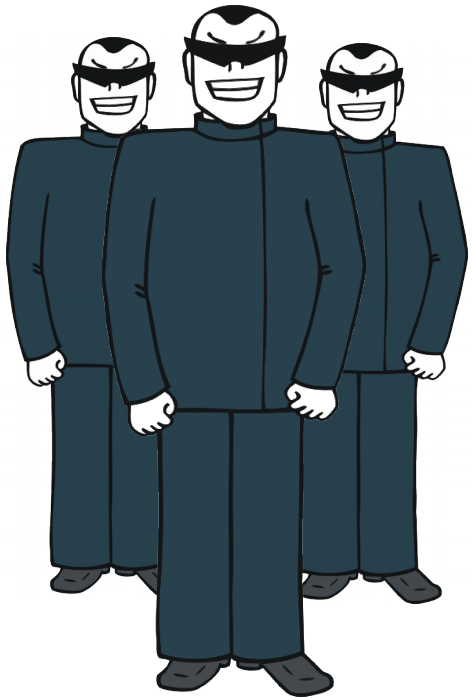
#SECFEST2017

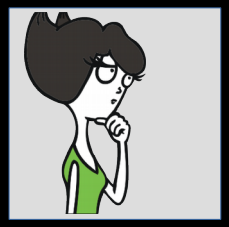


# Ransomware

## včera, dnes a zítra

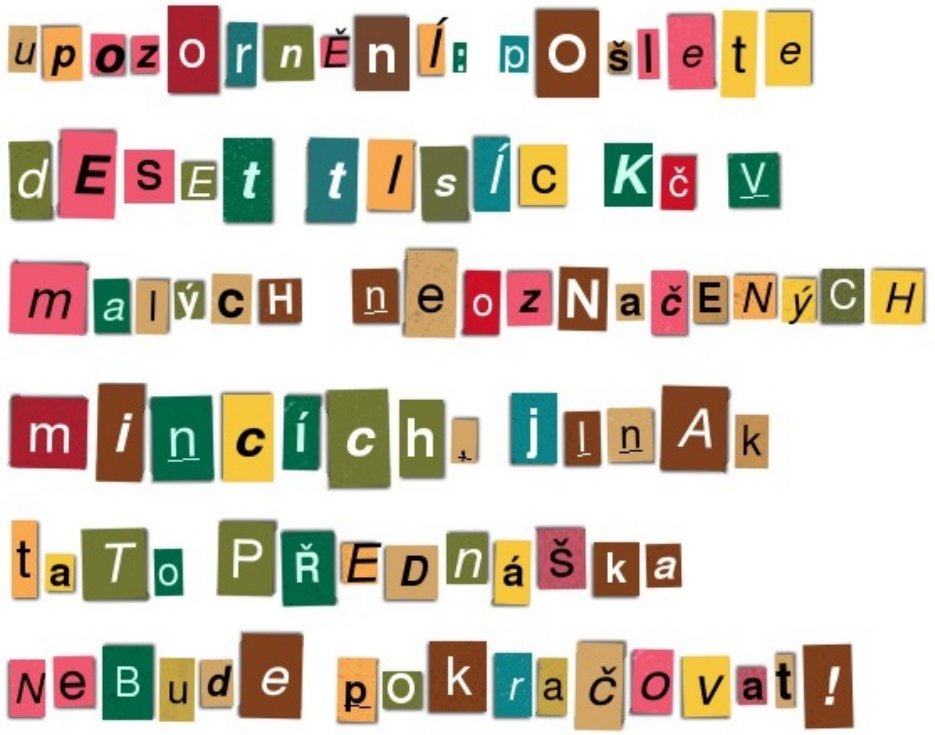
Aleš Padrta

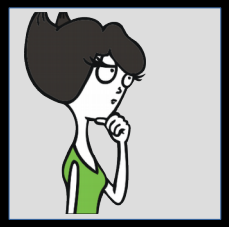
**apadrta@civ.zcu.cz**



# Trocha historie ...

- Vydírání
  - Od nepaměti
  - Nemorální výměna
- Elektronizace světa
  - e-mail
  - e-shop
  - e-banking
  - e-peníze
  - e-výkupné??

