Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

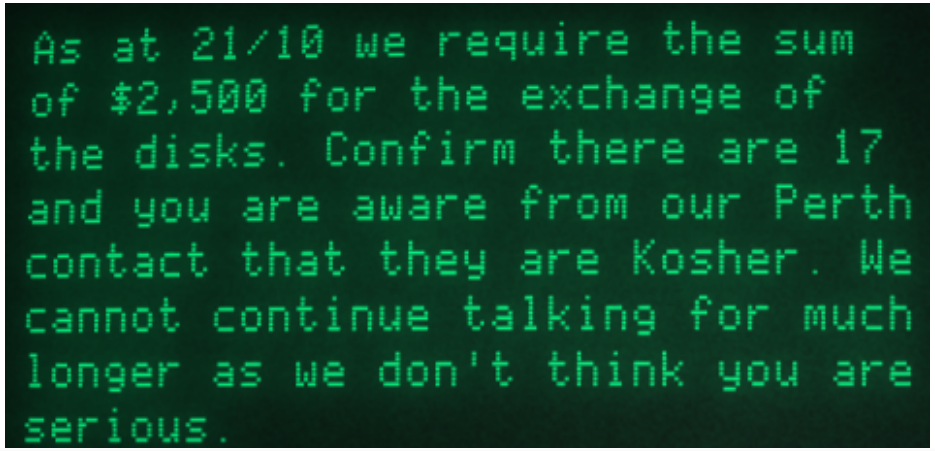
History and Evolution of Ransomware

Prof. Dr. Bruce Nikkel

1980s - Early Data Ransom Examples

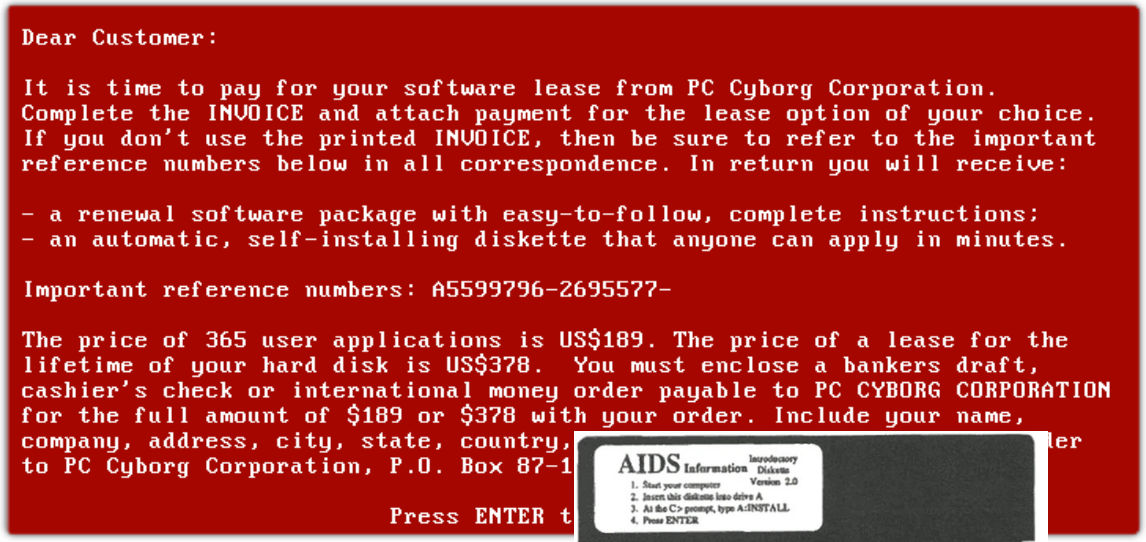
1981: Stolen Floppy Disks held Ransom

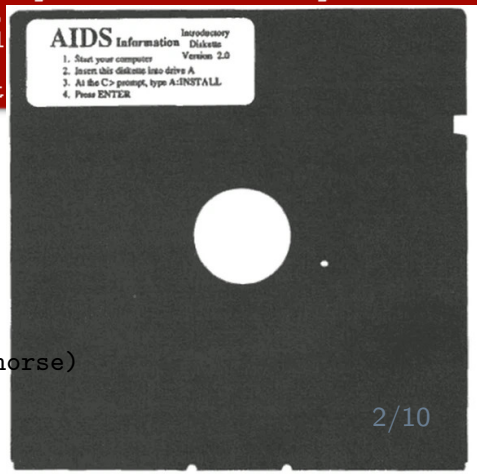
- From America's Cup in Australia
- 17 floppies with telemetry data
- Negotiation over dial-up BBS
- Initial ransom demand $10k



