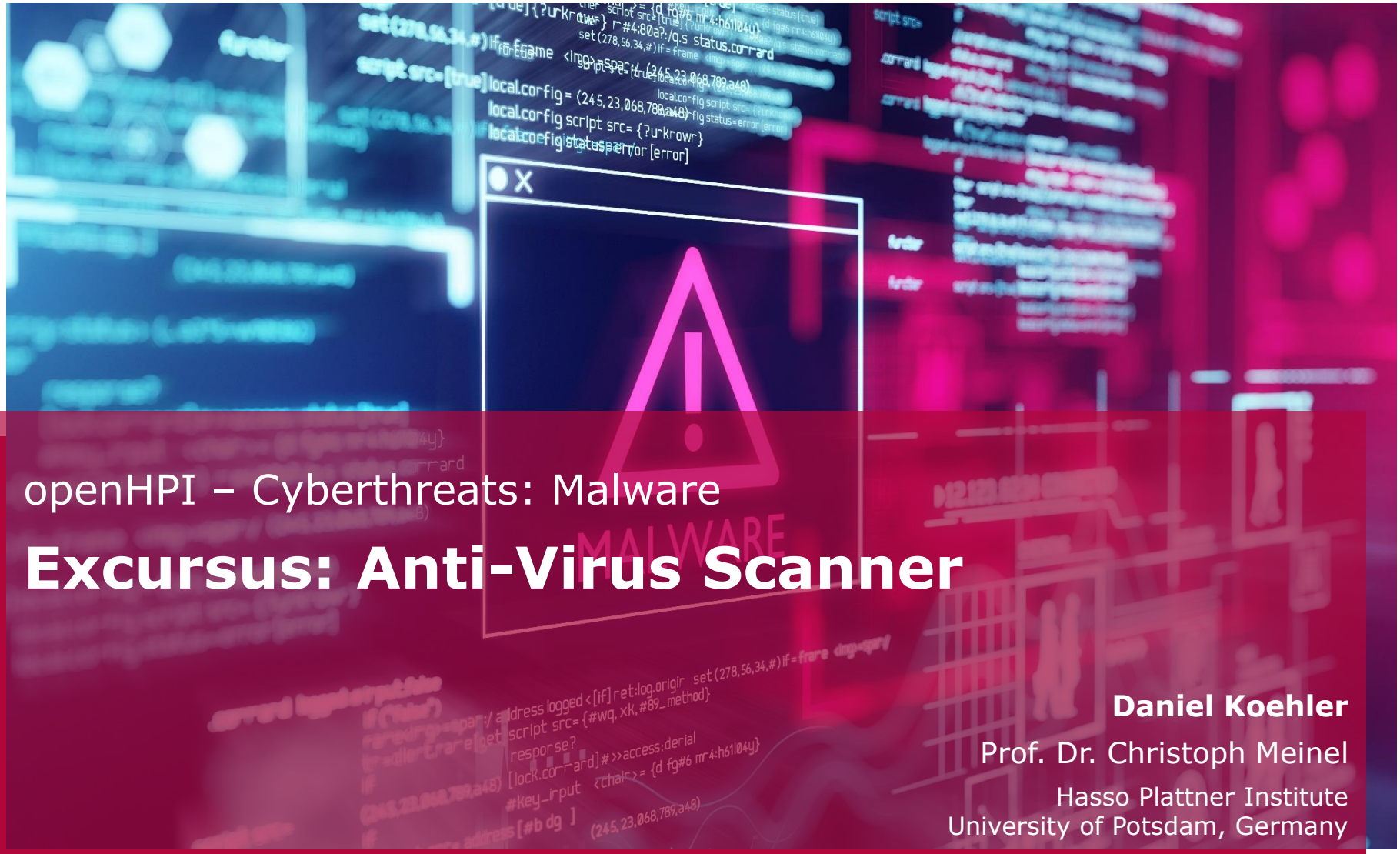


openHPI – Cyberthreats: Malware

Excursus: Anti-Virus Scanner

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

Anti-Virus Scanner

Short Repetition:

- Offers methods to detect **Viruses**
- Aside viruses, other malware such as Worms, Trojans, Spyware are detected
- Can therefore be considered **Anti-Malware Programs**
- Can also monitor Internet connections and warn before accessing unsafe websites, attachments or downloads

Anti-Virus (AV) Scanner

How do AV-Scanner work?

