SOPHOS
ANTI-VIRUS

Kompjuterski virusi

Lucijan Carić, Qubis d.o.o.

www.sophos.com

Kompjuterski virusi

SOPHOS
ANTI-VIRUS

- Osnove o virusima
- Kako virusi inficiraju

SOPHOS
ANTI-VIRUS

Osnove o kompjuterskim virusima

Maliciozni programski kôd

SOPHOS
ANTI-VIRUS

- Trojanski konji
- Virusi
- Crvi

Trojanski konji

SOPHOS
ANTI-VIRUS

- Su izvršni kôd
- Ne mogu se samokopirati
- Štetne popratne posljedice

Virusi

SOPHOS
ANTI-VIRUS

- Razmnožavaju se samokopiranjem
- Štetne popratne posljedice
- Prikrivanje

Crvi

SOPHOS
ANTI-VIRUS

- “Samodovoljni” virusi
- Obično koriste Internet

Sadržaji pogodni za infekciju

SOPHOS
ANTI-VIRUS

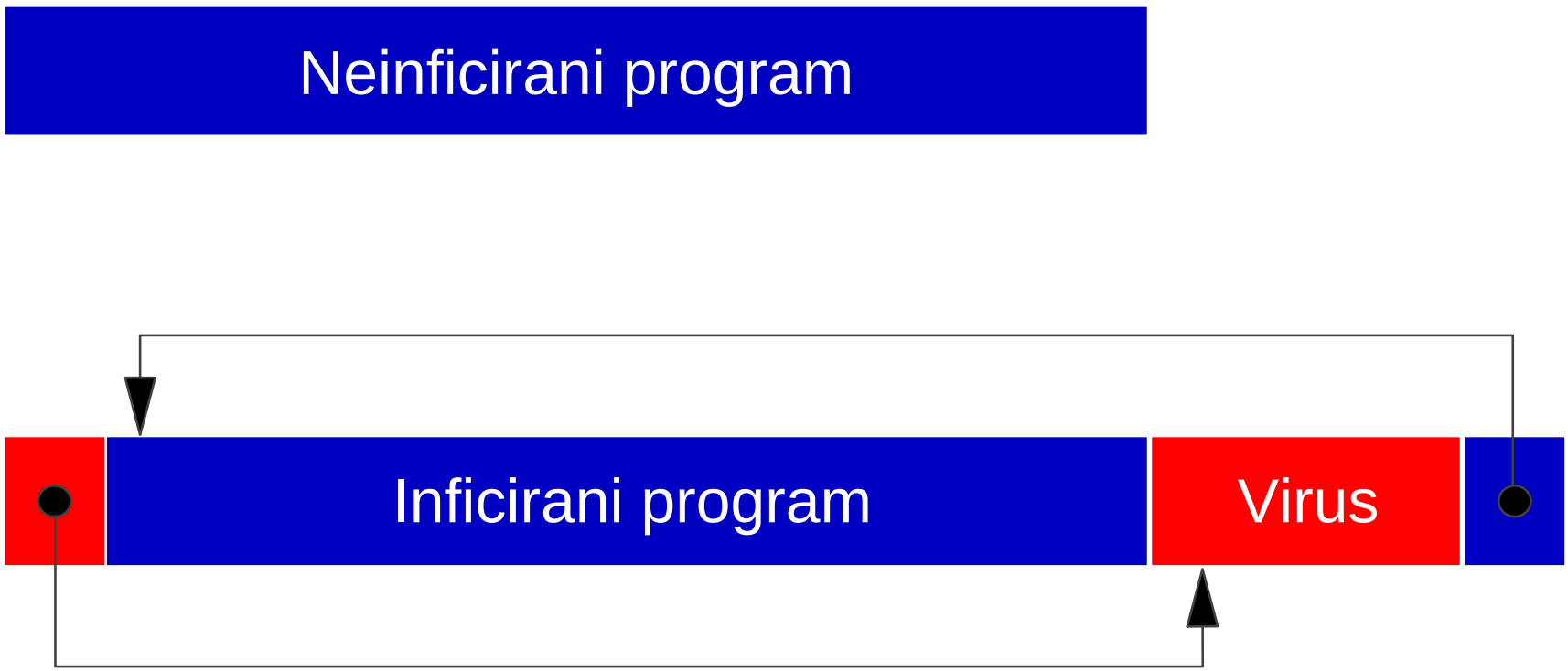
- ✓ Izvršni
- ✓ Izmjenjivi

Što napadaju virusi

SOPHOS
ANTI-VIRUS

- Master *boot* sektor
- DOS *boot* sektor
- Izvršne datoteke
- *Overlay*
- Datoteke s makro kôdom