1989: Aids Computer Virus

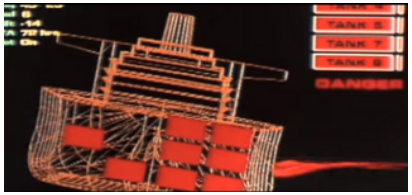
- Targeted AIDS researchers
- 20,000 infected floppies?
- Message after 90 boots
- Demand $189 licence fee
- Send to Panama P.O. Box
- File/directory names encrypted, not content
- Keys recoverable from binary

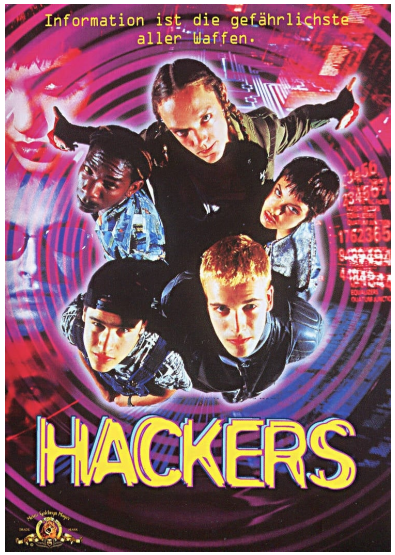




https://catless.ncl.ac.uk/Risks/4/23#subj2 https://en.wikipedia.org/wiki/AIDS_(Trojan_horse)

1990s - Research and Entertainment





1995 Movie: Hackers

- Insider infects oil tankers with virus called DaVinci
- Threatens to release oil and sink ships unless money is paid
- Group of teenage hackers are framed and expose the insider
- "*...unless 5 million dollars are transferred to the following numbered account in the next 7 days, I will capsize 5 oil tankers.*"

1996 Academic Research: Cryptovirology

- Academic researchers suggest the possibility of ransomware
- Coined the term "cryptovirology"
- Young, A. and Yung, M. Cryptovirology: Extortion-based security threats and countermeasures. In Proceedings of the IEEE Symposium on Security and Privacy, (1996), 129140.

`https://www.imdb.com/title/tt0113243` `https://www.cryptovirology.com/`

Advancing Technology for Humanity

2000 - 2005 Extortion and Forced Control Examples

2000(1999): CD Universe

- CD Universe site hacked by "Maxim"
- 300k users affected, 25k credit cards stolen
- Message sent by fax:
  "*pay me $100,000 and I'll fix your bugs and forget about your SHOP FOREVER.....or I'll sell your cards and tell about this incident in news.*"
- Money not paid, card info published on Internet

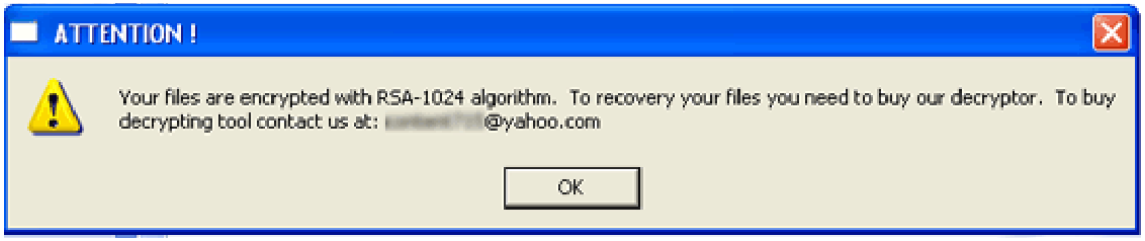
2005 Sony BMG's DRM Rootkit

- XCP - Extended Copy Protection
- Installed when a CD is played on a computer
- Like malware (rootkit, conceal, phone home)
- Prevented other programs from accessing the CD
- Similarities to ransomware (PC/CDROM hostage-taking)

https://en.wikipedia.org/wiki/Sony_BMG_copy_protection_rootkit_scandal

https://www.nytimes.com/2000/01/10/business/thief-reveals-credit-card-data-when-web-extortion-plot-fails.html

2005 - 2010 Ransom Examples with Encrypted Files



2005: pgpcoder or gpcode

- Binary has list of file extensions to encrypt
- Tells victim to send an email to given address
- Email response: "*The price of decryptor is 200 USD. For payment you may use one of following variants: 1. Payment to E-Gold account 5437838 (www.e-gold.com). 2. Payment to Liberty Reserve account U6890784 (www.libertyreserve.com).*"

2009: Manual Encrypt and Ransom

- Virginia state website for pharmacists hacked, published by Wikileaks
- "*I have your shit! In *my* possession, right now, are 8,257,378 patient records and a total of 35,548,087 prescriptions. Also, I made an encrypted backup and deleted the original. Unfortunately for Virginia, their backups seem to have gone missing, too. Uhoh :(For $10 million, I will gladly send along the password.*"

https://rump2008.cr.yp.to/6b53f0dad2c752ac2fd7cb80e8714a90.pdf

http://voices.washingtonpost.com/securityfix/2009/05/hackers_break_into_virginia_he.html

http://wikileaks.org/wiki/Over_8M_Virginian_patient_records_held_to_ransom,_30_Apr_2009

2010 - 2015 Growth and Professionalism

Bitcoin enables easier money laundering and less risk, ransomware proliferates...

