University of Applied Sciences and Arts Northwestern Switzerland
School of Life Sciences

S1 Personal Security
D4 – Data and Ethics

Agenda

KW		Date	#	Topics	LernSetting WI	Lecturer
38 39	Self Study	First 2 weeks	0	Awareness - Entry Test with Moodle Test (20% counted to course grade)	Virtual	Selfstudy
38		KW38	0 + 7	Coaching Session (according to the information of the respective school)	on site	JRN= Juchler Norman Rerabek Martin Nyfeler Matthias
38	Fr, afternoon	23.09.2022	1	Personal Security	Virtual	Pascal Moriggl
39		KW39	1	Coaching Session	on site	FHNW: Pascal Moriggl ZHAW: JRN
39	Fr, afternoon	30.09.2022	2	Information Security & Cybersecurity I	Virtual	Petra M. Asprion
40		KW40	2	Coaching Session	on site	FHNW: Petra M. Asprion ZHAW: JRN
40	Fr, afternoon	07.10.2022	3	Information Security & Cybersecurity II	Virtual	Petra M. Asprion
41		KW41	3	Coaching Session	on site	FHNW: Pascal Moriggl ZHAW: JRN
41	Fr, afternoon	14.10.2022	4	Data Stewardship I	Virtual	Pascal Moriggl
42		KW42	4	Coaching Session	on site	FHNW: Pascal Moriggl ZHAW: JRN
42	Fr, afternoon	21.10.2022	5	Data Stewardship II	Virtual	Pascal Moriggl
43		KW43	5	Coaching Session	on site	FHNW: Pascal Moriggl ZHAW: JRN
43	Fr, afternoon	28.10.2022	6	Data Ethics	Virtual	Pascal Moriggl
44		KW44	6	Coaching Session	on site	FHNW: Pascal Moriggl ZHAW: JRN
44	Fr, afternoon	04.11.2022	7	Data Privacy	Virtual (Flipped Classroom)	Pascal Moriggl

Relevance

Is Cybersecurity / Information Security relevant in 2021 for companies in Switzerland?

Otto Hostettler / 6. Oktober 2021
https://www.beobachter.ch/digital/sicherheit/dramatischer-anstieg-der-angriffe-hacker-sturzen-sich-auf-schweizer-firmen

Von Mark K. Peter (FHNW), Nicolas Mayencourt
https://shop.beobachter.ch/buchshop/arbeit/it-sicherheit-fuer-kmu

Relevance

As technology continued to evolve, hacking became more complicated in the years that followed, and a series of major data breaches largely characterize this era today.

- **Snowden & The NSA, 2013.** Edward Snowden - a former CIA employee and U.S. government contractor - copied and shared classified information from the National Security Agency (NSA), revealing that the government was actually "spying" on the public. To some, he is considered a hero; to others, a traitor.
- **Yahoo, 2013-2014.** hackers broke into Yahoo and compromised the accounts and personal data of all three billion users. The company was fined $35 million for failing to report the intrusion in a timely manner, and Yahoo's sales price dropped by $350 million as a result.
- **WannaCry, 2017.** widely known as the first "ransomware worm." WannaCry targeted computers running the Microsoft Windows operating system and demanded ransom payments in the cryptocurrency Bitcoin. In just one day, the worm infected over 230,000 computers in 150 countries.

Relevance

Internet

Yahoo: Daten von mindestens 500 Millionen Nutzern gestohlen

Bisher größter Datenklau?

23. September 2016, 17:10 Uhr

Sunnyvale (dpa) - Es könnte der größte Datenklau der Geschichte sein: Dem Internet-Konzern Yahoo wurden im Jahr 2014 Informationen zu mindestens einer halben Milliarde Nutzer gestohlen. Es geht um Namen, E-Mail-Adressen, Telefonnummern, Geburtsdaten und verschlüsselte Passwörter.

Watch the video.
https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html

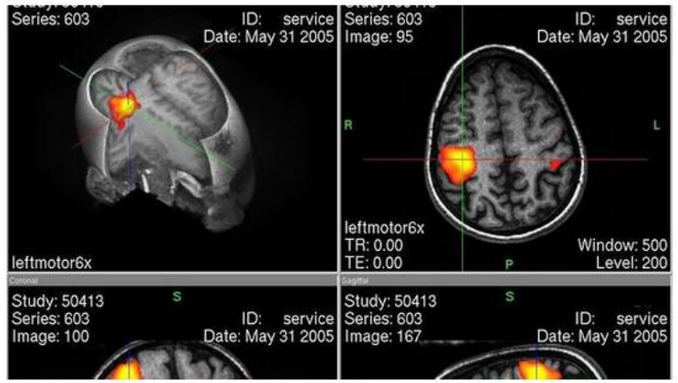
Why are there no simple solutions?

heise online > News > 2015 > KW 13 > Häufige Sicherheitsmeldungen langweilen Nutzer

23.03.2015 16:03 « Vorige | Nächste »

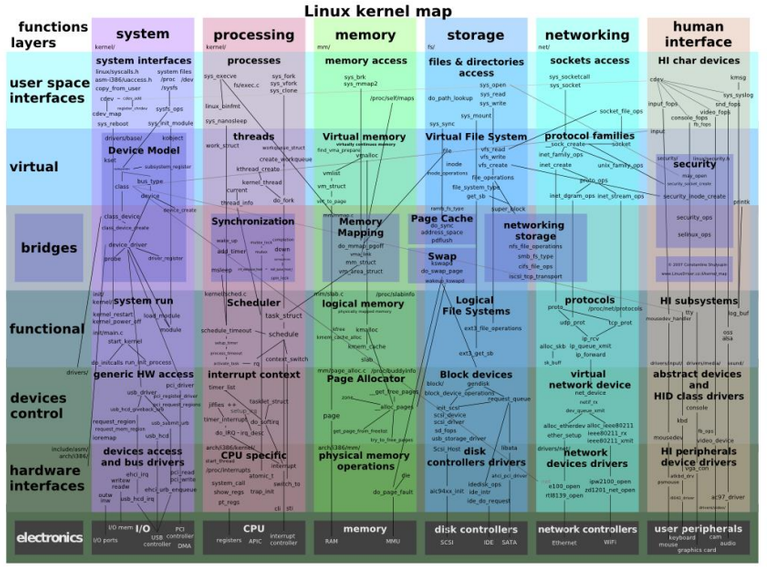
Häufige Sicherheitsmeldungen langweilen Nutzer

vorlesen / MP3-Download



(Bild: Wikipedia)

US-Wissenschaftler haben gezeigt, dass wiederholte Sicherheitsmeldungen schnell zu geringerer Aufmerksamkeit führen und schlagen andere Popups vor.

