PT LAB

PŘÍPADOVÁ STUDIE - SOLARWINDS

Co se stalo? A jak tomu předejít?

Lukáš Králík
PT LAB – Penetration Testing Laboratory
Fakulta aplikované informatiky
Univerzita Tomáše Bati ve Zlíně
E-mail: kralik@utb.cz
tel.: +420 576 035 188

Důvěřujete oficiálním dodavatelům SW nástrojů, že dodávaný produkt je stabilní a bezpečný?

White-box pentesty

Kontrola integrity dat

Definitivní knihovna médií

Zkoumáte a testujete SW dodávaný třetí stranou?

Externí pentesty

Interní pentesty

Black-box pentesty

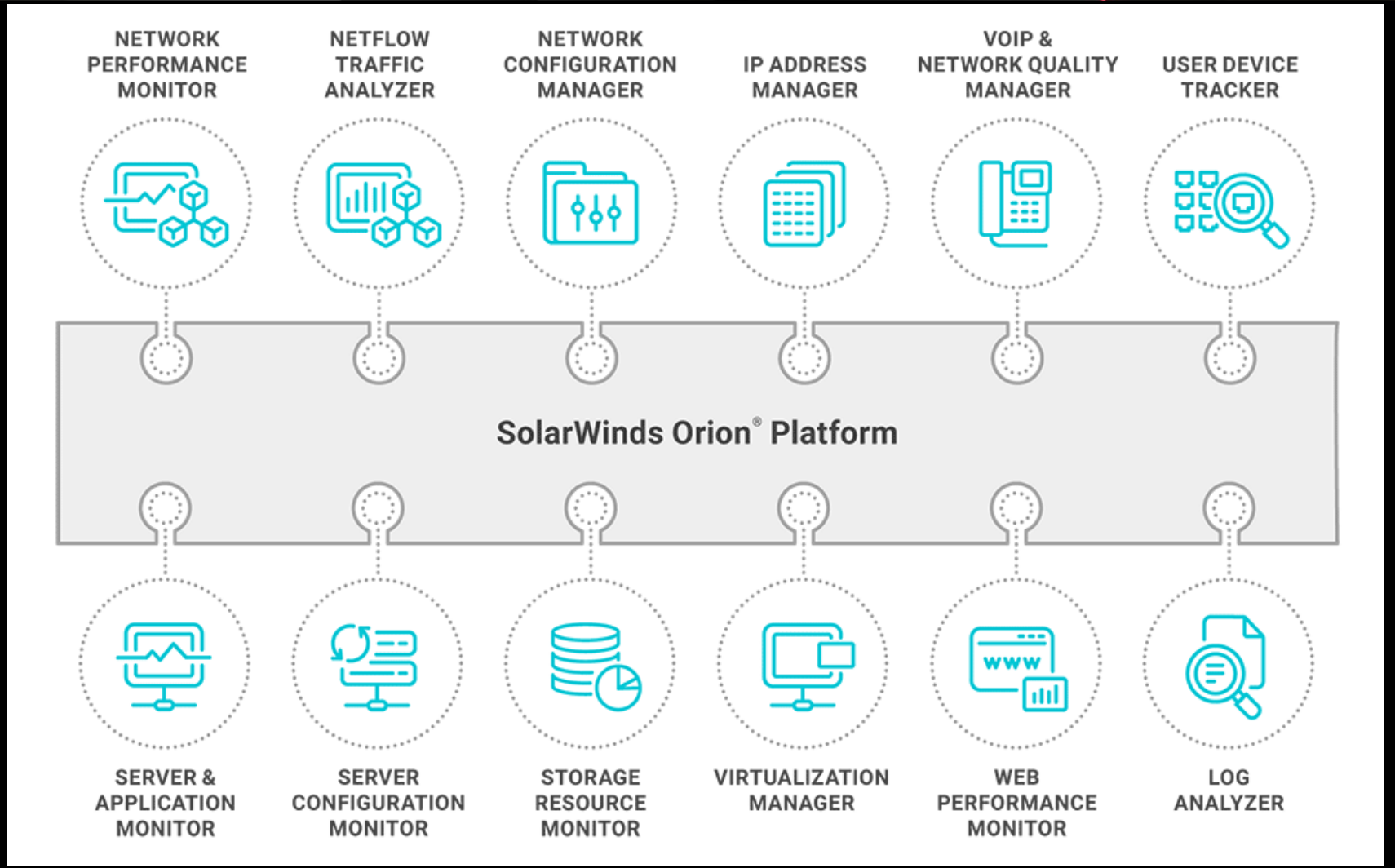
Patch management

O co jde?

- V ČR se o útoku příliš nevědělo
  - Zpráva proletěla médii jak kouř komínem
  - 17.12. články na novinky.cz, irozshlas.cz, lupa.cz, apod.
  - 14.12. oficiální varování – NÚKIB
- Zneužití supply-chain k distribuci malwaru
  - Infikování serverů Solarwinds
  - Distribuce přes oficiální update
  - Vytvoření backdooru do systému s nástrojem Solarwind Orion

Solarwind Orion

- Sofistikovaný nástroj pro komplexní monitoring a správu podnikové sítě a cloudu
- Okolo 30 tis. zákazníků
  - Dotčených 18 tis. (oficiální tvrzení… ☺)
- Cena:
  - Network Performance Monitoring 64 tis Kč/rok/100 zařízení
  - Server and Application Monitoring 66 tis Kč/rok/100 zařízení
  - Storage Resource Monitor 65 tis Kč/rok/25 disků

