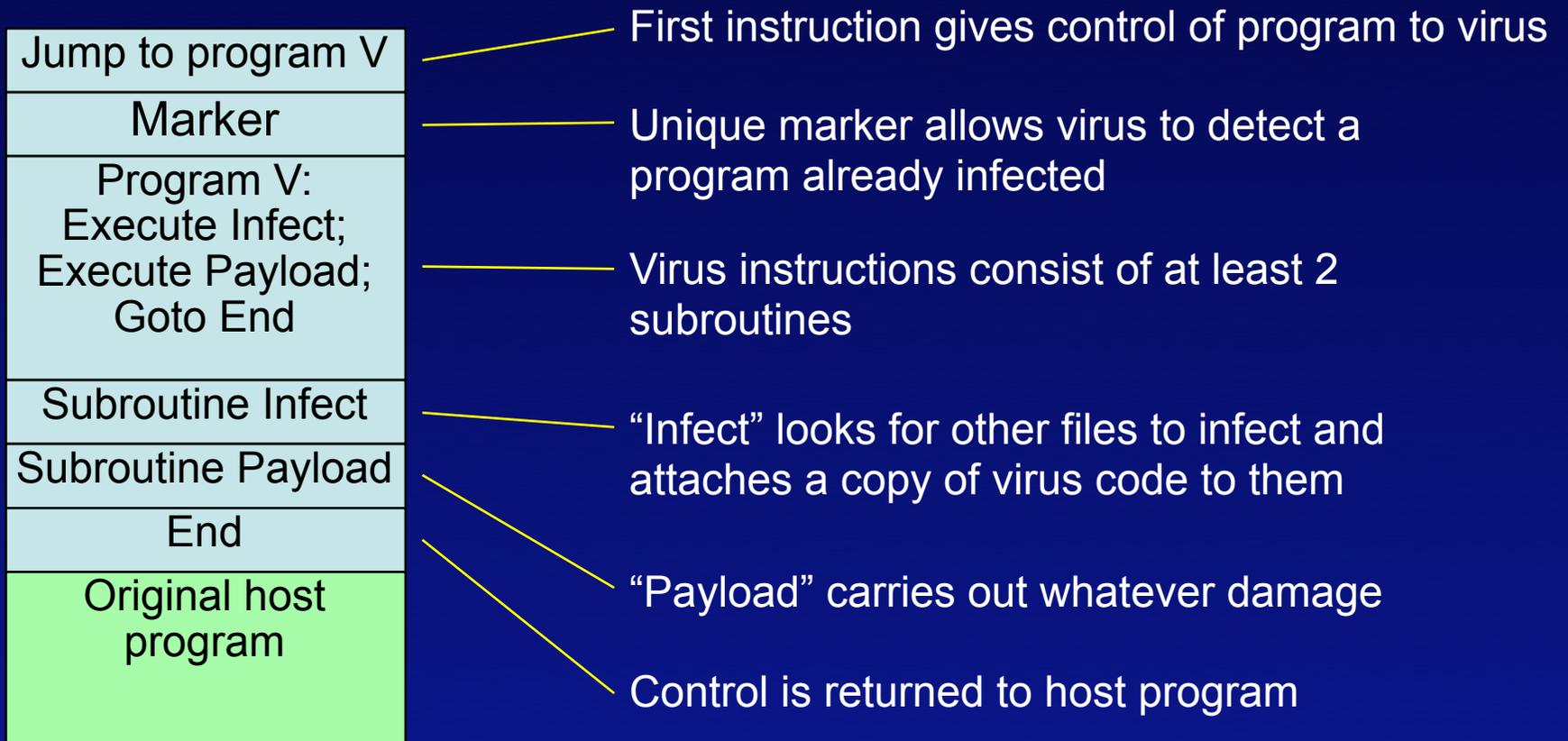


Virus Anatomy



- Prevents re-infection attempts
- Causes spread to other files
- Conditions for delivering payload
- Possible damage to infected computer (could be anything)

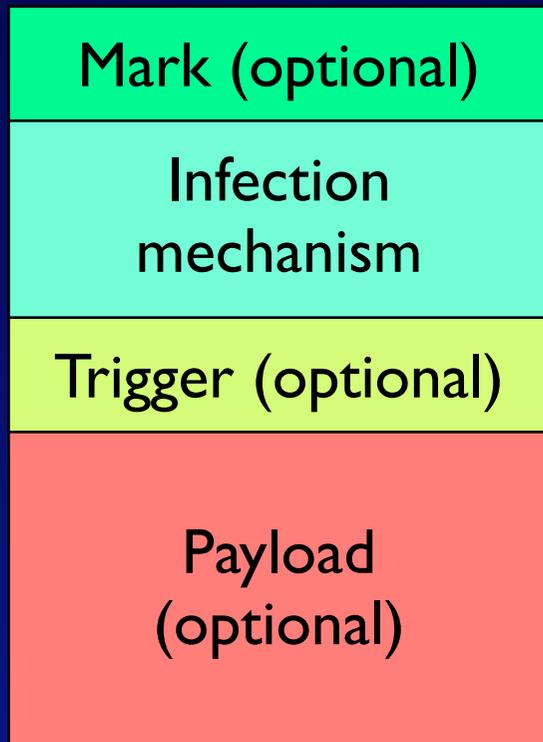
Simple Example



Worms

- Worm is a stand-alone program that exploits security holes to compromise other computers and spread copies of itself through the network
 - Unlike viruses, worms do not need to parasitically attach to other programs
 - Undetectable by file scanning
 - Do not need any human action to spread