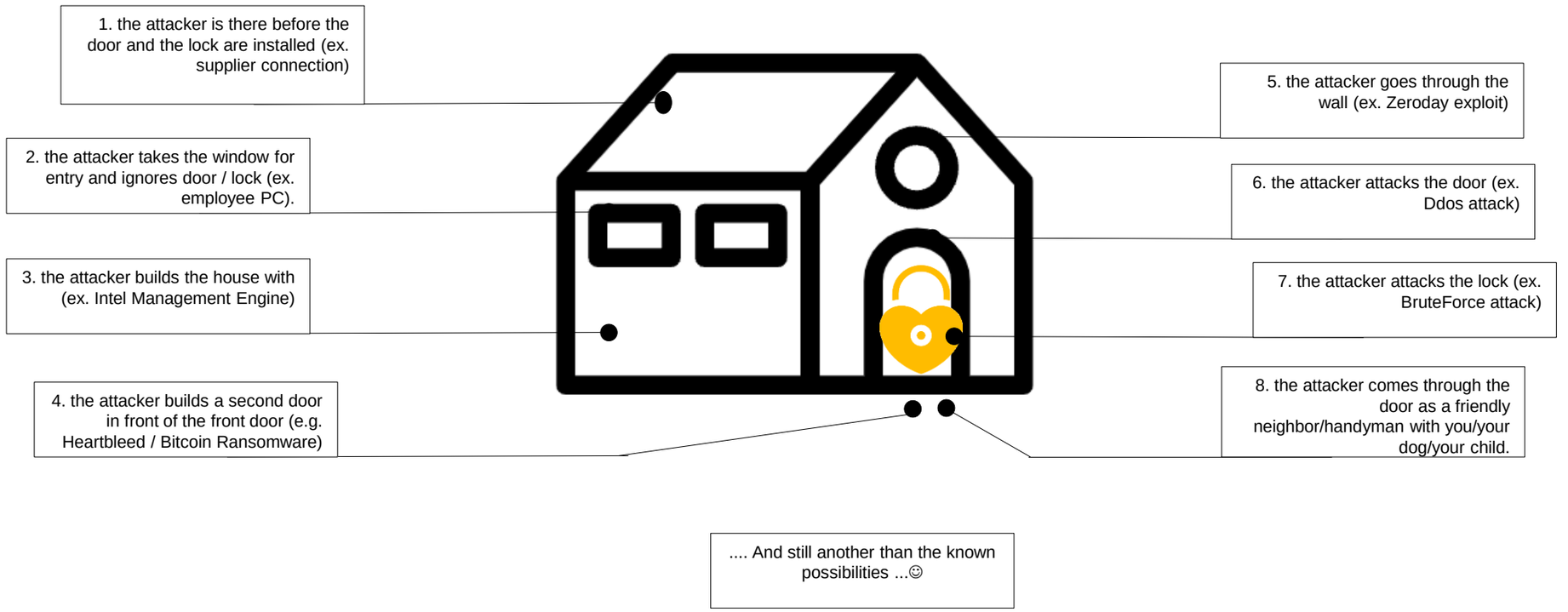


- Space shuttle - 500k lines of code
- Boeing 777 - 3-4 million lines of code
- Ford Taurus 2012 - 50+ million lines of code
- Today cars - 100 millions lines of code

* Various forecast sources

** petabyte=1 million gigabytes, terabyte=1,000 gigabytes)

I protect the contents of my house with a sturdy* door, which has a secure* lock….



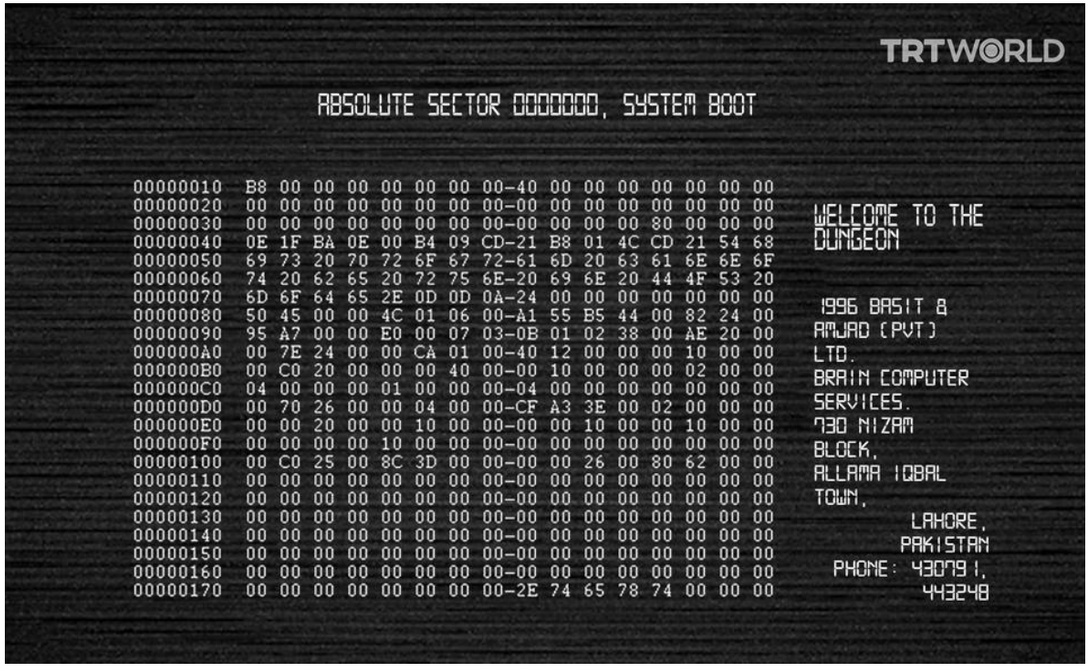
Introduction

- A brief History of incidents and what we can learn from them
- Some security fails
- Naming terminology
- Threat modeling
- Macros and why you should know about them

Are you ready?

