COMP3028 Lecture 12
Malware

This Lecture

- Malicious code: Malware
  - Vectors
  - Viruses
  - Trojan horses
  - Logic bombs
  - Worms
  - Ransomware

Malware

- A common characteristic of all types of malware is that it needs to be executed in order to cause harm
- How might malware get executed?
  - User action
    - Downloading and running malicious software
    - Viewing a web page containing a malicious ActiveX control
    - Opening an executable email attachment
    - Inserting a CD
  - Exploiting an existing flaw in a system
    - Buffer overflows in network daemons
    - Buffer overflows in email clients or web browsers

Exploit Vectors

- Vector - specifically when talking about malicious code, is the method that this code uses to propagate itself or infect a computer.
- Usually will be a software vulnerability
- Or someone clicked something he/she should hot have!

Viruses

- A virus is a particular kind of malware that infects other files
  - Traditionally, a virus could only infect executable programs
  - Nowadays, many data document formats can contain executable code (such as macros)
    - Many different types of files can be infected with viruses now
- Typically, when the file is executed (or sometimes just opened), the virus activates, and tries to infect other files with copies of itself
- In this way, the virus can spread between files, or between computers
- Notable computer viruses (see Wikipedia)

Infection

- What does it mean to “infect” a file?
- The virus wants to modify an existing (non-malicious) program or document (the host) in such a way that executing or opening it will transfer control to the virus
  - The virus can do its “dirty work” and then transfer control back to the host
- For executable programs:
  - Typically, the virus will modify other programs and copy itself to the beginning of the targets' program code
- For documents with macros:
  - The virus will edit other documents to add itself as a macro which starts automatically when the file is opened

Infection

- In addition to infecting other files, a virus will often try to infect the computer itself
  - This way, every time the computer is booted, the virus is automatically activated
- It might put itself in the boot sector of the hard disk
- It might add itself to the list of programs the OS runs at boot time
- It might infect one of more of the programs the OS runs at boot time
- It might try many of these strategies
  - But it's still trying to evade detection!

Spreading

- How do viruses spread between computers?

- Usually, when the user sends infected files (hopefully not knowing they're infected!) to his friends
  - Or puts them on a p2p network

- A virus usually requires some kind of user action in order to spread to another machine
  - If it can spread on its own (via email, for example), it's more likely to be a worm than a virus

Payload

- In addition to trying to spread, what else might a virus try to do?
- Some viruses try to evade detection by disabling any active virus scanning software
- Most viruses have some sort of payload
- At some point, the payload of an infected machine will activate, and something (usually bad) will happen
    - Erase your hard drive
    - Subtly corrupt some of your spreadsheets
    - Install a keystroke logger to capture your online banking password
    - Start attacking a particular target website

Spotting viruses

- When should we look for viruses?
  - As files are added to our computer
    - Via portable media
    - Via a network
  - From time to time, scan the entire state of the computer
    - To catch anything we might have missed on its way in
    - But of course, any damage the virus might have done may not be reversible
- How do we look for viruses?
  - Signature-based protection
  - Behaviour-based protection

Signature-based protection

- Keep a list of all known viruses
- For each virus in the list, store some characteristic feature (the signature)
  - Most signature-based systems use features of the virus code itself
    - The infection code
    - The payload code
  - Can also try to identify other patterns characteristic of a particular virus
    - Where on the system it tries to hide itself
    - How it propagates from one place to another

Polymorphism

- To try to evade signature-based virus scanners, some viruses are polymorphic
  - This means that instead of making perfect copies of itself every time it infects a new file or host, it makes a modified copy instead
  - This is often done by having most of the virus code encrypted
    - The virus starts with a decryption routine which decrypts the rest of the virus, which is then executed
    - When the virus spreads, it encrypts the new copy with a newly-chosen random key
- How would you scan for polymorphic viruses?

Behaviour-based protection

- Signature-based protection systems have a major limitation
  - You can only scan for viruses that are in the list!
  - But there are several brand-new viruses identified every day
    - Currently 70-75 thousand
  - What can we do?

- Behaviour-based systems look for suspicious patterns of behaviour, rather than for specific code fragments
  - Of course, this is only useful post-infection

False negatives and positives

- Any kind of test or scanner can have two types of errors:
  - False negatives: fail to identify a threat that is present
  - False positives: claim a threat is present when it is not

- Which is worse?

- How do you think signature-based and behaviour-based systems compare?

Trojan horses

- Trojan horses are programs which claim to do something innocuous (and usually do), but which also hide malicious behaviour

You're surfing the Web and you see a button on the Web site saying, "Click here to see the dancing pigs." And you click on the Web site and then this window comes up saying, "Warning: this is an untrusted Java applet. It might damage your system. Do you want to continue? Yes/No." Well, the average computer user is going to pick dancing pigs over security any day. And we can't expect them not to.