Worm Anatomy



- Structurally similar to viruses, except a stand-alone program instead of program fragment
- Infection mechanism searches for weakly protected computers through a network (ie, worms are network-based)
- Payload might drop a Trojan horse or parasitically infect files, so worms can have Trojan horse or virus characteristics

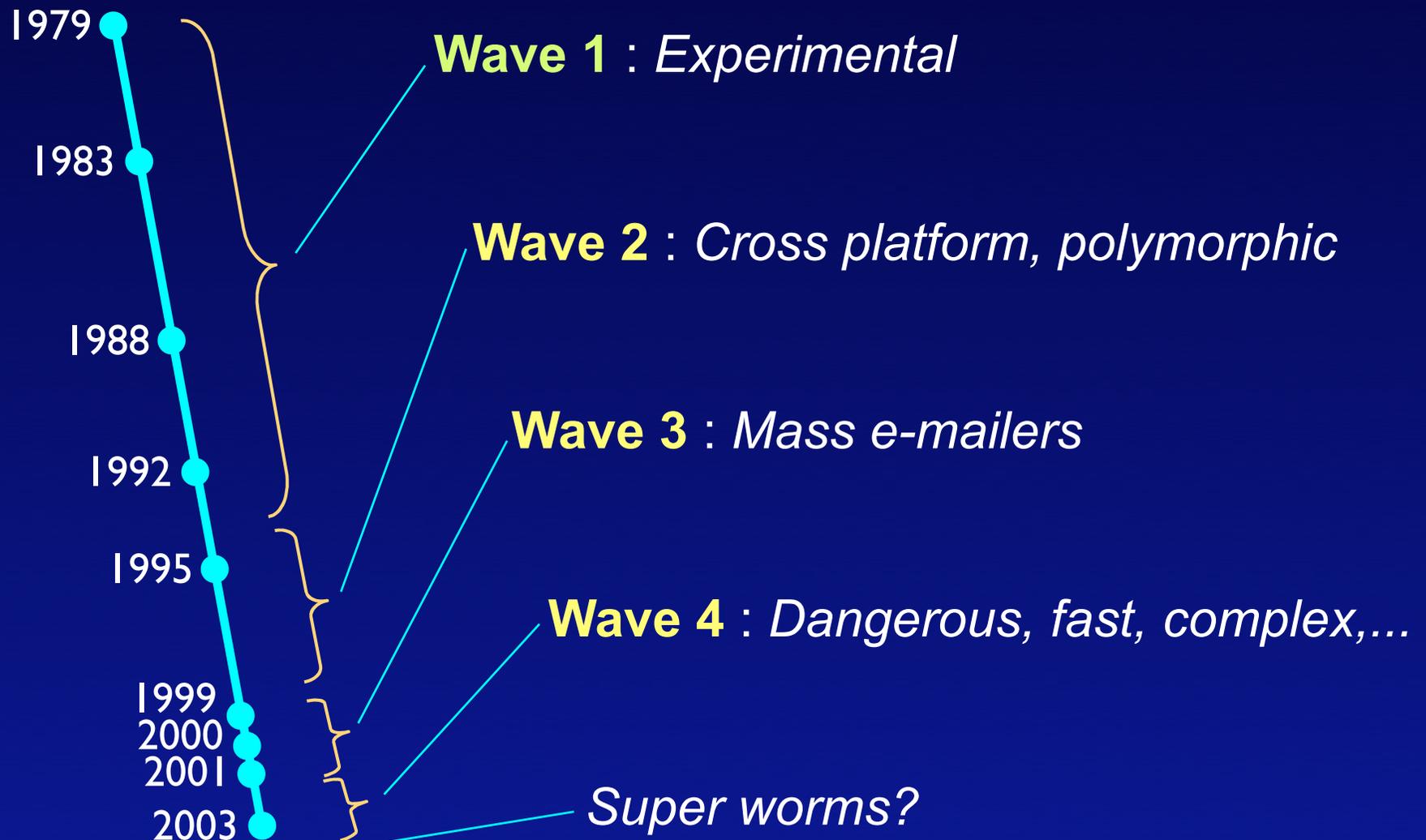
Vulnerabilities

- New vulnerabilities are continually published in Microsoft security bulletings, CERT advisories, Bugtraq, NIPC CyberNotes, MITRE CVEs,...
- SANS/FBI's Top 10 Microsoft Windows vulnerabilities (May 2003):