History of Malware

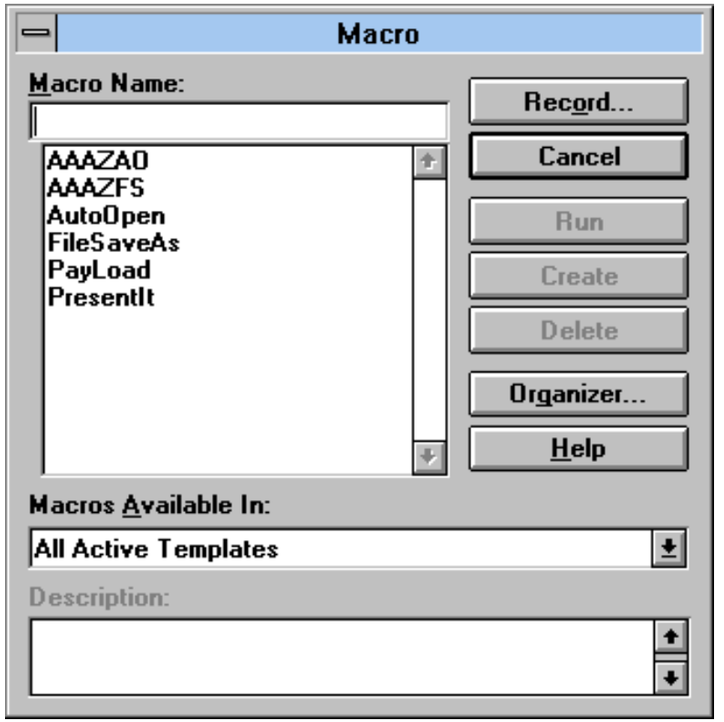
The first PC-Virus: Brain



- One of the first PC-Viruses
- Infects Boot Sector of MS-DOS floppies
- If Boot Sector is read, Virus returns original
- Spread by floppy to floppy (no disks back then)
- Printed a message, that system was infected and contact info for help

Lesson to learn: Don’t let programs access system resources

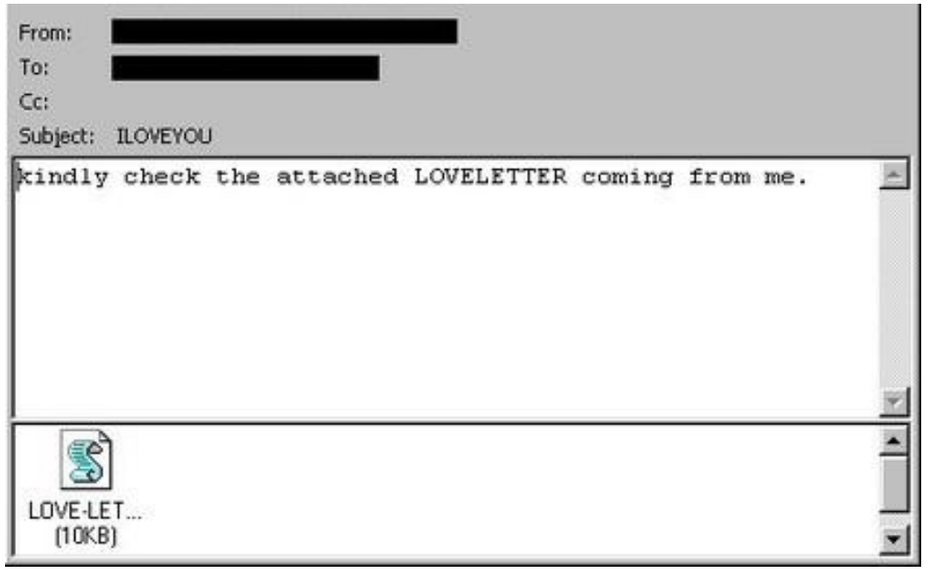
Concept (1995)



- First Virus to use MS-Word Macro to spread
- Idea: Documents travel more than other files
- Didn’t required a security issue, just use macro feature
- People tend to open their files to work with

Lesson to learn: Don’t let documents bring code with them

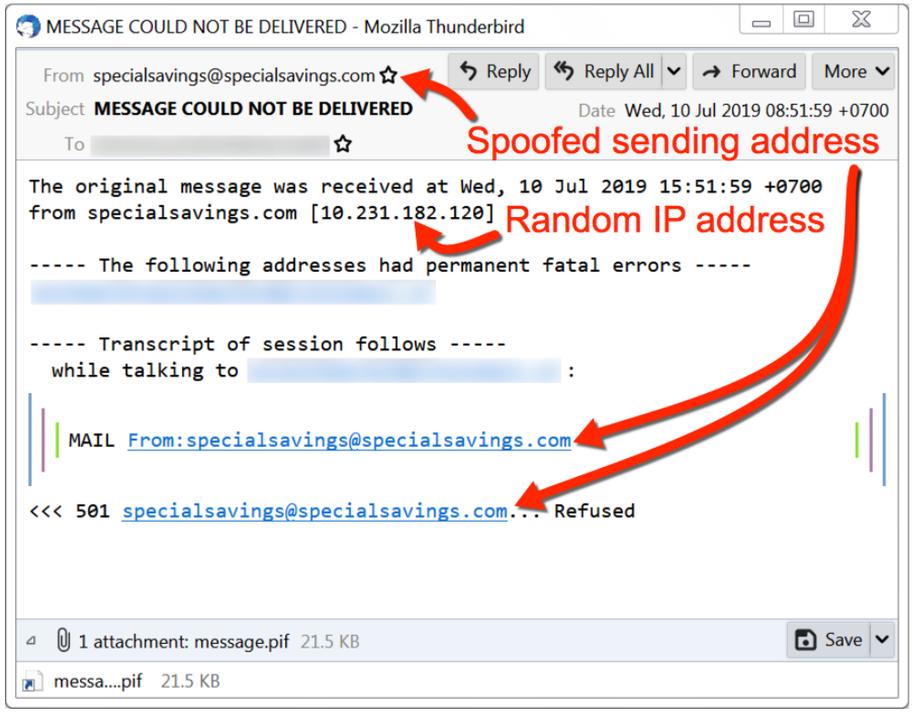
Love Letter / I love you (2000)



- Third highest damage: 10 Billion USD
- Send by mail, Appendix:
- LOVE-LETTER-FOR-YOU.TXT.vbs
- Windows doesn't show file endings by default, so looks like text file
- Outlook executes visual basic script
- Sent to all addresses in contact book, so looked like a friendly mail

