The Priciest Computer Viruses

At least the ones we know about

Konrad Pagacz, 26.01.2022

Mydoom

- caused estimated damage of $38 billion in 2004 (inflation-adjusted score is actually around $52.2 billion
- technically a “worm” - a self-contained virus not needing another software to execute and spread
- spread by mass emailing - at one point mydoom was responsible for 25% of all emails sent via www
- scraped addresses from infected machines, then sent copies of itself to those addresses
- also roped infected computers into a web of computers called a botnet that performed distributed denial of service (DDoS) attacks
- the source code is actually available to view, e.g. here: https://github.com/yorickdewid/MyDoom

WannaCry

- the 2017 WannaCry computer virus is a ransomware (a virus that takes over the host machine and holds them hostage)
- the virus infected over 200 000 computers worldwide and stopped when a 22-year-old security researcher in the U.K. found a way to turn it off
- Racked up a total $4 billion in damages

MEMZ

- a trojan virus supposedly created as a joke as explained by its creator
- the trojan alerts the user to the fact that it is a trojan ans warns them that if they proceed, the computer may no longer be usable
- it contains complex payloads corrupting the system, displaying artefacts on the screen as it runs
- once run, the application cannot be closed without causing further damage to the computer which will stop functioning properly regardless
- when the host is restarted, in place of the bootsplash is a message that reads “You computer has been trashed by the MEMZ Trojan. Now enjoy the Nyan cat..” followed by an animation of the Nyan Cat.

Malware glossary

- rootkit
- backdoor
- trojan horse
- virus
- worm
- spyware
- ransomware
- botnet
- logic bomb

- Rootkit
  - a collection of software designed to enable access to a computer or area of its software that is not otherwise allowed (for example, to an unauthroized user) and often masks its existence or the existence of other software.
- Backdoor
  - a typically covert method of bypassing normal authentication or encryption in a computer, product, embedded device or its embodiment. Often used for securing remote access to a computer.
- Spyware:
  - software with malicious behaviour that aims to gather information about a person or organisation and send it to another entity in a way that harms the user
- Virus
  - when executed, replicates itself by modifying other computer programs and inserting its own code

- Ransomware
  - a type of malware that threatens to publish the victim’s personal data or perpetually block access to it unless a ransom is paid
- Botnet
  - a number of internet-connected devices, each of which runs one or more bots. Can be used to perform DDoS attacks, steal data, send spam and allow the attacker to access the device and its connection
- Logic bomb
  - a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files, should they ever be terminated from the company

- Payload
  - in the context of a computer virus or worm, the payload is the portion of the malware which performs malicious action
- Polymorphic engine
  - sometimes called mutation engine or mutating engine
  - is a software component that uses polymorphic code to alter the payload while preserving the same functionality
  - the purpose is to make it ahrder for antivirus software to detect a virus
- Cross-site scripting (XSS)
  - a type of security vulnerability that can be found in some web applications. XSS attacks enable attackers to inject client-side scripts into web pages viewed by other users