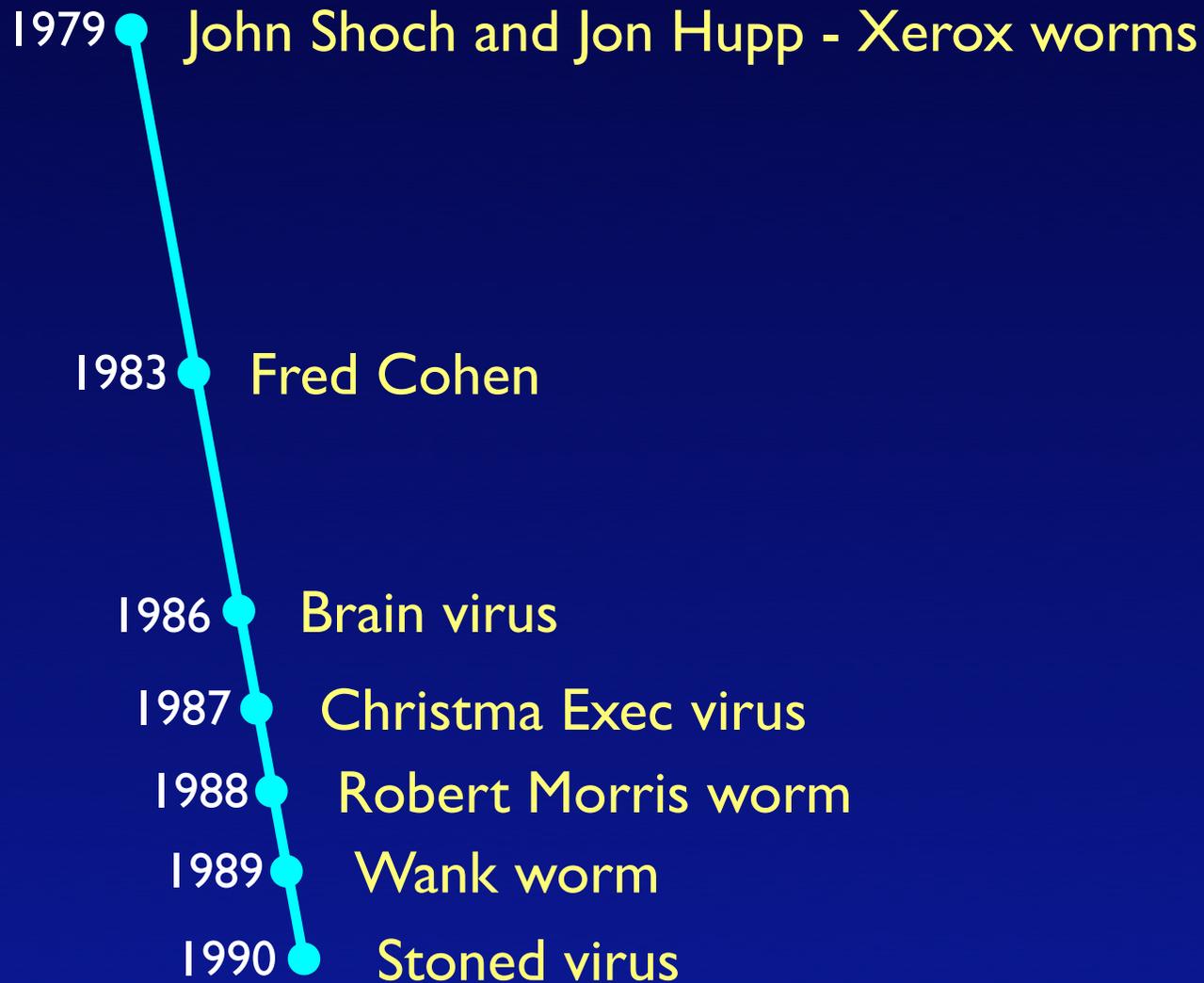
1	IIS server: buffer overflows, failure to handle unexpected requests
2	Remote Data Services component allows remote users to run commands with administrative privileges
3	SQL server: buffer overflows and various other vulnerabilities
4	Misconfiguration of network shares allows remote users full control of a host
5	Null Session connections (aka anonymous logon) allow anonymous remote users to fetch data or connect without authentication
6	LAN Manager passwords are weakly encrypted
7	User accounts with no passwords or weak passwords
8	Internet Explorer: various vulnerabilities
9	Improper permission settings allow remote access to Windows registry
10	Windows Scripting Host automatically executes .VBS scripts embedded in a file

