ThreatMark

Open source v bankovním prostředí

Michal Toman

Principal Software Developer, ThreatMark

O mně

- Nejdříve Red Hat - RHEL
- Pak MIPS - Fedora pro MIPS architekturu
- Teď ThreatMark

Agenda

- Střet open source vývojáře s bankovní praxí
  - Na co se připravit
  - Jak jsou na tom banky se vztahem k open source
  - Jak obecně vypadá bankovní infrastruktura
  - Jak funguje bankovní IT
- Příklady útoků
- Jak se bránit?

Agenda

Střet open source vývojáře s bankovní praxí

Na co se připravit

- NDA, NDA everywhere!

Na co se připravit

- NDA, NDA everywhere!
- I jednoduché věci můžou trvat dlouho

Na co se připravit

- NDA, NDA everywhere!
- I jednoduché věci můžou trvat dlouho
- Legální problémy na nečekaných místech

Na co se připravit

- NDA, NDA everywhere!
- I jednoduché věci můžou trvat dlouho
- Legální problémy na nečekaných místech
- Byrokracie, byrokracie, byrokracie

Na co se připravit

- NDA, NDA everywhere!
- I jednoduché věci můžou trvat dlouho
- Legální problémy na nečekaných místech
- Byrokracie, byrokracie, byrokracie
- Ne všichni používají PKI

Jak jsou na tom banky se vztahem k open source

- Prakticky všechna IB jsou zakázkový softvér
  - Možná změna díky PSD2

Jak jsou na tom banky se vztahem k open source

- Prakticky všechna IB jsou zakázkový softvér
  - Možná změna díky PSD2

- Bankovní backendy typicky rovněž

Jak jsou na tom banky se vztahem k open source

- Prakticky všechna IB jsou zakázkový softvér
  - Možná změna díky PSD2
- Bankovní backendy typicky rovněž
- Infrastruktura je relativně otevřená open source
  - Typicky kombinace otevřených a proprietárních řešení
  - Běžně najdeme Linux, databáze, webserver, monitoring

Jak obecně vypadá bankovní infrastruktura

- Izolovaně

Jak obecně vypadá bankovní infrastruktura

- Izolovaně
  - Často bez připojení k internetu

Jak obecně vypadá bankovní infrastruktura

- Izolovaně
  - Často bez připojení k internetu
  - Jestli je připojená k internetu, přístup je záměrně nepohodlný

Jak obecně vypadá bankovní infrastruktura

- Izolovaně
  - Často bez připojení k internetu
  - Jestli je připojená k internetu, přístup je záměrně nepohodlný
  - Výjimečně je možné zřídit VPN přístup pro konkrétní osoby

Jak obecně vypadá bankovní infrastruktura

- Izolovaně
  - Často bez připojení k internetu
  - Jestli je připojená k internetu, přístup je záměrně nepohodlný
  - Výjimečně je možné zřídit VPN přístup pro konkrétní osoby

- Víc testovacích prostředí, než je běžný vývojář zvyklý

Jak obecně vypadá bankovní infrastruktura

- Izolovaně
  - Často bez připojení k internetu
  - Jestli je připojená k internetu, přístup je záměrně nepohodlný
  - Výjimečně je možné zřídit VPN přístup pro konkrétní osoby
- Víc testovacích prostředí, než je běžný vývojář zvyklý
- Typicky virtualizace přes několik datacenter

Jak funguje bankovní IT

- Záleží od banky
  - Někde jsou malé jednotky IT techniků a vše je outsourcované
  - Někde je větší tým, který udržuje infrastrukturu

Jak funguje bankovní IT

- Záleží od banky
  - Někde jsou malé jednotky IT techniků a vše je outsourcované
  - Někde je větší tým, který udržuje infrastrukturu