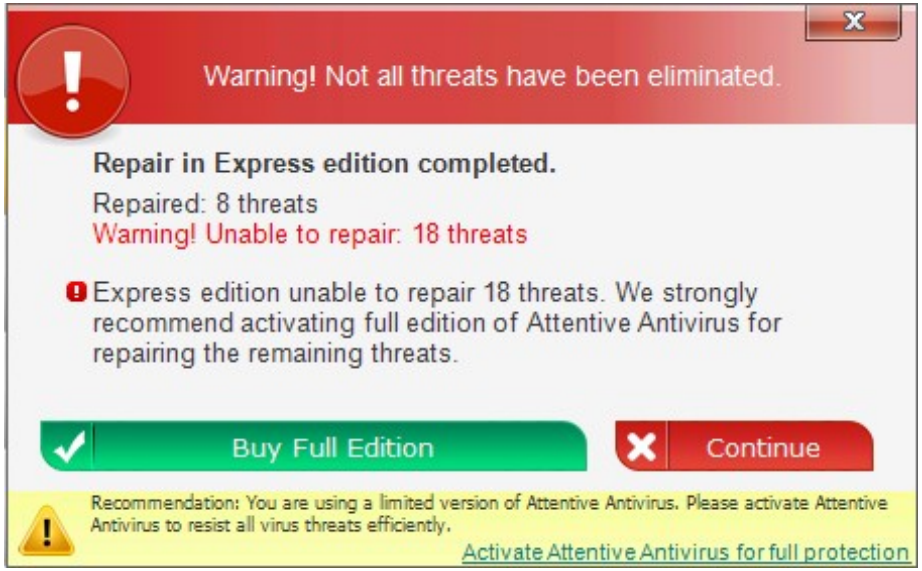


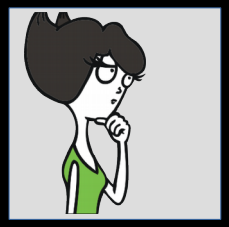


# Počátky ransomware

- Ransom + software ⇨ ransomware
  - Vrácení „funkčnosti“ za peníze
- Nesmělé začátky ~ 2005
  - Spoléhání na sociální inženýrství
  - Technicky primitivní
  - Snadné odstranění

SpySheriff, RegistryCare, Antivirus Plus, Notrel Antivirus, E-Set, ...

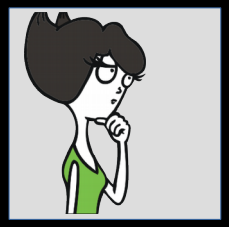




# Pokrok nelze zastavit

- Větší rozšíření ~ 2011-2012
- Vylepšení
  - Sociální inženýrství
  - Technicky pokročilejší
- „Snadné“ odstranění
  - Blokuje „jen“ přístup
  - Data bez povšimnutí

Trojan.Ransom.C, Reveton, ...



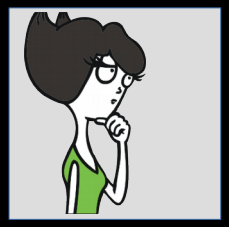
# Současný ransomware

- Uživatel nespolupracuje (nechce platit)

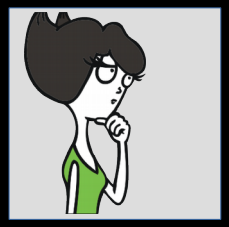
  ⇨ Evoluce pokračuje

- Důraz na techniku ~ 2013
  - Technicky
    - Zašifrování dat
  - Odstranění
    - Vyžaduje dešifrování
    - Komplikované

CryptoWall, CryptoLocker, ...

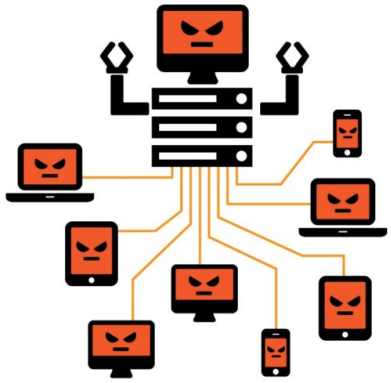


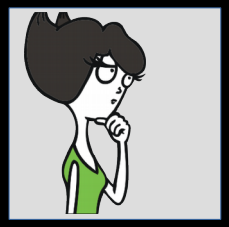
# Zálohujete svá data?



# Ransomware @ ZČU

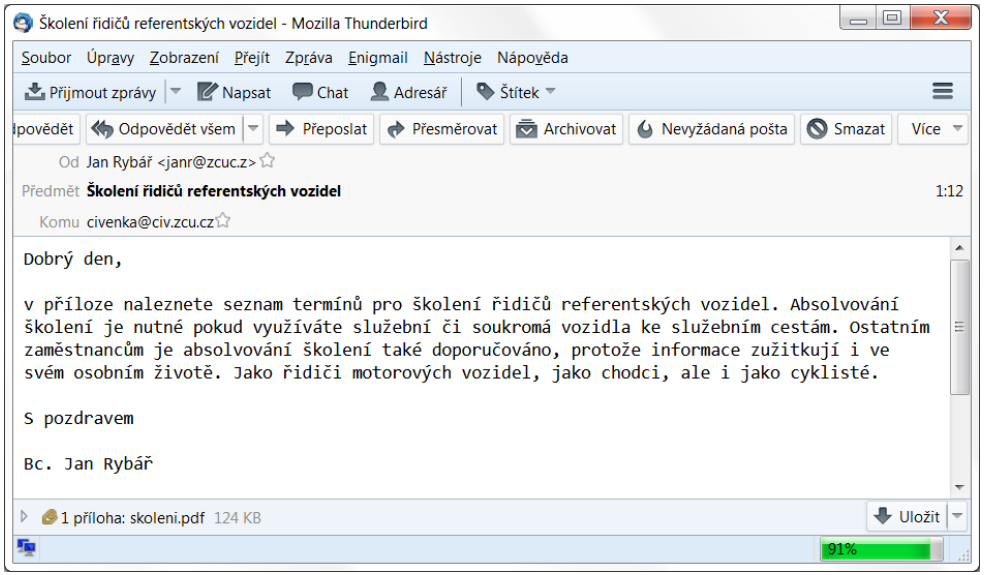
- ZČU nestojí stranou
  - Zařízení bez centrální správy
    - Různá kvalita zabezpečení
  - Uživatelé
    - Různý přístup
    - Různé bezpečnostní povědomí
  - Výskyt malware
    - Zapojení do botnetu („centrální správa“)
    - Očekávání rozkazů
    - Instalace ransomware