Historical Cases

Past Trends: 4 Waves



Wave 1



Wave 1

- 1971 Bob Thomas (BBN) wrote “creeper” program that moved around ARPAnet and displayed message on computer screens challenging people to catch it
 - An annoyance more than serious program
 - In response, others wrote “reaper” programs to chase and delete “creeper” programs (first antivirus)

Wave 1 - First Worms

- 1979 John Shoch and Jon Hupp at Xerox PARC coined “worm” after network-based “tapeworm” monster in John Brunner’s “The Shockwave Rider”
 - Experimented with worms for overnight diagnostics on internal Ethernet LAN
 - One worm mysteriously got out of control and crashed several computers, reason unknown

Wave 1 - First Viruses

- 1983 Fred Cohen (PhD student at USC) conceived, wrote and demonstrated first documented virus
- Early viruses spread by diskettes among DOS computers
 - 1981 IBM-compatible PCs introduced and became most popular platform -> largest target for viruses

Wave 1 - DOS Viruses

- Early DOS viruses spread by
 - Infecting .EXE or .COM files
 - Infecting device drivers (.SYS or .DRV files)
 - Infecting boot sector of diskettes (take over initial boot sequence)

Early DOS Viruses (cont)

- 1986 early boot sector virus, Brain,
written by 2 Pakistani programmers
 - First seen at U. Maryland campus
 - Spread by infecting boot sector of floppy disks
 - Infected disk would copy itself from boot sector into memory, then monitor floppy disk drive and copy itself to any floppies used

Early DOS Viruses (cont)

- Brain was example of stealth virus: hid itself in memory by catching all DOS systems calls usually used to detect viruses and simulated responses to give appearance that it was not there
- Stealth viruses tend to be system-specific so not that widespread

Early DOS Viruses (cont)

- 1987 “Lehigh virus” spread on Lehigh U. campus
 - Infected DOS command interpreter (file “command.com”) to infect first 4 disks encountered
 - Then destroyed all disks in system by overwriting FAT (file allocation table) that keeps a list of file and directory names and disk sectors

Wave 1 - Christmas Tree

- 1987 Christma Exec virus spread by email, promising to display a Christmas tree graphic
 - Secretly emailed copies of itself to user's list of outgoing mail addresses, using user's name (to trick recipients to open the attachment)
 - Early example of social engineering attack

Wave 1 - Morris Worm

- Nov. 2, 1988 Robert Morris Jr (Cornell student) released worm that disabled 6,000 computers - 10% of Internet at the time
 - Programming bug caused worm to re-infect already infected computers, until they crashed
- First case to bring worms/viruses to public awareness

Wave 1 - Morris Worm

- First to use combination of attacks to spread
 - Exploited buffer overflow of Unix “finger” daemon: caused victim computers to run a shell code
 - Exploited debug mode of “sendmail” program: caused victims to run set of commands to copy the worm
 - Cracked password files: guessed common words from a dictionary

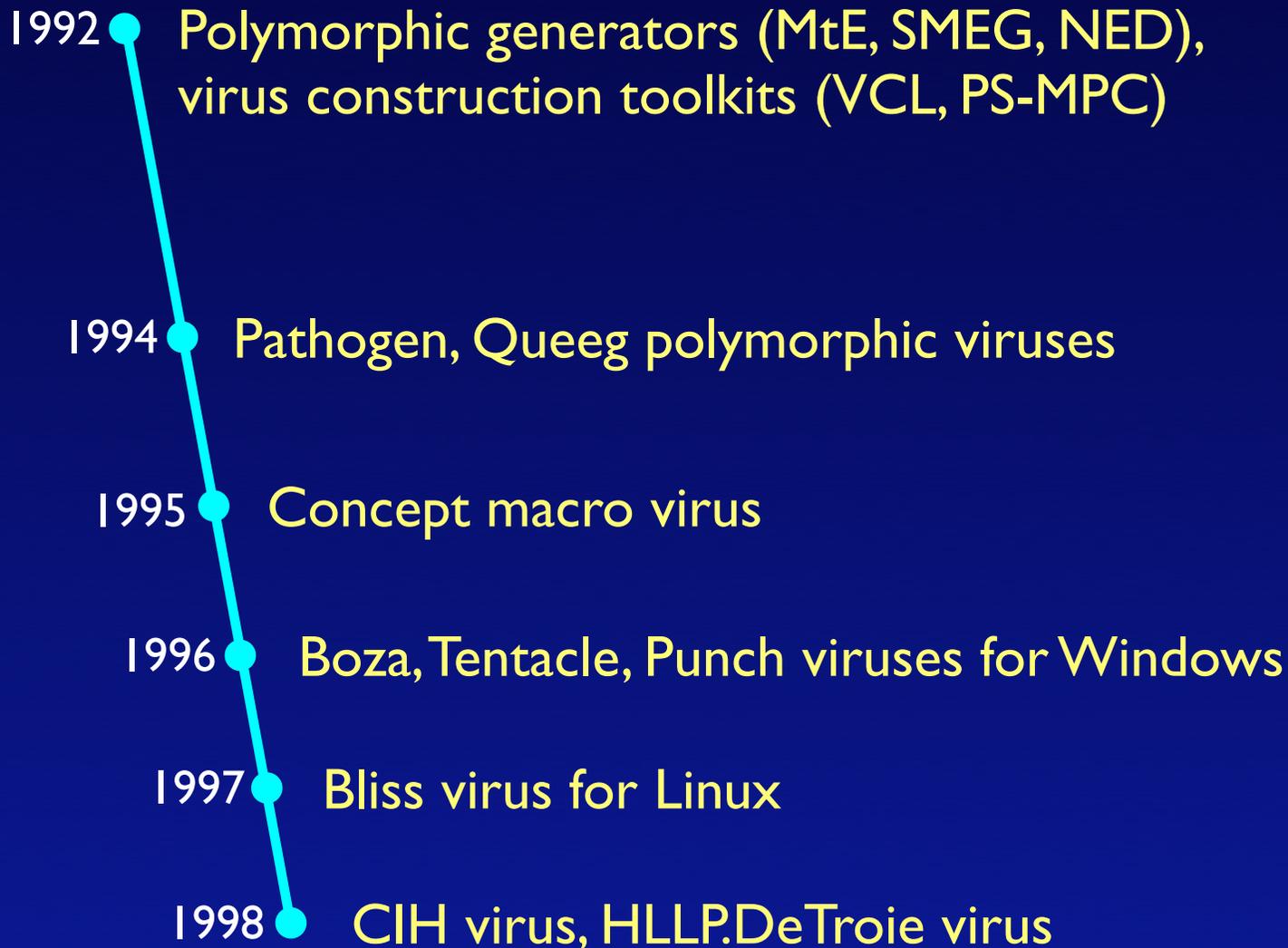
Wave 1 (cont)