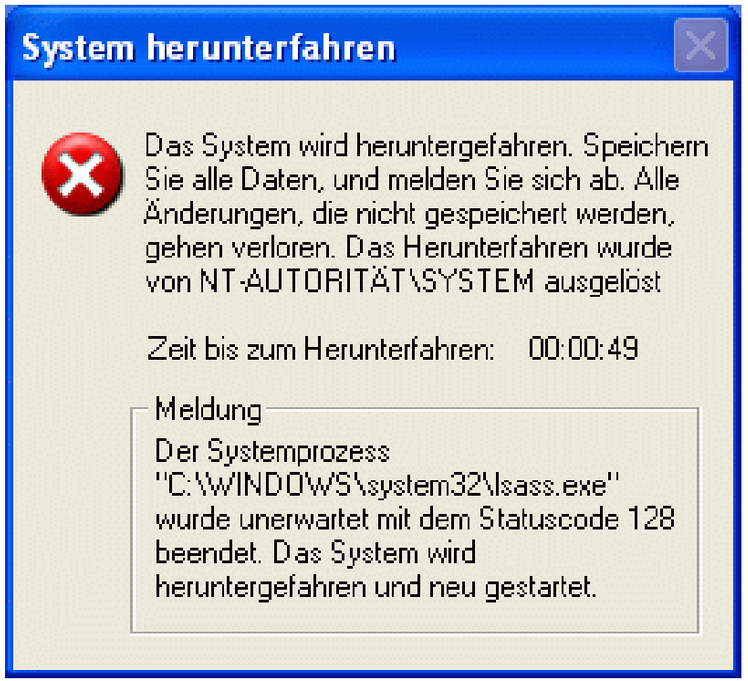
Lesson to learn: Always show the file extensions

MyDoom (2004)



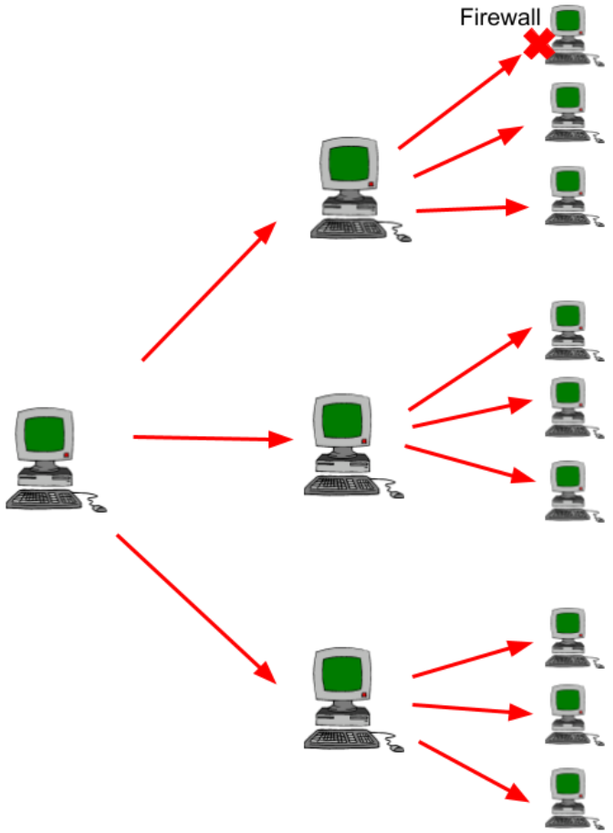
- Highest Damage: 38 Billion USD
- Send by mail, pretends to be a transmission error
- Executable appended. Sends to all contacts, spare security comapanies, universities
- Blocks access to MS-Update Page and to Anti Virus
- Installs Backdoor on the system
- DOS-Attack against SCO Group (may not worked correctly)

Sassar (2004)



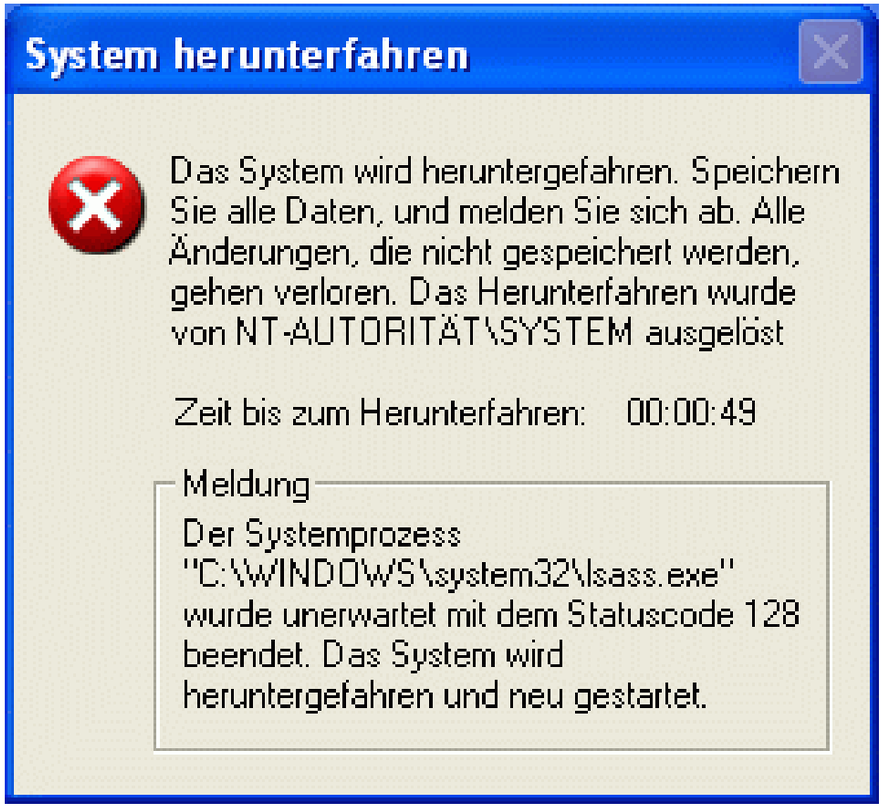
- Did not spread by mail, but by itself
- 2004 Windows computer where not shipped with firewall
- Computer run with open ports, where everyone could connect to.
- Use vulnerability in Local Security Authority Subsystem Service (LSASS)
- Issued crash of lsass.exe and restart of PC. Randomly increased CPU Load.