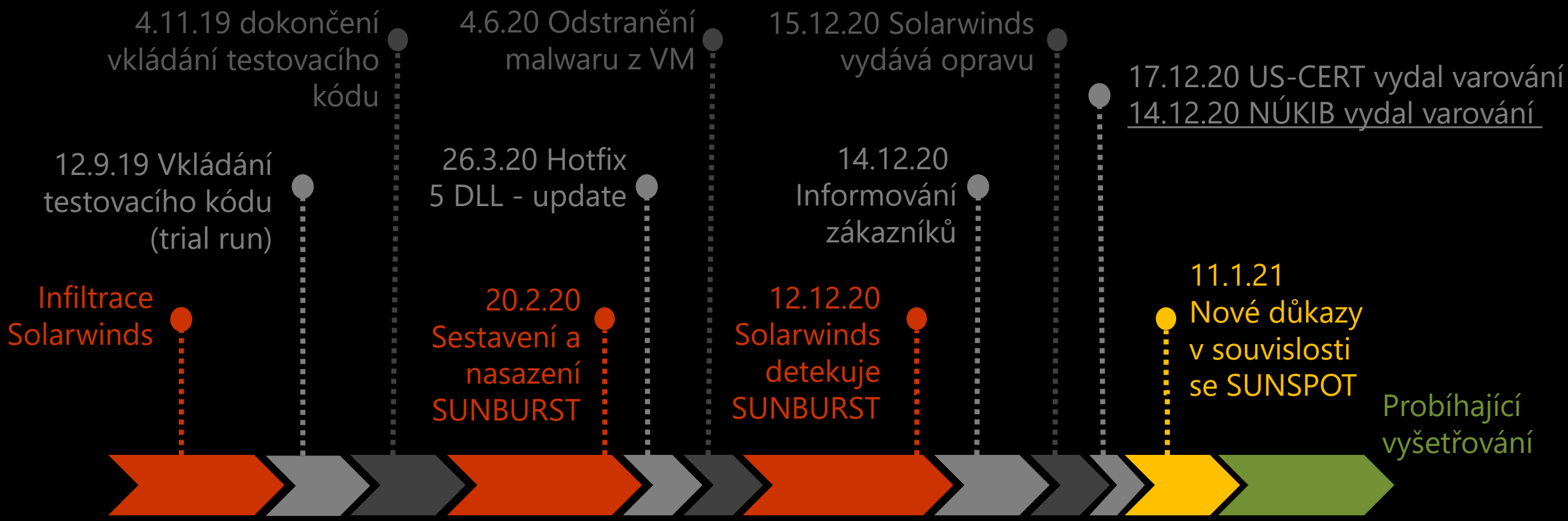

NETWORK PERFORMANCE MONITOR
NETFLOW TRAFFIC ANALYZER
NETWORK CONFIGURATION MANAGER
IP ADDRESS MANAGER
VOIP & NETWORK QUALITY MANAGER
USER DEVICE TRACKER
SolarWinds Orion® Platform
SERVER & APPLICATION MONITOR
SERVER CONFIGURATION MONITOR
STORAGE RESOURCE MONITOR
VIRTUALIZATION MANAGER
WEB PERFORMANCE MONITOR
LOG ANALYZER

Detaily útoku

- Výchozím bodem byl soubor s trojským koněm obsahující backdoor
- Standartní windows installer patch file
  - Zcela běžný obsah zdrojů pro update
  - *Infikovaná knihovna DLL - SolarWinds.Orion.Core.BusinessLayer.dll*
- Virus total označil tento soubor jako škodlivý **„pouze“ ve 14 případech** (celkem 69 AV enginů)
- Při detailnější analýze byl objeven blocklist k detekci forenzních a AV nástrojů pomocí procesů, služeb a ovladačů

Detaily útoku

- APT!!!
- Supply-chain byl kompromitován prostřednictvím následujících produktů:
  - Orion Platform 2019.4 HF5, version 2019.4.5200.9083
  - Orion Platform 2020.2 RC1, version 2020.2.100.12219
  - Orion Platform 2020.2 RC2, version 2020.2.5200.12394
  - Orion Platform 2020.2, 2020.2 HF1, version 2020.2.5300.12432
- Kompletní výčet indikátorů kompromitace na webu NÚKIB



Zdroj: OrangeMatter

Pamatujete na TrueCrypt?

- Šifrované kontejnery – kaskádové šifrování
- Ver. 7.2 – backdoor
- Ver. 7.1 – bezpečná

WARNING: Using TrueCrypt is not secure as it may contain unfixed security issues