- 1989 WANK (worms against nuclear killers) worm spread through DECnet by guessing default accounts and passwords (often not changed), spreading anti-war propaganda
- Stoned, Jerusalem, other viruses - mostly targeted to DOS

Wave 1 Trends

- Most viruses limited to DOS and spread slowly by diskettes
- Experiments with worms (Xerox, Morris) got out of control
- Beginnings of stealth viruses and social engineering attacks

Wave 2



Wave 2 - Encryption

- Encryption scrambles virus to hide its signature (code pattern)
 - But decryption routine stays constant -- antivirus can still detect signature of a specific decryption scheme

Without encryption

Virus and host file
(plaintext source code)

With encryption

Decrypt
routine

Virus and host file
(scrambled)

Wave 2 - Polymorphism

- 1989 polymorphic virus appeared in Europe
- Polymorphic viruses permute with each infection to avoid detection by antivirus
 - No more than a few bytes common between generations

Polymorphism (cont)

- 1992 Dark Avenger's user-friendly Mutation Engine (MtE) let anyone add polymorphism to any virus
 - Followed by many other mutation engines: TPE, NED, DAME, SMEG
 - Created high risk of false alarms for antivirus
- 1994 Pathogen and Queeg: complicated viruses created by Black Baron's SMEG

Wave 2 - Virus Toolkits

- 1992 Virus Creation Lab: user-friendly virus construction toolkit allowed anyone to generate hundreds of viruses easily
 - Followed by many other toolkits: PS-MPC, IVP
 - Antivirus companies flooded with thousands of (lame) viruses
 - Best known example: 2001 Anna Kournikova VBScript email virus

Wave 2 - Win32 Viruses

- 1995 Concept macro virus for Microsoft Word for Windows95
 - Macro viruses: easy to write and cross-platform (mostly targeted to MS Office)
- 1996 Boza, Tentacle, Punch, other viruses target Windows95
- 1997 Bliss: first virus for Linux

Wave 2 (cont)

- 1998 CIH (Chernobyl) very destructive virus
 - Overwrote PC hard disks with random data and overwrote flash ROM BIOS firmware - PCs cannot boot up
- 1998 HLLP.DeTroie virus: first to steal private data from infected PCs and send to virus creator

Wave 2 Trends

- Large-scale automated creation of viruses
- Easy polymorphism challenges antivirus software
- Most viruses target Windows
- Macro viruses go cross-platform

Wave 3



Wave 3 - Mass E-mailers

- Jan 1999 Happy99 worm spread as e-mail attachment “happy99.exe”
 - Displayed fireworks on screen for New Years Day 1999
 - Secretly modifies WSOCK32.DLL to e-mail second message (with worm) after every message sent

Wave 3 - Melissa

- March 1999 Melissa macro virus set new record, infecting 100,000 computers in 3 days
 - Launched MS Outlook and mailed itself to 50 addresses in address book
 - Infected Word normal.dot template