Database from AV-Scanner contains so-called **Signatures**

- „**Fingerprints**“ of already known Malware
- „Fingerprints“ can be of different types:
  - **Hash-value** of a File
  - **Characteristic Code Sequences**
- Once AV-Scanner has found a known Fingerprint, the corresponding file is most-probably malicious
- Corresponding files are then removed / quarantined

Hash-Signature based Detection

Anti-Virus Scanner with Signature Database

Name	Hash Signature
Virus_1	76b5b94247f6c47bdde683239b1dedaa
Virus_2	06221bdf4844888372472b95aa4deab7
Worm_1	**8fad2b440e501c83276223b417655c05**
Trojan_1	D2e20c337ef4bf076dcadc92871d2b86
...	...

Course-Information.txt

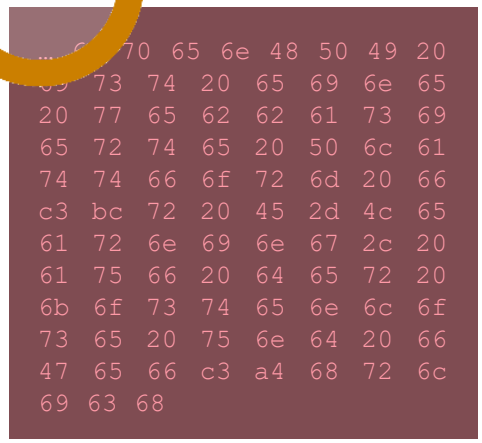
Hash Calculation

Byte-Signature based Detection

Anti-Virus Scanner with Signature Database

Name	Byte Signature
Virus_1	56 69 72 75 73 5f 31
Virus_2	47 65 66 c3 a4 68 72 6c 69 63 68
Worm_1	77 75 72 6d 5f 31
Trojan_1	74 72 6f 6a 61 6e 65 72 5f 31

Course-Information.txt



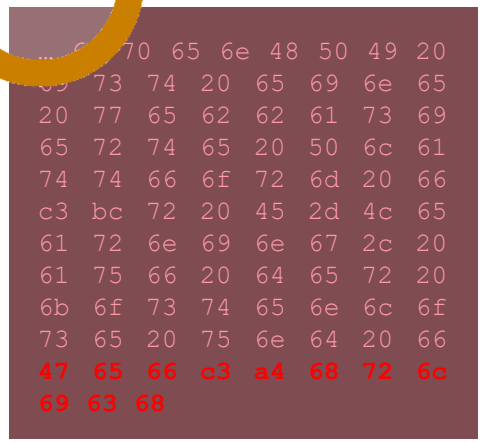
Byte-Sequence from Course-Information.txt

Byte-Signature based Detection

Anti-Virus Scanner with Signature Database

Name	Byte Signature
Virus_1	56 69 72 75 73 5f 31
Virus_2	**47 65 66 c3 a4 68 72 6c 69 63 68**
Worm_1	77 75 72 6d 5f 31
Trojan_1	74 72 6f 6a 61 6e 65 72 5f 31

Course-Information.txt



Byte-Sequence from Course-Information.txt

Anti-Virus Scanner: **Updates**

Regular updates are particularly important for AV-Scanner!

- Developers and researchers constantly find new malware with new signatures that are added to the databases
- Regular updates therefore ensure that the most-current information is available to each scanner
- Furthermore, as with every Software, Updates help to keep the Software secure!

Anti-Virus Scanner: **Challenge**

- Malware can be modified easily by the cybercriminals to receive a „new" / different signature
  - With **any** change in the original Malware, the **Hash Fingerprint** will be completely different
  - The **Byte-Signatures** can be changed by slightly modifying the commands that are executed by the malware
- Some Malwares are able to alter themselfes to circumvent AV-Scanner, so-calles **Polymorphic Malware**

Anti-Virus Scanner: **Heuristic Analysis**

Heuristic Analysis is a method to identify **new** malware versions, two approaches are differentiated:

Static Heuristic Analysis

- Assessment of Byte-Sequence of a file
- Analysis if **partial** sequences of a file are known to malware databases
- Upon level of risk, alarm can be raised

Dynamic Heuristic Analysis

- File for assessment is brought into a shielded execution environment
- File is executed / opened and **behavior** is monitored
- If behavior is „strange", alarms can be raised / file can be deleted