Computer Infections

Case Studies

ICTSAS308

aie
SPECIALIST EDUCATORS IN
GAMES, ANIMATION & FILM VFX

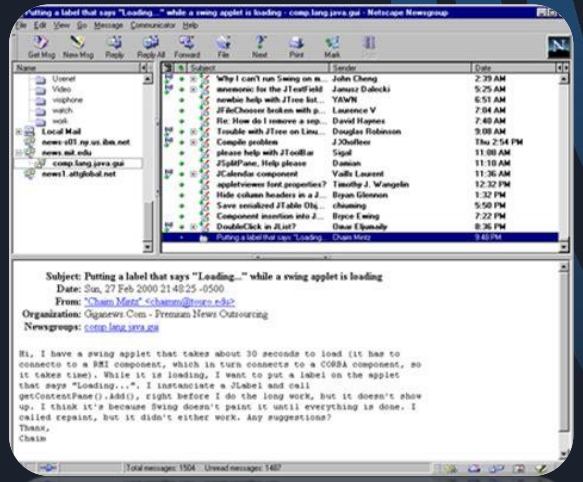
Contents

- We'll *investigate* some famous Case Studies
  - Melissa virus
  - ILOVEYOU worm
  - MyDoom worm
  - Slammer worm
  - CryptoLocker ransomware

aie
SPECIALIST EDUCATORS IN
GAMES, ANIMATION & FILM VFX

Melissa virus

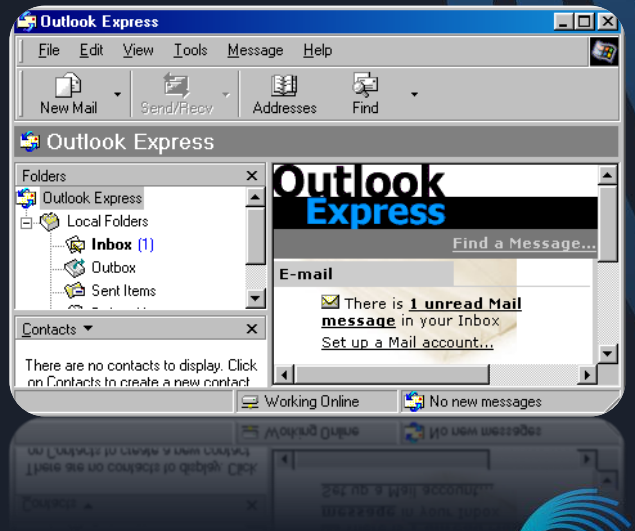
- The Melissa virus was a mass-mailing macro virus
  - Targeted MS Word and Outlook-based software
- David Smith posted his attachment in newsgroups, suggesting it contained a *list of access codes* for well-known websites
- His intention was for victims to open the attachment, which then automatically ran the macro and infected their MS software



aie
SPECIALIST EDUCATORS IN GAMES, ANIMATION & FILM VFX

Melissa virus

- The virus changed security settings and made machines vulnerable to subsequent attacks
- After this, it sent emails with the attachment to 50 contacts, thus propagating the virus
- On December 10, 1999, David Smith pleaded guilty to releasing the virus and was sentenced to 10 years
- Estimated cost:
  - $80 million



aie
SPECIALIST EDUCATORS IN GAMES, ANIMATION & FILM VFX

ILOVEYOU worm

- The ILOVEYOU worm was another macro-based infection
- Released in 2000, it swept through banks, securities firms, and Web companies at a time when users were *less informed and more naive*
- It was propagated in an email attachment entitled “I Love you”

aie
SPECIALIST EDUCATORS IN
GAMES, ANIMATION & FILM VFX

ILOVEYOU worm

- Victims being curious types, clicked into the email and opened the attachment, thus running the macro
- It overwrote system & personal files and propagated using email
- Estimated cost:
  - $15 billion

aie
SPECIALIST EDUCATORS IN GAMES, ANIMATION & FILM VFX

MyDoom worm

- The MyDoom worm is considered to be the one of the *most damaging* ever released
  - Was the *fastest-spreading* email-based worm ever

- Released in 2004, it affected companies like Microsoft & Google with a Denial-of-Service

- A DOS attack attempts to clog up internet traffic that 'denies' access to the server

aie
SPECIALIST EDUCATORS IN GAMES, ANIMATION & FILM VFX

MyDoom worm

- It spammed junk emails through infected computers at such a rate that servers were unable to cope with the traffic
- In 2004, approximately 16-25% of *all* emails had been infected
- Estimated cost:
  - $38 billion

aie
SPECIALIST EDUCATORS IN GAMES, ANIMATION & FILM VFX

Slammer worm

- The Slammer worm infected Microsoft SQL servers
  - Software used to manage databases
- After a few minutes from infecting its first victim, it was doubling itself *every few seconds*.
- 15 minutes in and Slammer had infected half of the servers that essentially ran the internet.

aie
SPECIALIST EDUCATORS IN GAMES, ANIMATION & FILM VFX

Slammer worm

- On initiation, an MS SQL server started spewing millions of Slammer clones, targeting computers at random
- By swamping internet traffic, servers crashed or were denied service
- Estimated cost:
  - $1 Billion

aie
SPECIALIST EDUCATORS IN GAMES, ANIMATION & FILM VFX

CrytpoLocker ransomware

- CryptoLocker is one of the newest types of malware called ransomware
  - A kind of malware that takes your computer files hostage

- Released in Sep 2013, CryptoLocker spread through email attachments

aie
SPECIALIST EDUCATORS IN GAMES, ANIMATION & FILM VFX

CrytpoLocker ransomware

- It encrypted user files so that they couldn't access them
- The program then used blackmail
  - Would only send a decryption key in return for a sum of money
- Estimated cost:
  - 500,000 victims returned $30 million in 100 days

aie
SPECIALIST EDUCATORS IN GAMES, ANIMATION & FILM VFX

Summary

- We *investigated* famous Case Studies of malware
- *Discovered* how they infiltrated a system
- *Discussed* how they propagated across a network

aie
SPECIALIST EDUCATORS IN
GAMES, ANIMATION & FILM VFX

References

- Norton. 2019. Famous Computer Viruses. [ONLINE] Available at: https://uk.norton.com/norton-blog/2016/02/the_8_most_famousco.html. [Accessed 4 July 2019].

- Wired. 2019. Slammer. [ONLINE] Available at: https://www.wired.com/2003/07/slammer/. [Accessed 4 July 2019].

- National Archives. 2019. Melissa virus. [ONLINE] Available at: https://webarchive.nationalarchives.gov.uk/20050302072533/http://www.dti.gov.uk/bestpractice/assets/security/virus_case_studies.pdf. [Accessed 4 July 2019].

aie
SPECIALIST EDUCATORS IN GAMES, ANIMATION & FILM VFX

References

- Wikipedia. 2019. Melissa virus. [ONLINE] Available at: https://en.wikipedia.org/wiki/Melissa_(computer_virus). [Accessed 4 July 2019].

- Sophos. 2019. CryptoLocker ransomware. [ONLINE] Available at: https://nakedsecurity.sophos.com/2013/10/18/cryptolocker-ransomware-see-how-it-works-learn-about-prevention-cleanup-and-recovery/. [Accessed 4 July 2019].

- CNN Money. 2019. ILoveYou virus. [ONLINE] Available at: https://money.cnn.com

- Wikipedia. 2019. MyDoom. [ONLINE] Available at: https://en.wikipedia.org/wiki/Mydoom. [Accessed 4 July 2019].

aie
SPECIALIST EDUCATORS IN GAMES, ANIMATION & FILM VFX