This page exists only to help migrate existing data encrypted by TrueCrypt.

The development of TrueCrypt was ended in 5/2014 after Microsoft terminated support of Windo
platforms (click here for more information). You should migrate any data encrypted by TrueCrypt

Migrating from TrueCrypt to BitLocker:

If you have the system drive encrypted by TrueCrypt:

1. Decrypt the system drive (open **System** menu in TrueCrypt and select **Permanently Decryp**
2. Encrypt the system drive by BitLocker. Open the Explorer:

Solarwind Orion

- Vydání oficiálního updatu obsahující backdoor
- Manipulace s originálními zdroji
  - Injektace malwaru

TrueCrypt

- Vydání oficiálního updatu obsahující backdoor
- Manipulace s originálními zdroji
  - Vydání nové verze
  - Odlišný „rukopis“ kódu

Nízké riziko ≠ nulová pravděpodobnost

Proaktivní přístup

1) Připravit se i na málo pravděpodobné scénáře
   - Vytvoření plánů a postupů na řešení krize
   - Záložní řešení při nedostupnosti služeb
2) Segmentace sítě
3) Detailní nastavení práv pro zápis do jednotlivých složek
4) Monitoring sítě
   - SIEM
   - Využití strojového učení
5) Patch management
6) Definitivní knihovna médií
7) Testování SW nástrojů třetích stran
   - Hash otisky
   - Obsah souborů ve složce
   - Pentesty

„Bezpečnost je matka nebezpečí a babička destrukce.“

Thomas Fuller

Lukáš Králík
PT LAB – Penetration Testing Laboratory
Fakulta aplikované informatiky
Univerzita Tomáše Bati ve Zlíně
E-mail: kralik@utb.cz
tel.: +420 576 035 188