Wave 3 - PrettyPark

- Mid-1999 PrettyPark worm spread as e-mail with an attachment “PrettyPark.exe” showing icon of South Park character
 - Installed itself into system folder and modified Registry to ensure it runs
 - Emailed itself to addresses in Windows address book
 - Stole password data and sent to certain IRC servers

Wave 3 - ExploreZip

- June 1999 ExploreZip worm appeared to be WinZip file attached to e-mail
 - If executed, it displayed an error message but secretly installs itself into System directory
 - E-mailed itself via Outlook or Exchange to recipients in unread inbox messages, and replied to all incoming messages with a copy of itself

Wave 3 - KAK Worm

- Jan 2000 KAK worm was an embedded VBScript in HTML e-mail message with no visible text
 - Previewing or opening message in Outlook executed the script
 - Worm copied itself into Windows start-up folder, and attached itself as a signature in all outgoing e-mail

Wave 3 - Love Letter

- May 2000 Love Letter worm demonstrated social engineering attack, pretending to be e-mail love letter
 - Attachment appeared to be text but is VBScript that infects Windows and System directories and various file types
 - E-mailed itself via Outlook to everyone in address book, infected shared directories, tried to spread by IRC channels

Wave 3 - Dynamic Plug-ins

- Oct 2000 Hybris worm spread by e-mail
 - Modified WSOCK32.DLL file to send itself as a second message to same recipient after every normal message sent
 - Connected to a newsgroup to download encrypted plug-ins (code updates)
 - Potentially very dangerous - worm can get new instructions or payload at any time

Wave 3 Trends

- Mass e-mailing becomes most popular infection vector
 - Attacks increase in speed and scope
- Social engineering becomes common
- Worms start to become dangerous (data theft, dynamic plug-ins)

Wave 4



Wave 4 - Linux Worms

- Linux is targeted by Ramen worm (Jan 2001) and Lion worm (March 2001)
- Lion is very dangerous
 - Stole password data, installed rootkit “t0rn” (hides presence of worm from “syslogd” and other system utilities)
 - Installed distributed DoS agent “TFN2K”
 - Installed backdoor root shells, listens on certain ports for remote instructions

Wave 4 - More Vectors

- Feb 2001 Gnutelman/Mandragore worm infected users of Gnutella peer-to-peer networks
 - Disguises itself as a searched file
- Blended (combination) attacks:
 - May 2001 Sadmind worm targeted Sun machines and Microsoft IIS web servers
 - July 2001 Sircam spread by e-mail and network shares

Wave 4 - A Modern Worm

- July 12, 2001 Code Red I version 1 worm targeted buffer overflow vulnerability in Microsoft IIS servers
 - Tried to install DoS agent targeted to “www.whitehouse.gov”
 - Programming bug caused worm to probe same set of IP addresses instead of generate random addresses, so spread was slow

Wave 4 - Code Red

- Week later, Code Red I version 2 fixed programming bug and spread much faster
 - Infected 359,000 computers in 14 hours (peak rate of 2,000 computers per minute)
- Aug 4, Code Red II used same exploit, ran 300 parallel threads on each machine to probe for new victims
 - Worm's fast probing caused DoS-like congestion

Wave 4 - New Sophistication

- Sept 2001 Nimda worm used blended attack via 5 vectors:
 - E-mailed itself using its own SMTP engine
 - Infected MS IIS web servers via buffer overflow exploit
 - Infected network shares
 - Added Javascript to web pages, infected any web browser
 - Used backdoors left by Code Red and Sadmind

Nimda (cont)

- Nimda infected 450,000 computers in 12 hours
 - Spreading rate caused DoS-like congestion
 - Extensively modified Registry and System directory to hide its presence and make hard to remove
 - Created backdoor administrative account for remote control

Wave 4 - Armoring

- “Armored” worms attack and disable antivirus programs
- Klez (Oct 2001), Bugbear (Oct 2001), Winevar (Nov 2002), Avril (Jan 2003) look for common antivirus processes and stop them, scan hard drive for critical antivirus files and delete them
- Winevar also masquerades as a Trojan version of an antivirus program

Wave 4 - More Dangerous

- Gibe worm (March 2002) pretends to be e-mailed Microsoft security bulletin and patch, but secretly installs backdoor
- Badtrans (Nov 2001), Bugbear, Lirva, Fizzer (May 2003) worms install keystroke logging Trojan horses
- Lirva e-mails password data to virus writer, and downloads Back Orifice to infected PCs (gives complete remote control)

Wave 4 - Slammer

- Jan 2003 Sapphire/Slammer worm demonstrated that simple worm (in only one 404-byte UDP packet) could spread very fast
 - Targeted Microsoft SQL servers, hit 90 percent of vulnerable hosts within 10 minutes (120,000 machines)
 - At peak rate, infection doubled every 8.5 seconds - reached peak rate of 55,000,000 scans/sec after only 3 minutes

