openHPI Course: Cyberthreats by Malware

Ransomware

Prof. Dr. Christoph Meinel
Hasso Plattner Institute
University of Potsdam, Germany

Ransomware

Ransomware – malware that denies the victims access to their systems or encrypts important files on the systems

- Name derived from **ransom** (extortion) and **ware** (software)
- After infection blackmailers demand a **ransom** for unlocking the system or decrypting the files
  - pay by crypto currencies (Bitcoin, MoneyPak, …) or other online payment methods
  - **but no guarantee** that the victims will be able to fully access their systems again after the payment

Ransomware

- **How ransomware is installed in the victim's system?**
  - by opening malicious email attachments
  - by installing fake software with malware
  - by accessing malicious websites
- **How ransomware becomes noticeable**
  - blocked screen
  - alerts and pop-up messages of blackmail letter
  - system failed to work
- Some ransomware variants initially "sleep" on the system unnoticed and are later "switched on" by the attackers

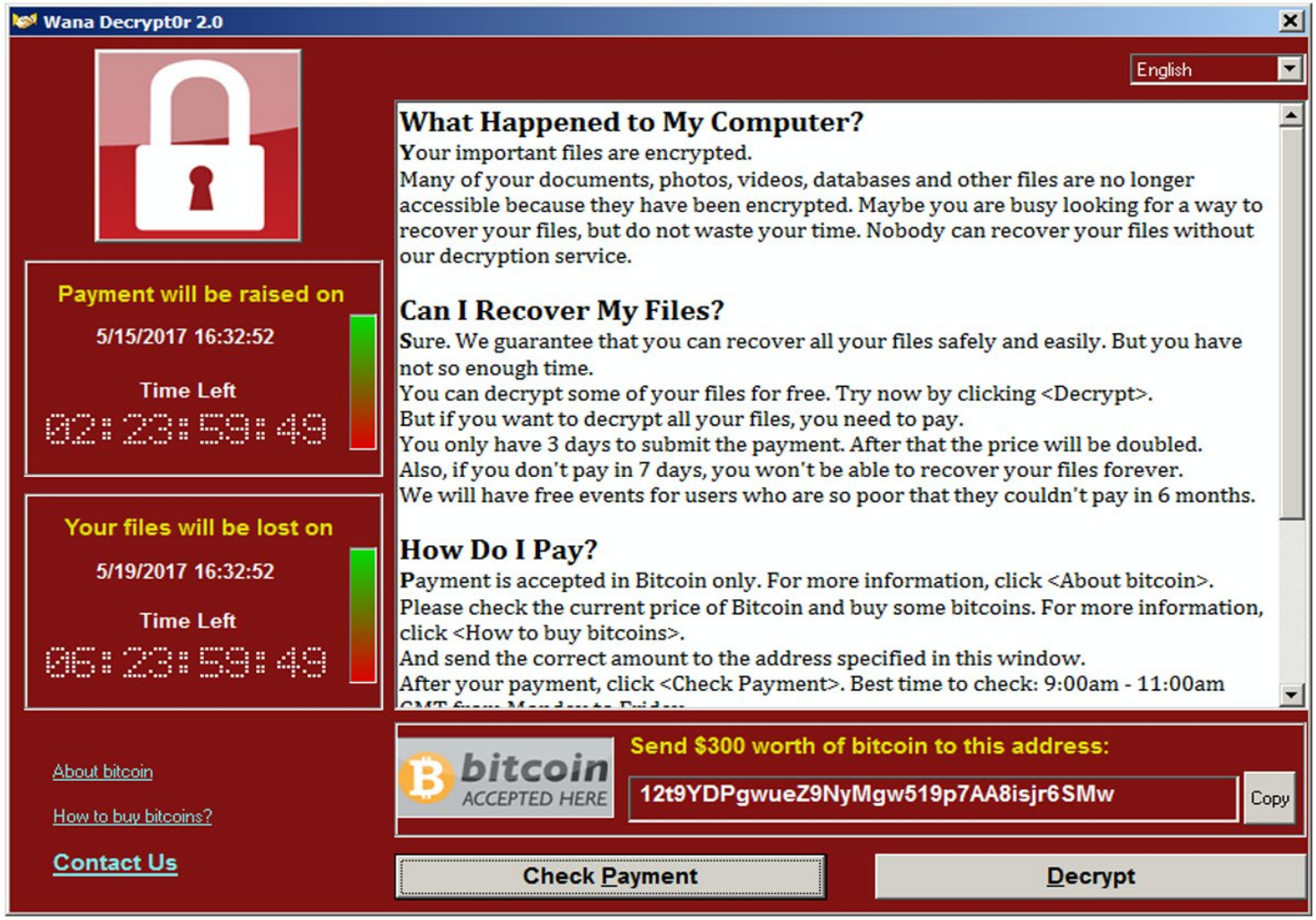
Ransomware
Example: WannaCry (1/3)

- Worldwide known **ransomware campaign** in 2017
  - made use of malicious code **Eternal Blue** leaked from the National Security Agency of USA
  - targeted at Windows systems without security updates
- **More than 200,000 affected computers**
  - encrypts hard disks on the infected systems
  - later eventually unlocked after the victims paid Bitcoins
  - most sensitive areas of society are affected
    - critical infrastructures
    - hospitals
    - energy Utilities

Ransomware
Example: WannaCry (2/3)