Sassar (2004) (2)



- Infected PC starts scanning IP Addresses.
- Sends Exploit-Code to vulnerable computer
- Loads the actual virus from the previous to the new computer
- Exponential growth (yeah, its also true for computer pandemics)
- Microsoft patched the issue before Sassar started spreading

Sassar (2004) (3)



Lesson to learn:

- Reduce the surface for attacks (FIREWALL)
- Firewall blocks connections to open ports e.g. depending on sender IP.
- INSTALL PATCHES

Fizzer (2003)

- Spread by mail
- Shift of focus. Used to distribute spam
- Start of monetarisation of malware
- Developer shift. More viruses from development countries. Focus on monetarisation.

Sony DRM (2005)

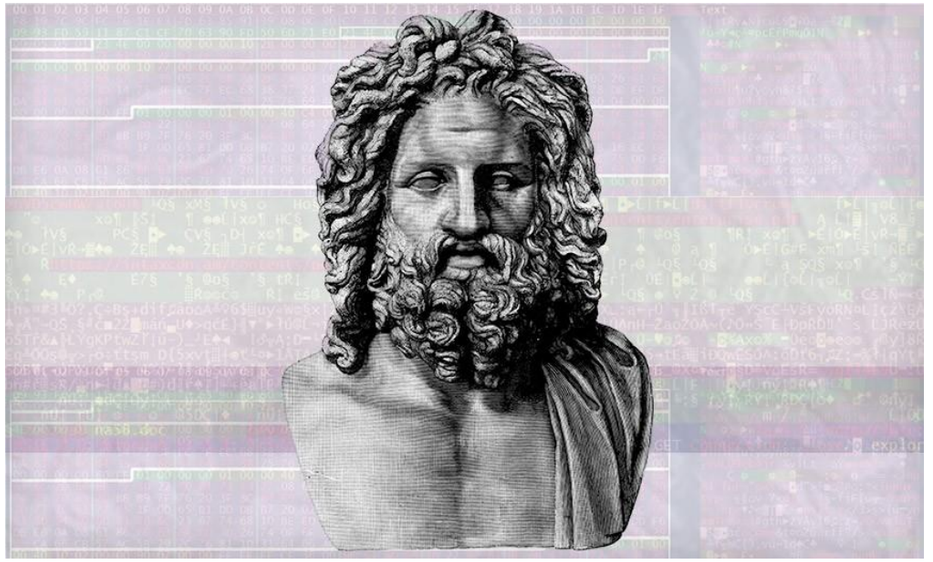
- E.g. Beyonce Audio CD
- Install Rootkit on PC, to prevent copy of CD
- Hide files starting with $ $
- Hide installed software
- Malware use this feature to hide.

Lesson to learn: don’t install shit that bypasses OS features

Mebroot (2007)

- Rootkit, hide from user
- Sit in MBR (difficult under Windows)
- BotNet used for DDoS Attacks
- Spread over ActiveX issue (Just by opening a website (drive-by infection)

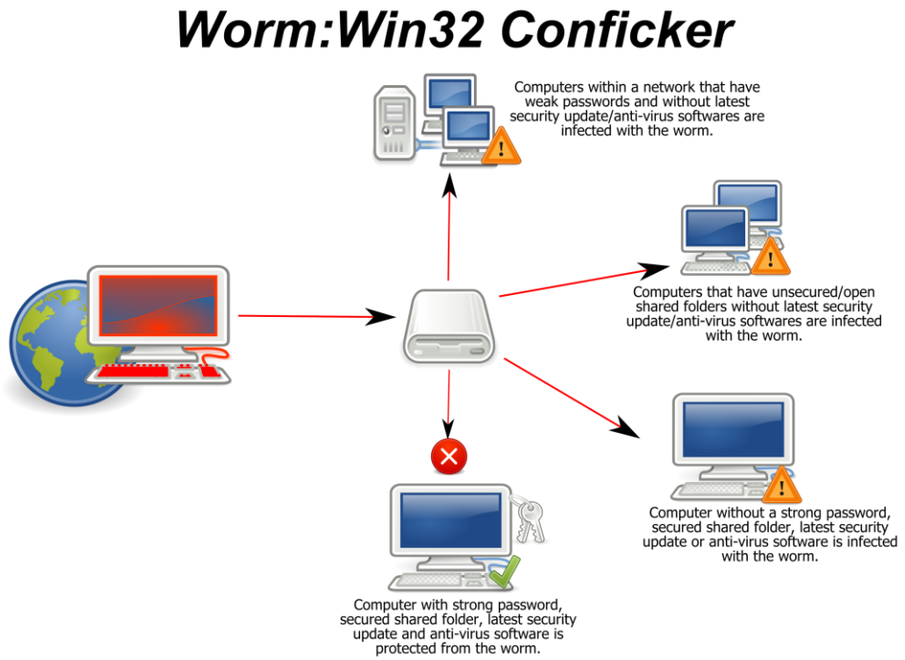
Zeus (2007)



- Banking Trojan Toolkit
- Use Man-in-the-Middle Attacks, key-logging etc to steal banking credentials
- Infected >10mio computers
- >100mio USD have been stolen
- Zeus was sold by the developer. It was more like an easy to use toolkit for criminal market.
- Postfinace Browser tries to block other software from reading its memory