Wave 4 - Blaster

- August 2003 Blaster targeted DCOM RPC vulnerability on Win2000 and WinXP - demonstrated majority of PCs are vulnerable
 - Infected 400,000 computers but not nearly the maximum potential spreading rate due to bad programming
 - Carried DoS agent targeted at “www.windowsupdate.com”

Wave 4 - Sobig

- Aug 19, 2003 Sobig.F was 6th variant of Sobig, spread by e-mail among Windows PCs
 - At peak rate, Sobig.F was 1 out of every 17 e-mail messages
 - Produced 1 million copies within 24 hours
 - Preprogrammed stopping date and empty payload suggests intention was proof-of-concept

Wave 4 Trends

- New infection vectors (Linux, peer-to-peer, IRC chat, instant messaging,...)
- Blended attacks (combined vectors)
- Dynamic code updates (via IRC, web,...)
- Dangerous payloads - backdoors, spyware
- Active attacks on antivirus software
- Fast and furious spreading

Top 2004 Worms

- MyDoom spreads by email to Windows PCs, searches for email addresses in various files, opens backdoor for remote access
- Netsky spreads by email, exploits Internet Explorer to automatically execute email attachments, removes MyDoom and Bagle from PCs, carries message against Bagle worm writer

Top 2004 Worms (cont)

- Bagle spreads by email, tries to remove Netsky from PCs, opens backdoor for remote access or download files from Web
- Sasser worm exploits buffer overflow in Win2000 and WinXP on TCP port 445, FTPs itself to target

Defenses

Antivirus Software

- Goals of antivirus software:
 - Detection of virus
 - Identification of specific virus and infected program
 - Removal of virus and restoration of program to original state

Antivirus (cont)

- First generation antivirus
 - Simply scanned for known virus signatures (constant bit patterns) or changes in file length
- Second generation antivirus
 - Followed heuristic rules to search for probable infection
 - Integrity checking by adding a checksum or encrypted hash function to each program

Antivirus (cont)

- Third generation antivirus
 - Identify a set of actions that indicate an infection is being attempted and then intervene
- Fourth generation antivirus
 - Combined various techniques including file scanning, activity trapping, access control

OS Patching

- Microsoft publishes frequent patches for Windows critical vulnerabilities
- Usually worms appear some time after a patch is available
 - But many do not apply patches for various reasons
- Microsoft is studying automatic patching

Perimeter Defense

- Firewalls, intrusion detection systems, and routers can filter malicious traffic including worms
- Partially effective but
 - Needs expert configuration of filter rules or access control lists
 - Needs constant updating on new attack signatures
 - May not detect new (zero-day) exploits

Why Attacks Continue

Software Vulnerabilities

- Attacks will continue as long as computers have vulnerabilities that can be exploited
 - Software is written in unsecure manner, eg, vulnerable to buffer overflows
 - When vulnerabilities are announced, many people do not apply patches (too inconvenient, too frequent, sometimes unstable)

Legal Issues

- Who can be held accountable?
 - Software vendors have acknowledged their responsibility to produce secure software but have avoided liability
 - Virus writers are the criminals, but hard to identify and prosecute

Legal Issues (cont)

- Viruses/worms are hard to trace to creator from analysis of code, unless there are accidental clues left
 - Most skilled virus writers are too good to get caught

Legal Issues (cont)

- Prosecuted get light sentences:
 - Robert Morris - 3 years probation, \$10,000 fine
 - Onel de Guzman for LoveLetter - released due to lack of laws in Philippines
 - Jan De Wit for Anna Kournikova - 150 hours community service

Network Issues

- Most organizations use firewalls, IDSs, antivirus software, OS patching
 - Not always configured properly or kept up to date
- Worm outbreaks depend on weakest point in network defenses
 - Perimeter defenses are useless if passed through

Some Research Issues

Global Early Detection

- Worms can spread in minutes, so early detection is critical to allow time for response
- Current efforts at worldwide detection systems are limited

Global Early Detection (cont)

- Symantec DeepSight Threat Management System
 - Collects log data from hosts, firewalls, IDSs from 19,000 organizations in 180 countries
 - Symantec correlates and analyzes traffic data to track attacks by type, source, time, targets
 - Snapshot of current activity

Global Early Detection (cont)