Source: heise.de

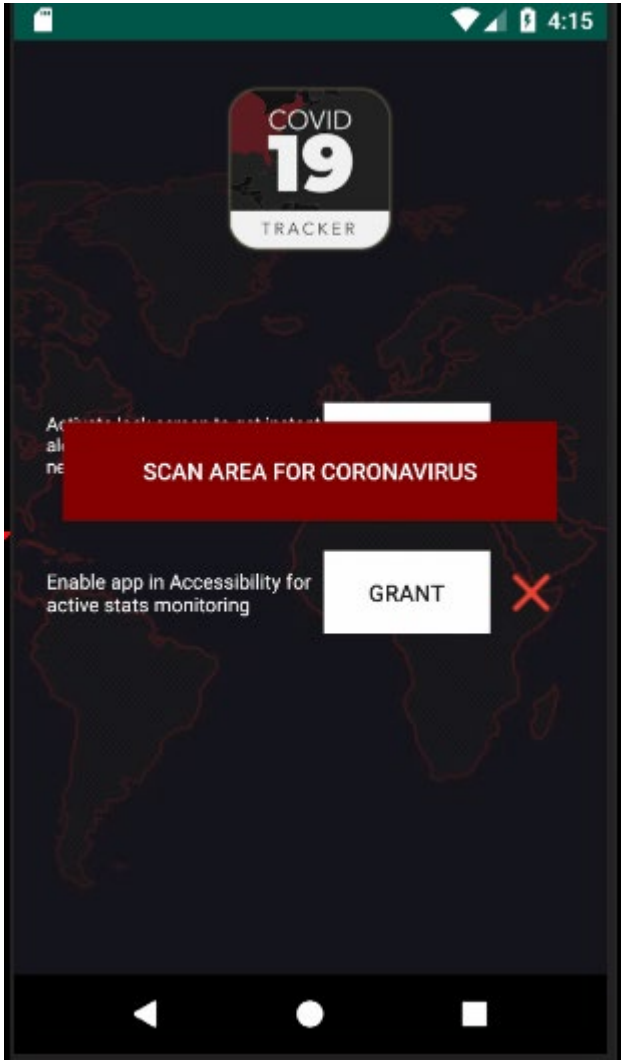
Ransomware
Example: WannaCry (3/3)



Source: silicon.de

Ransomware
Example: CovidLock (1/2)

- Disguises itself as useful smartphone app
- Current campaign exploiting concerns about COVID-19
- Promises statistics and maps about the spread of the virus in the victim‘s area



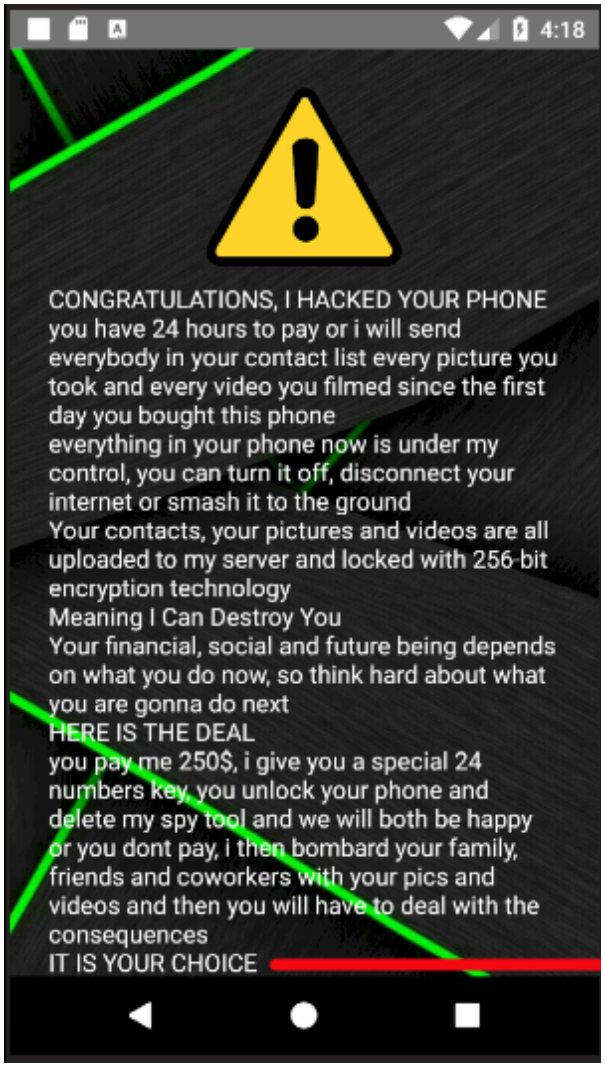
Quelle: Shivang Desai, "CovidLock: Android Ransomware Walkthrough and Unlocking Routine". Zscaler, 2020

Ransomware
Example: CovidLock (2/2)

- Demands a ransom of $250
- Encrypts contacts, pictures and videos on the smartphone
- Internet is not used by the ransomware, i.e.
  - data is not uploaded to the attacker's server
  - local decryption either very easy or impossible to crack

Unlock Code

4865083501



Quelle: Shivang Desai, "CovidLock: Android Ransomware Walkthrough and Unlocking Routine". Zscaler, 2020

Ransomware
Protective Measures

- Major consensus advices not to paying the ransom since there is no guarantee that the attacker will unlock the system or the data after the payment
- Most effective protective measure against ransom goods: **create backups** of the data and the system
  - then systems and files can easily be restored in case of ransomware infection
- General security measures, such as the **installation of virus** and **malware scanners** to detect ransomware

➢ **"Protective Measures"** chapter this week