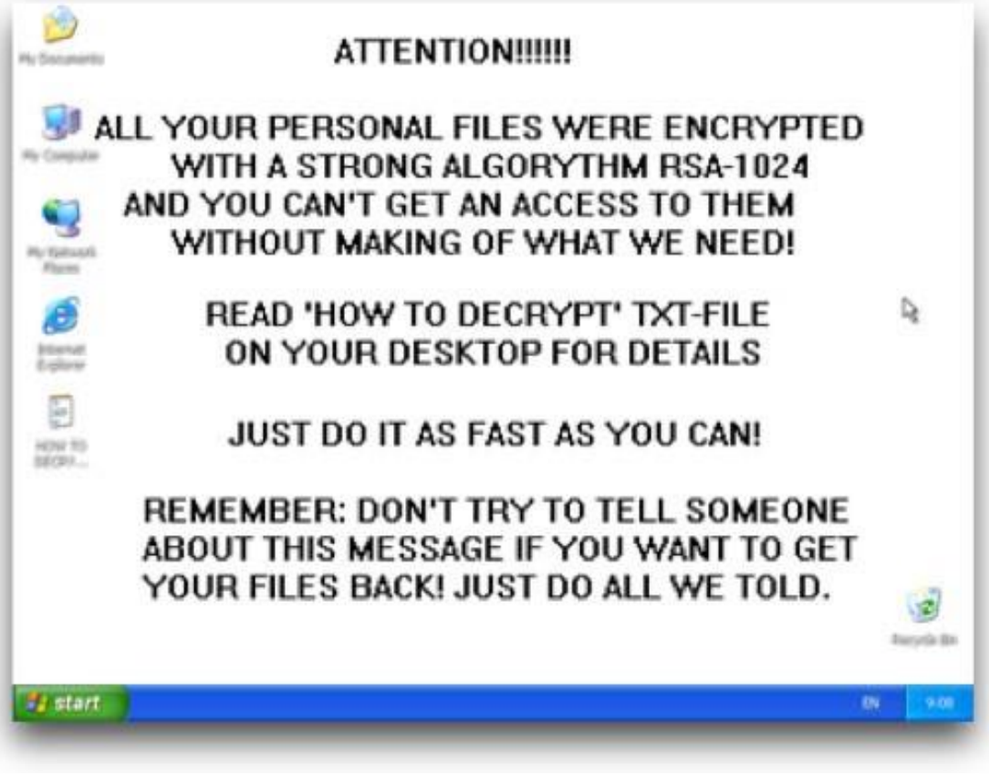
Lesson to learn: online banking required a second factor. Double check the data shown by the second factor device.

Conficker (2008)



- Building the biggest botnet till today
- Attacked Windows Server without requiring Interaction
- Spread to Clients
- Spread Client to Client using Windows Share
- Firewalls are now a thing, can only spread in local networks client to client (lateral movement)
- Spread also over USB-Devices.
- Ended up in an offline controller of a German Nuclear Power Plant (2016!)

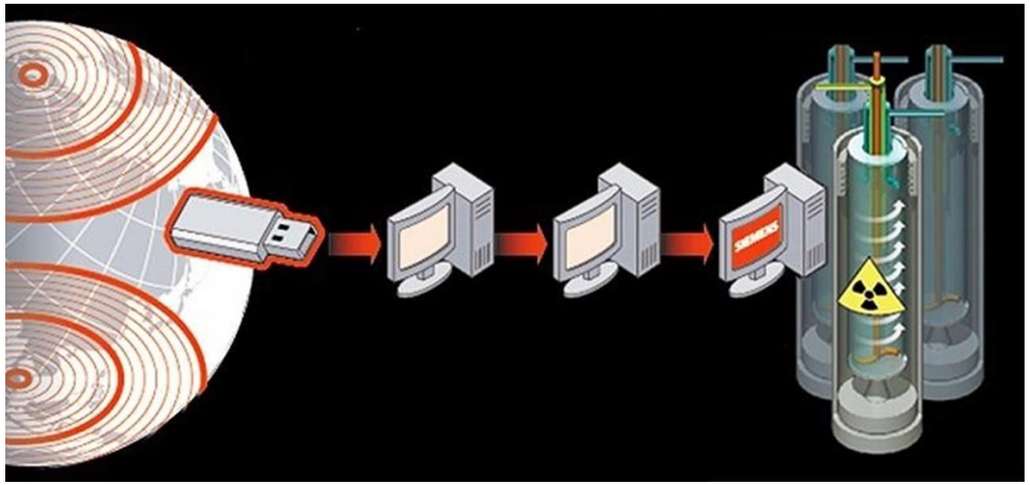
GPcode (2008)



- Ransomware. New way of monetarisation.
- Encrypt files of the user, asks for money
- Usually by paying, you get your data back
- Backups protect you!

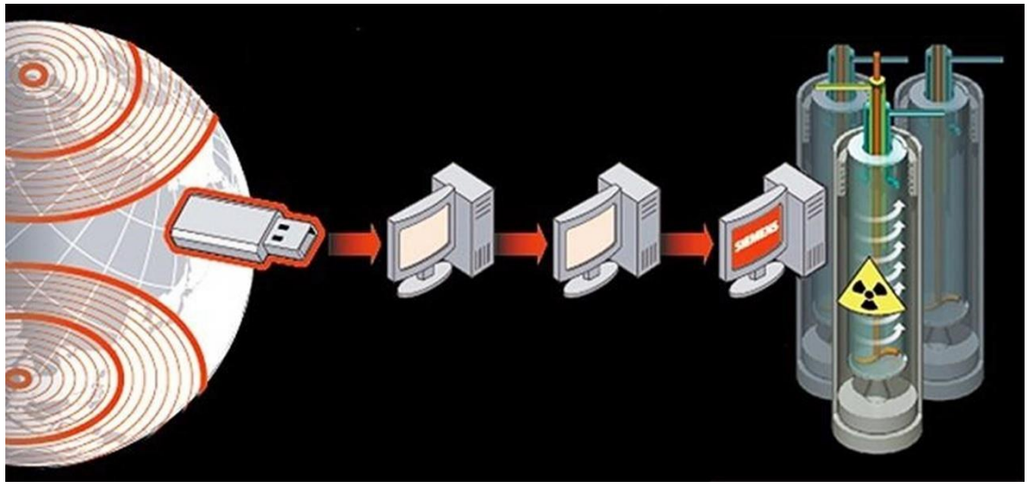
Lesson to learn: don’t let programs unchecked access files, DO BACKUPS!