- Development je v podstatě vždy externí

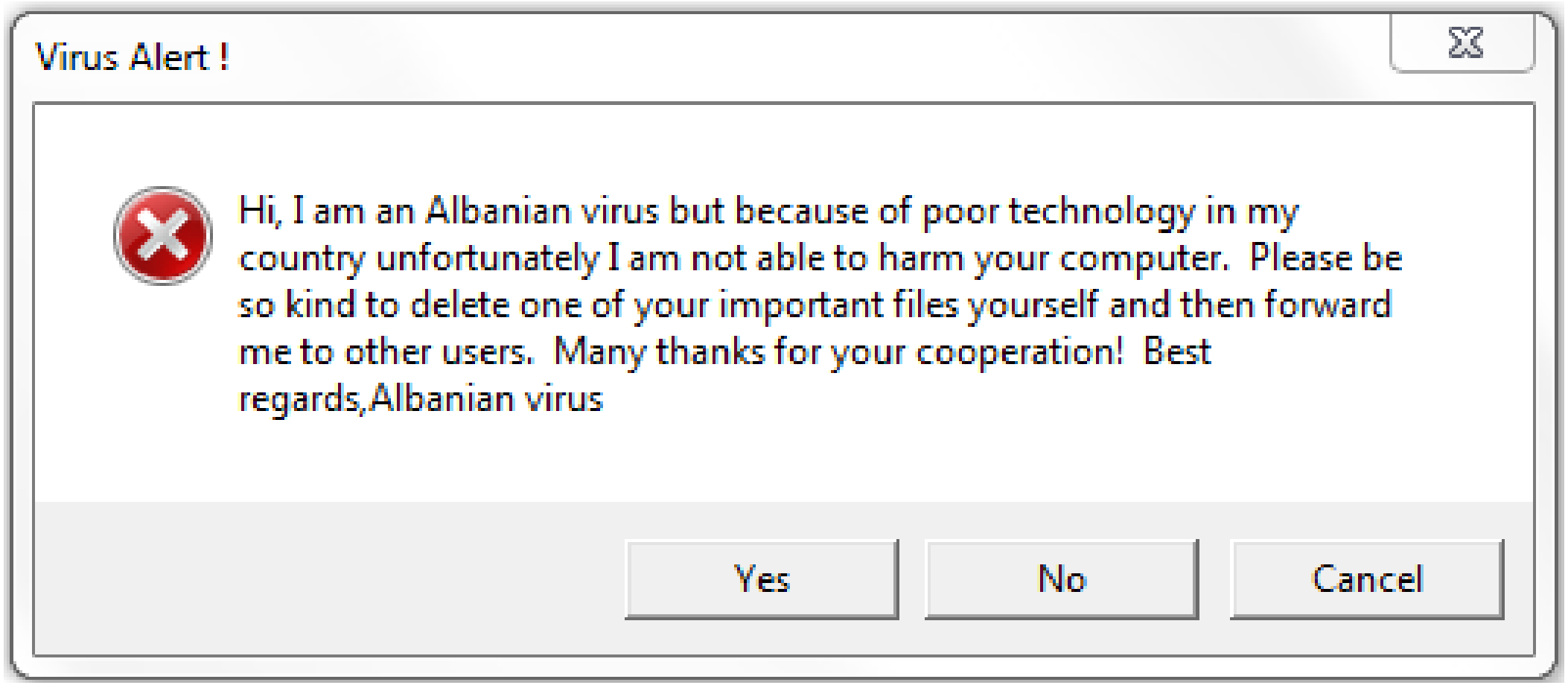
Jak funguje bankovní IT

- Záleží od banky
  - Někde jsou malé jednotky IT techniků a vše je outsourcované
  - Někde je větší tým, který udržuje infrastrukturu
- Development je v podstatě vždy externí
- Konzervativní přístup k novým technologiím
  - „Když to funguje, tak na to nešahejme“

Agenda

Příklady útoků

Agenda


Virus Alert !
Hi, I am an Albanian virus but because of poor technology in my country unfortunately I am not able to harm your computer. Please be so kind to delete one of your important files yourself and then forward me to other users. Many thanks for your cooperation! Best regards,Albanian virus
Yes
No
Cancel

Agenda

- Phishing
  - Útočník skopíruje stránku a spustí jí na své doméně

Agenda

- DOM tampering
  - Útočník využije například plugin v prohlížeči pro upravení DOM stromu stránky

Agenda

- SMS hijacking
  - Útočník nahraje do mobilního tokenu aplikaci, která čte 2. faktor z SMS
- Overlay aplikace
  - Útočník nahraje do mobilního tokenu „neviditelnou“ overlay aplikaci, zachytává touchscreen eventy

Agenda

- DNS hijacking
  - Útočník propašuje vlastní DNS server do klientského zařízení

Agenda

Jak se bránit?

Q&A

Zajímá vás víc? Stavte se na našem stánku
https://www.threatmark.com/career/

michal.toman@threatmark.com

www.threatmark.com