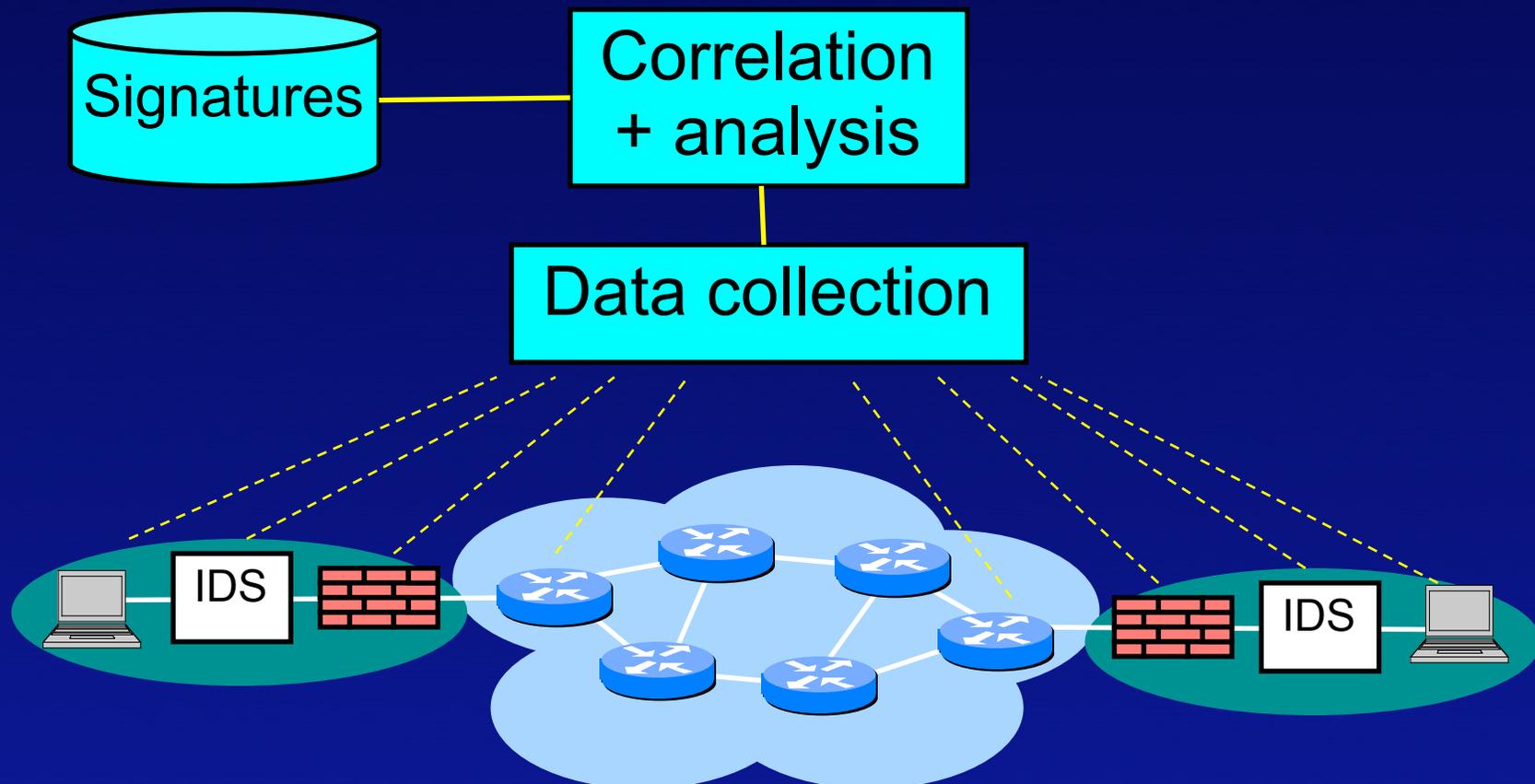
- AT&T Internet Protect Service
 - Monitors traffic data in AT&T IP backbone network as reflection of larger Internet
 - AT&T correlates and analyzes data for worms, viruses, DOS attacks
 - Threats are reported to customers

Global Early Detection (cont)

- Internet Storm Center operated by SANS and Incidents.org
 - Collects log data from 3,000 firewalls, IDSs 60 countries
 - Correlates and analyzes log data for suspicious activities
 - Claims discovery of LION worm in March 2001, detected increase in probes to port 53 (DNS)

Global Early Detection (cont)

- General architecture



Dynamic Quarantine

- Worms spread too quickly for manual response
- Dynamic quarantine tries to isolate worm outbreak from spreading to other parts of Internet
- Does not exist yet

Dynamic Quarantine (cont)

- Cisco Network Admission Control (NAC)
 - Cisco Trust Agents run on servers and desktops, collect security-related status (OS version, patch level, antivirus software running)
 - Data is sent to NAC-enabled routers
 - Routers follow security policies to decide whether machines can access network

Dynamic Quarantine (cont)

- Microsoft Network Access Protection (NAP)
 - Verify desktop PCs are securely configured with updated patches and antivirus software
 - Unsecure PCs are not allowed to access network, and may be automatically shut down

Dynamic Quarantine (cont)

- Rate throttling
 - Proposed to limit number of new connections made per time interval
 - Legitimate traffic does not open many new connections, but worms do
 - Rate throttling is viewed as “benign” control
 - slows down worms with no effect on legitimate traffic

Conclusions

- New worms expected to be fast and more dangerous
 - Current solutions only partially effective
- Major research problems include
 - How to detect new worms early
 - How to prevent catastrophic spreading