- 2011: police ransomware (or scareware) Europol holds meeting to discuss

  https://blog.emsisoft.com/en/3699/2011-ransomware-renaissance

  https://www.europol.europa.eu/sites/default/files/publication

- 2012: Citadel banking malware delivers reveton ransomware

  https://pdf.ic3.gov/2012_IC3Report.pdf

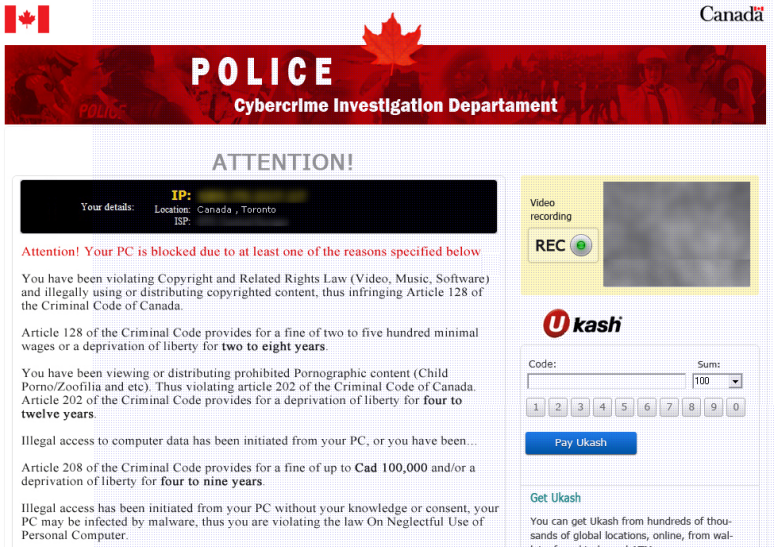
- 2013/2014: cryptolocker, cryptowall

  https://www.ic3.gov/Media/PDF/AnnualReport/2013_IC3Report.pdf

  https://www.us-cert.gov/ncas/alerts/TA13-309A

- 2014/2015: ctb-locker, TorrentLocker, Scatter, Cryakl, others

Opportunistic ransomware targeting anyone, reliable, must always provide decryption keys! Victims must trust the criminals will deliver.



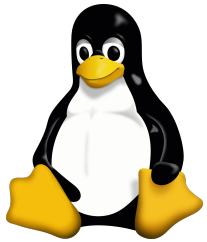
2015 - 2020 Scalability and Refinement

Examples of mass distribution and infection

- 2016: Locky, millions of phishing emails per week
- 2017: WannaCry, Petya, NotPetya

Examples of sophistication and refinement

- Multi-platform: Mac and Linux variants
- Starting to research and select targets
- Pre-attack phase - lateral movement to destroy/encrypt backups first
- 2019: MAZE, data exfiltration for additional extortion -> "extortionware"



https://www.avg.com/en/signal/mac-ransomware-remove-protect

https://en.wikipedia.org/wiki/Linux.Encoder

https://www.hhs.gov/sites/default/files/maze-ransomware.pdf

2020/2021 Enhancement and Creativity

RaaS - Ransomeware as a Service:

- Underground economy, renting components, outsourcing services
- Botnets, hosting, spamming, etc: supported service
- Ryuk, REvil, Cerber, Darkside, GandCrab, Locky, others

Re-extortion:

- months after first ransom was paid, criminals approach victims again
- criminals demand additional money

Fake Ransomware:

- Website defacement
- Not encrypted, just a visual
- Countdown timer for dramatic effect

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-enabler-of-widespread-attacks
https://cyware.com/news/re-extortion-by-ransomware-an-increasing-trend-48be439e
https://threatpost.com/fake-ransomware-infection-wordpress/176410/
https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/

US DOJ gives ransomware same priority as terrorism, starts global initiatives

Future?

Fantasy predictions about the future...

- Expanding from theft-of-data to theft-of-control
- IoT: many devices, many small payments (update/controller server compromise)
- Supply chain extortion - threaten to harm a company's customers (lose business, damage reputation)
- Self-driving car hijacking/kidnapping?
- Industrial IoT control: extortion involving medical devices, Industry 4.0 infra?
- Smart: homes, cars, buildings, etc.
- Insurance companies still cover ransom?
- Legislation criminalizing ransomware payments?

Thanks!

Contact me: bruce.nikkel@bfh.ch

Slides available on my website: `https://digitalforensics.ch`

Interested in computer history?
Visit the Enter computer museum in Solothurn.
Group tours can be arranged. Great for team events!
`https://enter.ch/`

ENTER.ch
Das Museum
für Computer und
Unterhaltungselektronik