Stuxnet (2010)



- Military Usage: targeting Iranian Nuclear Program
- Most sophisticated known Malware
- Nobody in InfoSec was prepared for that
- Most probably developed by US-Cybercom
- Spread using four Zero day exploits.
- Hides itself as rootkit by stolen Signatures (now, rootkit required signatures)

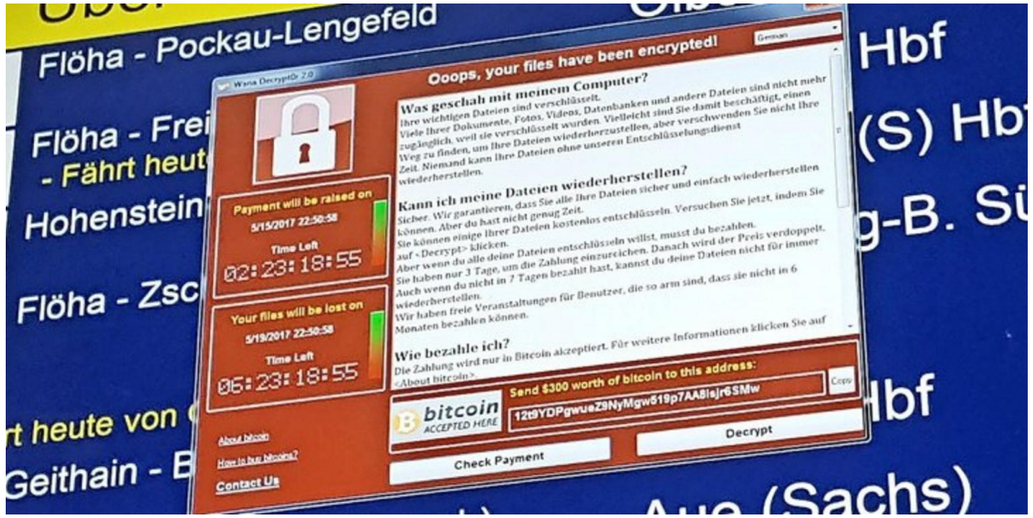
Stuxnet (2010) (2)



- Encrypted payload, hard to analyse.
- Hop by USB key into a highly secured offline facility
- Install rootkit in Siemens SCADA (Industry Control Device)
- Minimally change speed of Uranium centrifuges
- Ended up with destroying the centrifuges
- That is what you do if the only alternative is war

Lesson to learn: Nobody was ever caught using something similar

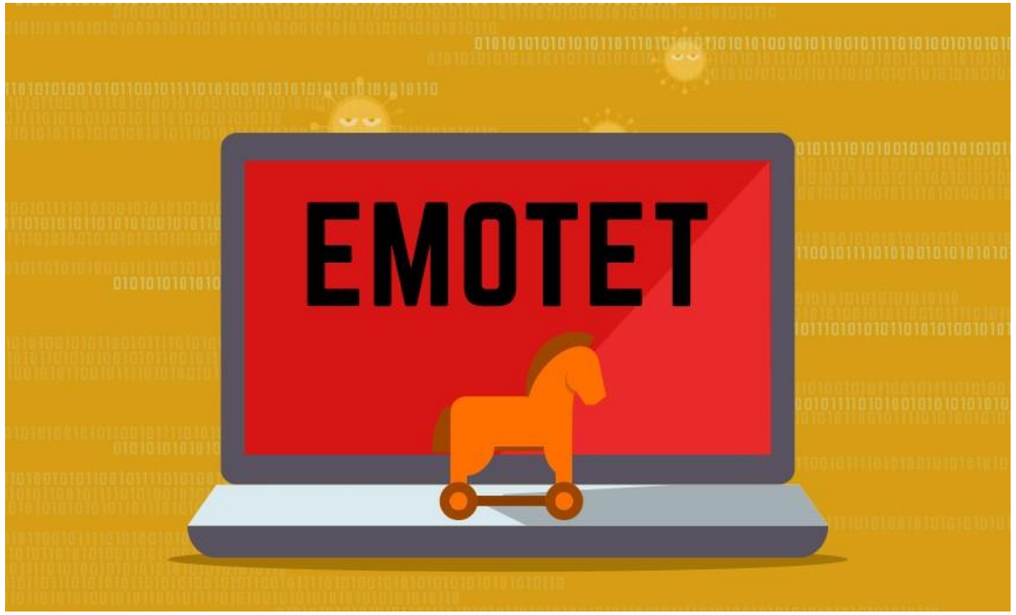
WannaCry (2017)



- Ransomware
- Used an Issue which was stolen and sold by a NSA-Employee
- Most probably developed by North Korea
- Spread over Windows Share and USB
- Infected Deutsche Bahn, FedEx, Renault, NHS, 911 ...
- Security Expert found a kill-switch

Lesson to learn: Patch the holes, don't leave them open. Govware is a stupid idea.

Emotet (2014-2020)



Lesson to learn: Why are MS Office Macros still a thing?

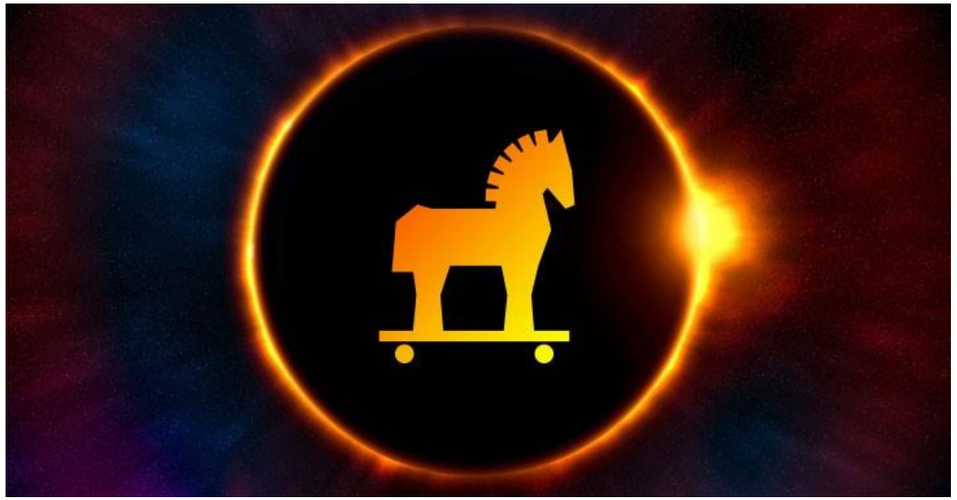
- Dynamit-Phishing, dropper for ransomware and other payload
- Not only ransom, but steals data
- Used to distributed MS Office Macro Viruses
- Creates reasonable mails by scanning mail-program to spread
- Created a botnet (used for political purpose by Russia)
- Botnet destroyed 2020/2021 by US-Cybercom, BKA, Microsoft, GDATA, ...