-- Bruce Schneier

Trojan horses

- Trojan horses:
  - Gain control by getting the user to run code of the attacker's choice, usually by also providing some code the user *wants* to run
    - “PUP” (potentially unwanted programs) are an example
  - The payload can be anything; sometimes the payload of a Trojan horse is itself a virus, for example
  - Trojan horses usually do not themselves spread between computers; they rely on multiple users executing the “trojaned” software
    - Better: users share the trojaned software on p2p networks

Notable Trojan horses

- 1989: The AIDS Trojan, encrypt all files filenames on the system and requests a ransom
- 2002: Beast, affects Windows machines from 95 – XP and provides the attacker with a remote admin tool (RAT) – there are a lot of these types
- 2013: Cryptolocker, a massive ransomware

Logic bombs

- A logic bomb is malicious code hiding in the software already on your computer, waiting for a certain trigger to “go off” (execute its payload)

- Logic bombs are usually written by “insiders”, and are meant to be triggered sometime in the future
  - After the insider leaves the company

- The payload of a logic bomb is usually pretty dire
  - Erase your data
  - Corrupt your data
  - Encrypt your data, and ask you to send money to some offshore bank account in order to get the decryption key!

Logic bombs

- What is the trigger?
- Usually something the insider can affect once he is no longer an insider
  - Trigger when this particular account gets three deposits of equal value in one day
  - Trigger when a special sequence of numbers is entered on the keypad of an ATM
  - Just trigger at a certain time in the future (called a “time bomb”)

Spotting Trojan horses and logic bombs

- Spotting Trojan horses and logic bombs is extremely tricky. Why?

- The user is intentionally running the code!
  - Trojan horses: the user clicked “yes, I want to see the dancing pigs”
  - Logic bombs: the code is just (a hidden) part of the software already installed on the computer

- Don't run code from untrusted sources?
- Better: prevent the payload from doing bad things
  - More on this later

Worms

- A worm is a self-contained piece of code that can replicate with little or no user involvement
- Worms often use security flaws in widely deployed software as a path to infection
- Typically:
  - A worm exploits a security flaw in some software on your computer, infecting it
  - The worm immediately starts searching for other computers (on your local network, or on the Internet generally) to infect
  - There may or may not be a payload that activates at a certain time, or by another trigger

The Morris worm

- The first Internet worm, launched by a graduate student at Cornell in 1988
- Once infected, a machine would try to infect other machines in three ways:
  - Exploit a buffer overflow in the “finger” daemon
  - Use a back door left in the “sendmail” mail daemon
  - Try a “dictionary attack” against local users' passwords. If successful, log in as them, and spread to other machines they can access without requiring a password
- All three of these attacks were well known!
- Thousands of systems were offline for several days

The Code Red worm

- Launched in 2001
- Exploited a buffer overflow in Microsoft's IIS web server (for which a patch had been available for a month)
- An infected machine would:
  - Deface its home page
  - Launch attacks on other web servers (IIS or not)
  - Launch a denial-of-service attack on a handful of web sites, including www.whitehouse.gov
  - Installed a back door and a Trojan horse to try to prevent disinfection
- Infected 250,000 systems in nine hours