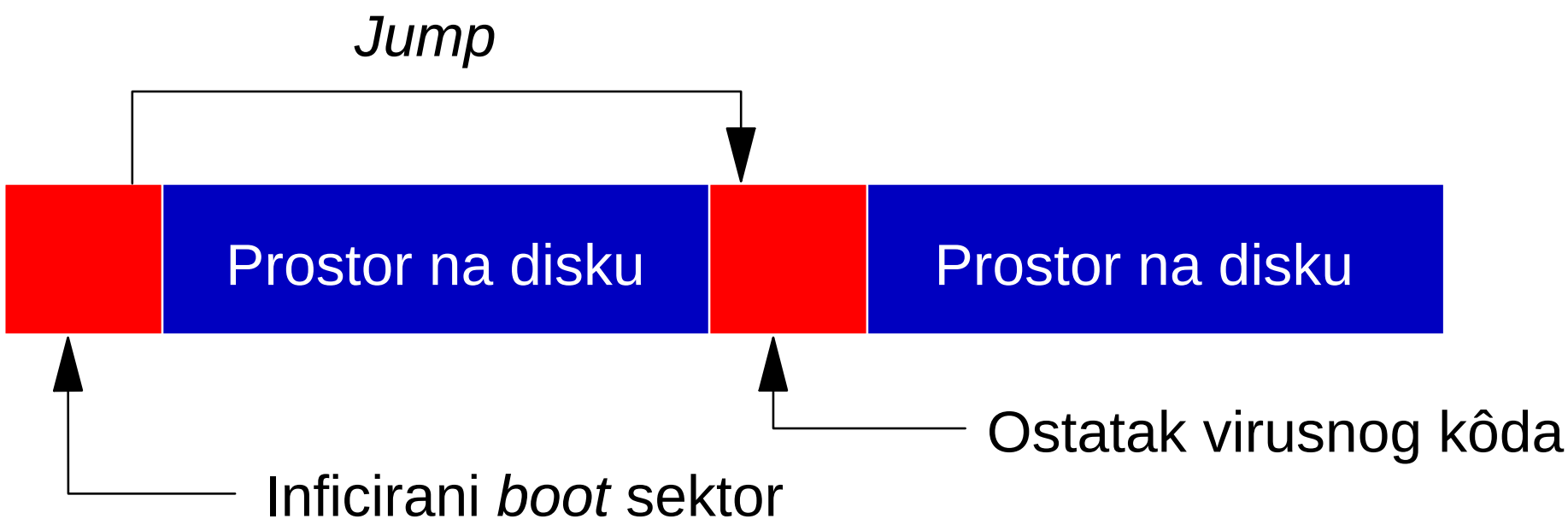
Parazitski virusi



Šire se razmjenom programa

Boot sektor virusi

SOPHOS
ANTI-VIRUS



Šire se razmjenom diskova

Makro virusi

SOPHOS
ANTI-VIRUS

Šire se otvaranjem i razmjenom dokumenata

Crvi

SOPHOS
ANTI-VIRUS

Registry:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
      WormCode = “C:\HIDDEN\WORMCODE.EXE”
```

WORMCODE.EXE
Nađi slijedeći kompjuter
i instaliraj se na njega

Crvi su “samodovoljni” virusi

SOPHOS
ANTI-VIRUS

Kako virusi inficiraju

Što izaziva infekciju?

SOPHOS
ANTI-VIRUS

- Izvođenje inficiranog programa
- Dvostruki klik = IZVRŠI!
- *Open* (otvori) = IZVRŠI!
- Startanje sustava s inficiranog diska
- Otvaranje inficiranog dokumenta