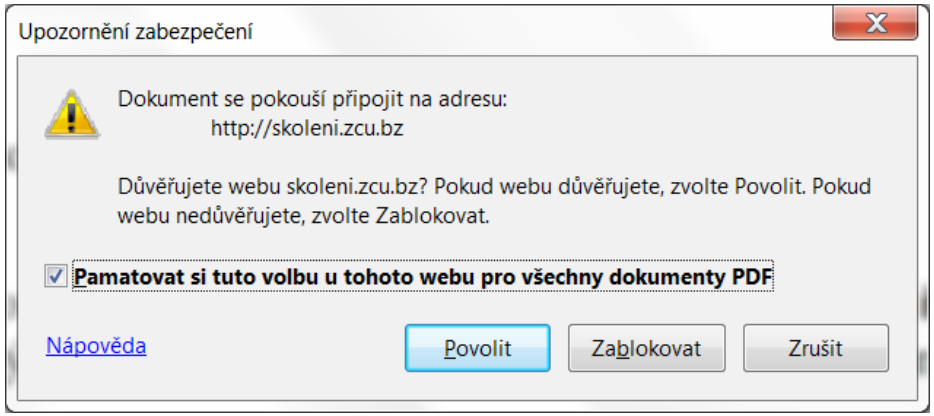


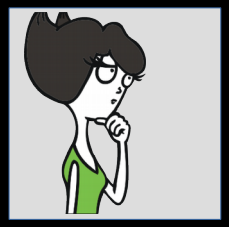


# Způsob infekce

- Podvodný e-mail
  - Nejčastější příčina!
  - Uživatel = slabý článek
- Otevření přílohy
  - Skript (program)
  - Dokument s makrem
  - Závadné PDF
- Stažení malware
- Zašifrování dat

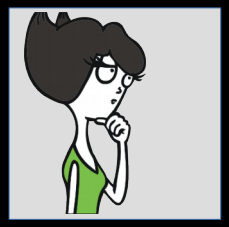




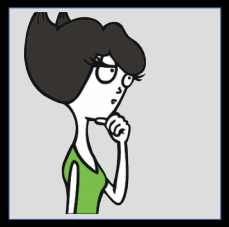
# Jak přežít ransomware?

- Předejití problémům
  - Vzdělaný uživatel
  - Zabezpečená zařízení
- Minimalizace dopadů
  - Minimální přístupy
  - Zálohování a plán obnovy
- Platit nebo neplatit?
  - S ~~teroristy~~ vyděrači se nevyjednává
  - Možnost přijít o data … i peníze



# Vize do budoucna

- Výskyt ransomware
  - Standardní zařízení
  - Mobilní zařízení
  - Internet věcí
  - Infrastruktura
- Portfolium hrozeb
  - Nedostupnost dat
  - Zveřejnění dat (!)
  - Omezení služeb

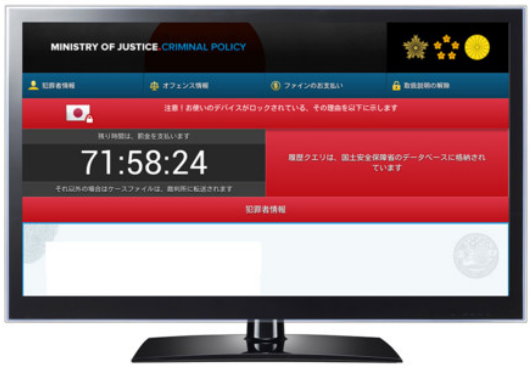



# Dotazy


STOP
PAY $10,000
TO DRIVE
YOUR CAR


EBI
YOUR DEVICE HAS BEEN BLOCKED
DETECTED ILLEGAL CONTENT
This device is locked due to the violation of the federal laws of the United States of America:
* Article 1, Section 8, Clause 8
* Article 202


Abfahrt
Linie
Ziel
Zeit
Über
Nach
Gleis
Olbernhau
Aue (Sachs)
Dresden Hbf
BMG | MIS


MINISTRY OF JUSTICE.CRIMINAL POLICY
71:58:24


FEDERAL BUREAU OF INVESTIGATION
computer has been locked!


TAMAGOTCHI