The Slammer worm

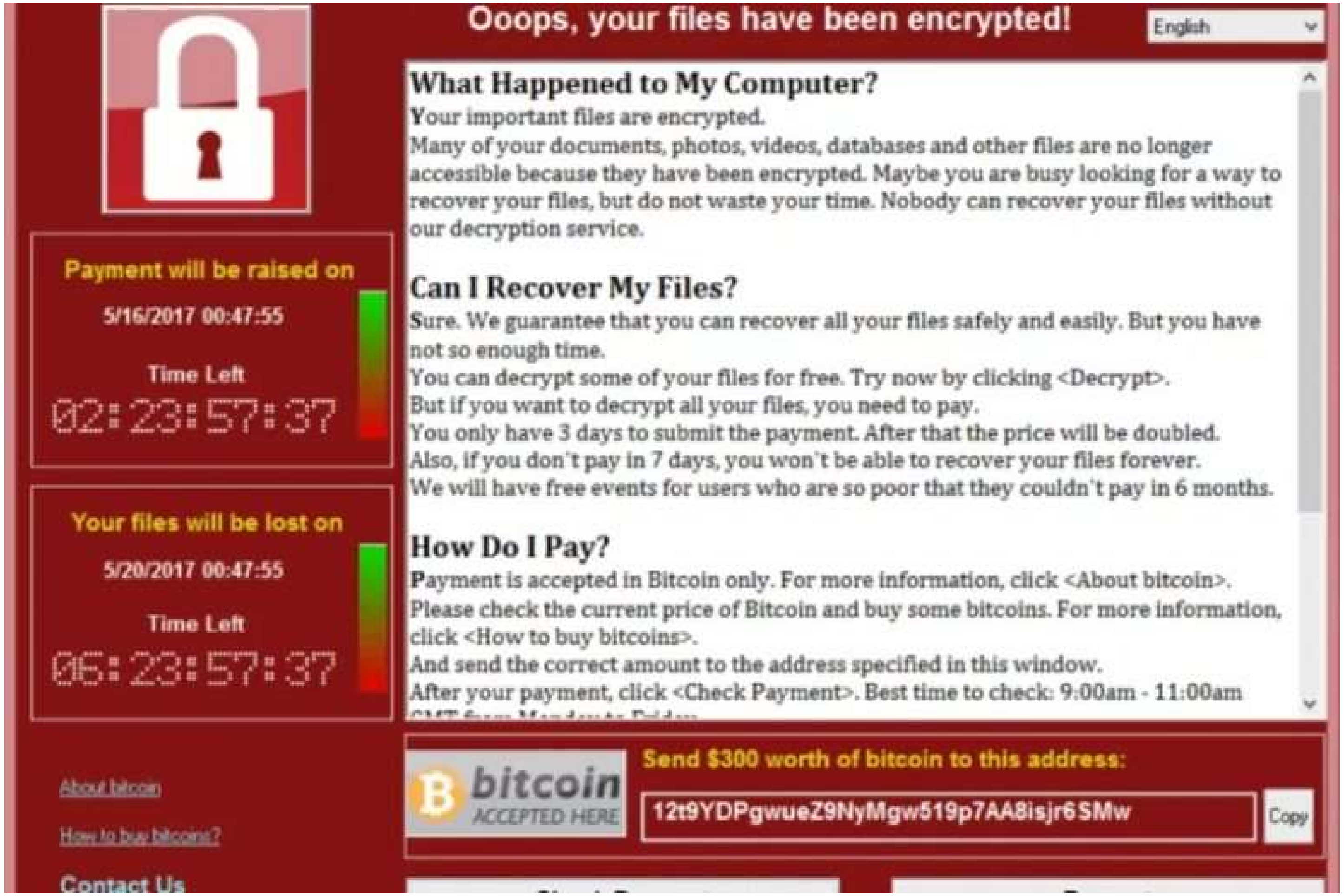
- Launched in 2003
- First example of a “Warhol worm”
  - A worm which can infect nearly all vulnerable machines in just 15 minutes
- Exploited a buffer overflow in Microsoft's SQL Server (also having a patch available)
- A vulnerable machine could be infected with a single UDP packet!
  - This enabled the worm to spread extremely quickly
  - Exponential growth, doubling every 8.5 seconds
  - 90% of vulnerable hosts infected in 10 minutes

Other notable worms

- 1999, Melissa, Not originally intended as harmful, but crashed servers by flooding them with e-mail
- 2000, the ILOVEYOU worm, one of the most damaging worms ever, shows how powerful social engineering can be
- 2004, Sasser, Network worm. At startup, it kills the process lsass.exe, a windows process which handles file permissions. Killing lsass causes the computer to reboot one minute later, which would cause sasser to run again. This would continue in an infinite loop until the computer is shut down manually.

Ransomware

- 2013-2015 saw the rise of Ransomware



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

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

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Ransomware

- Will usually encrypt or block access to files and demand a ransom
- It is a clever solution, because if the antivirus system removes it, it is often too late
- Usually distributed on malicious websites, or already infected machines
- The file decryption keys are protected by encrypting using the public key of a C&C server

Ransomware Variants

- Most of the challenge in successfully using ransomware is tricking a user into running it, and bypassing antivirus and browser protection
  - fake emails
  - Malicious web pages
  - Obfuscated Javascript attachments
  - Deployed using exploit kits

Notable Ransomware

- In May 2017, the **WannaCry** ransomware attack spread through the Internet, using an exploit vector named **EternalBlue**, which was leaked from NSA. The attack infected more than 230,000 computers in over 150 countries, using 20 different languages to demand money from users using Bitcoin cryptocurrency. The attackers gave their victims a 7-day deadline from the day their computers got infected, after which the encrypted files would be deleted.

Summary

- Malicious code: Malware
  - Vectors
  - Viruses
  - Payloads
  - Trojan horses
  - Login bombs
  - Worms
  - Ransomware