Meltdown & Spetre (2018)

- Conceptional Hardware Security issues
- Branch Prediction of CPU can be used to extract secrets
- Further hardware issues:
  - Timing Attacks against SGX (Hardware enclave)
  - Timing Attacks against Encryption

Lesson to learn: Its not enough to consider only software for security

Solarwinds/Supernova/Sunburst (2021)



- Attack over Network Management Software Orion of Solarwinds
- Combination of insecure passwords, ignorance and bad design
- Most probably executed by Russia.
- Targets: US Government, Microsoft, Fireeye, Palo Alto Networks
- Palo Alto Networks claims they defended by Cortex XDR (combining different defense mechanism)
- Attacks with big impact, but technically far less impressive than Stuxnet

Lesson to learn: Its not enough to consider only software for security

Security Fails

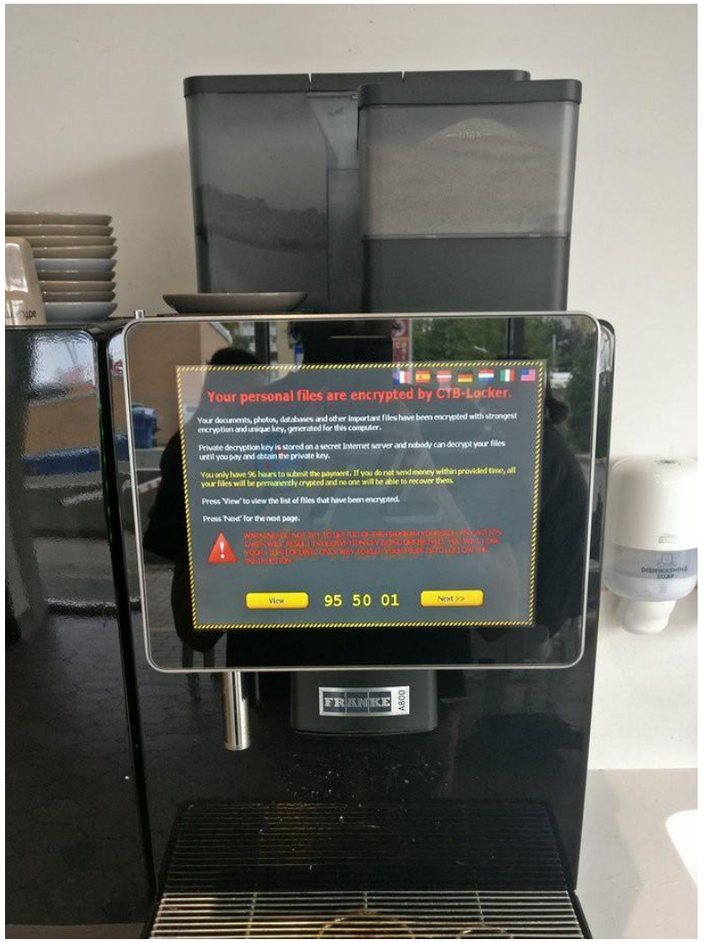
Some examples what goes wrong, when you have no idea what you are doing

- There are a lot of examples for bad security practices
- We will look at some now
- It is funny to see, but in general, we should learn from that
- If you are not sure what you are doing, do NOT do it!

Coffe Machine

- A big pharma company has two Wifi, one for production, one for employees
- Employee-Wifi is internet connected, production wifi is airgapped.
- New connected coffee machine is delivered.
- Manager does not know about Wifi-Isolation, but knows both passwords
- Added to the wrong Wifi first, coffee machine could not connect to internet
- Added other Wifi to coffee machine, without deleting the first one.
- GUESS WHAT HAPPENS NEXT?

Coffee Machine (2)



- Coffee machine got infected by Ransomware
- Ransomware spreads lateral, using all install Wifi
- Makes Coffee machine to join other stored Wifi
- Spreads in the Production-Wifi, Production needs to stop

E-Voting Systems

- Idea: Directly count votes or vote online
- Several approaches, one worse than the other
- Florida-Voting Systems counting negative Votes for Gore (2000)
- Philippines: fraudy memory cards (2010)
- Swiss Post E-Voting Systems (poor design, high complexity, weak keys) (2019)
- Dominion-Voting System 2020 accused of wrongdoing. Just the accusation of fraud is problematic, since it is hard to understand what happens inside.

E-Voting Systems (2)

- Hard to proof accusation of fraud
- Need trust in hardware and software
- Hard to make anonymous and secure
- Can’t trust the software on either end
- Attacks scale
- Threat models need to contain attacks of foreign intelligence

Corona Access Control Device (FootfallCam 3D)

- Device to counting Number of people in a store.
- Connected over Ethernet. But Wifi Active.
- SSID and WPA-Key cannot be changed. Admin PW neither (=123456)
- Configuration Interface accessible using Ethernet and Wifi
- Raspberry Pi Compute Module, default user still active (SSH, too)
- History in terminal from developers not deleted
- Developer does not react on issues

Clear your projects before shipping

Solarwinds / Supernova / Sunburst

- Solarwinds builds a Management Software (Orion)
- Agent on EndPoint Devices
- Monitors Network, Keeps Software up to date, delivers updates
- This kind of management software often runs with high rights deep integrated into the OS
- Solarwinds Orion is used by a lot of companies: Fireeye, Microsoft, US-DoD.

Solarwinds / Supernova / Sunburst (2)

- What happens, when the updates of such Mgmt-Software gets corrupted or manipulated?
- Malware is distributed to all customers
- Mgmt-Software has high rights, so manipulated updates are terrible.
- So, Solarwinds is doing everything to protect updates

Solarwinds / Supernova / Sunburst (3)

- Well, no.
- Password for Update Server in GitHub account
- The password was solarwinds123
- No independend checksums for update client
- Customers got infected
- Classic third vendor attack

Solarwinds / Supernova / Sunburst (4)

- Mgmt-Software is important to manage computers in large enterprises
- But having software with high rights is a risk.
- Strong isolation required. E.g. OS deliverers Monitoring data using API
- Management tools and Anti-Virus Software need to be extreme carefully engineered
- IPhone, Android and ChromeOS Mgmt shows how to run Mgmt-Tools on systems which do not provide root to administrator or user

Avast - TLS Man in the Middle

- Avast Antivirus installed a Man-in-the-Middle certificate in web-browsers
- Idea: Antivirus encrypts data before giving it to the web-browser to check for viruses
- The problem: the browser/user does not see the original certificate, but the Avast certificate
- Implementation weakness can undermine the security of encrypted connection
- Avast can analyse and store data from your encrypted connections (and sell them)
- Feature was removed after discovered by Google