openHPI Course: Cyberthreats by Malware

Short History of Cybercrime

Prof. Dr. Christoph Meinel

Hasso Plattner Institute
University of Potsdam, Germany

Computer Security and Crime:
From Phone-Freaking to Cyberwar

Since electronic systems have existed, there have been many attempts to attack them for various reasons and purposes

- In 1903, when Guglielmo Marconi demonstrated a public radio link in London, Nevil Maskelyne intercepted the communication and sent an "unauthorized" Morse code message to the receiver → **first hacking in the history**
- Since the 1930s and during the Second World War (in the end even industrially organized) successful attempts to break the Enigma encryption
- In the 1970s – emergence of the phreaking (**Phone Freaking**) movement

Computer Security and Crime: **Phone Freaking**

Telephone hackers (phreakers) in the 1960s and 70s:

- Searching for weak points in telephone systems to make free calls
- Convoluted ideological justification: "Freedom of communication is a prerequisite for the freedom of humanity"

Example: Blueboxing

- Connections could be terminated ostensibly by an internal control tone of 2,600 Hz but the line for the exchange remained open
- Phreakers ware able to make new (expensive long distance) calls at the original (cheap local) rate
- **Bluebox**: device for generating various control tones

Computer Security and Crime: **First Generation Hacker** (1/2)

With more people could own an PCs (personal computer), the fast growing hacking scene first established itself in the underground. In 1981, one of the biggest hacker associations, the **CCC – Chaos Computer Club** – was founded in Berlin

- Originally from Germany, now an international organization
- Since 1984, CCC has organized annual internal conferences → Chaos Communication Congresses (C3)
- Due to Corona crisis instead of the 37C3 the first rC3 – Remote Chaos Experience – were organized
- Features lectures and workshops related to the latest issues on computer security area

Computer Security and Crime:
First Generation Hacker (2/2)

Spectacular actions of tgeh CCC revealed software errors and various security holes, such as

- **1984**: Abuse of the newly introduced BTX service of the Hamburger Sparkasse by transferring DM 134,000 to CCC
- **1996**: CCC demonstrated attack against Microsoft ActiveX
- **1998**: CCC broke the COMP128 encryption algorithm used by many GSM SIM cards at that time
- **2008**: CCC published fingerprints of German Federal Interior Minister to oppose the use of biometric data in German IDs (e-passport)
- **2011**: CCC published an analysis of the (poorly crafted) federal Trojans

Computer Security and Crime: **Hacking in The 1990s**

- Rapid spread of computer systems lead to equally rapid development of the hacking scene
- State legal systems began to enact legal regulations, e.g.
  - Computer Misuse Act, United Kingdom, 1990
- Attacks on computer systems were increasingly automated
- Automated worms, scanners, or other attack tools caused a huge flood of security incidents
- First **IDS** (**Intrusion Detection Systems**) and surveillance systems were developed

Computer Security and Crime: **Cybercrime in The 2000s**

Meanwhile almost every computer system was connected to the open Internet. As a result, the number of security incidents were rising dramatically:

- Viruses, worms, Trojans, ...
- Botnets
- Industrial espionage
- No large company could do without IT security department
- Hacking software tools now could be downloaded from the Internet by everyone, e.g., Script Kiddies
- Rise of underground networks like Tor, I2P (Invisible Internet Project), and Freenet

Computer Security and Crime: **Cyberwar**

Security services of most countries build cyber defense departments for both inside and outside the country, e.g.

- □ Germany: National Cyber Defense Centre
- □ NATO: Coop. Cyber Defense Centre of Excellence
- □ USA: United States Cyber Command

- ■ Various groups of hackers are repeatedly accused of being close to the government
  - □ connections are often difficult to prove
  - □ professionalism, financial resources, and the targets of the attacks are indications

Computer Security and Crime:
Spectacular Examples in Recent Years

- **2020: New details: Crypto AG / Project "Rubicon"**
  - □ Swiss company sold encryption machines to various governments (>100) after World War II
  - □ For a long time owned by the CIA (until 2018) and the BND (until 1990s), who could read everything via the back door

Quelle: https://www.washingtonpost.com/graphics/2020world/national-security/cia-crypto-encryption-machines-espionage/

- **2018: Hack of Jeff Bezos' phone**
  - □ Jeff Bezos, Amazon CEO, owner of Washington Post, multi-billionaire → valuable target
  - □ hack was done probably through a video obtained sent from Saudi Crown Prince via WhatsApp

Source: https://assets.documentcloud.org/documents/6668313/FTI-Report-into-Jeff-Bezos-Phone-Hack.pdf