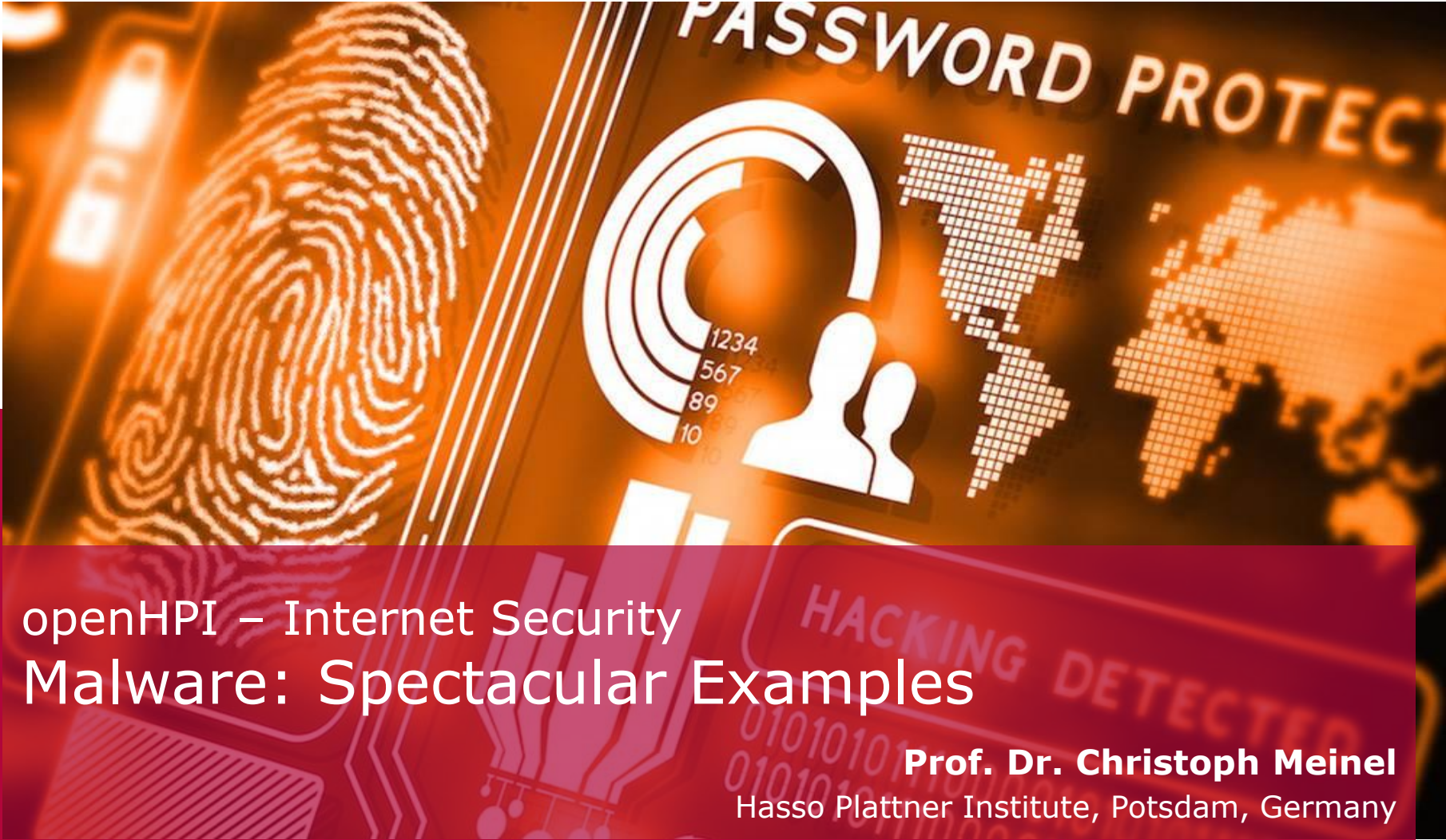




openHPI – Internet Security Malware: Spectacular Examples

Prof. Dr. Christoph Meinel
Hasso Plattner Institute, Potsdam, Germany

Malware - Some Spectacular Examples

Here are some popular attacks and security incidents on the Internet caused by malware:

- „cookie monster“
- macro viruses „I love you“
- conficker
- stuxnet
- regin
- „campaign“ malvertising
- Ransom32
- WannaCry

Cookie Monster

Cookie monster is neither a proper virus (replicates itself) nor a worm (does not spread), it is therefore called a "proto virus"

- First world-wide example of computer malware
- Did its worst in the late 1960s
- Originally intended for users of the computer network of Brown University
- Sent messages that blocked other applications and asked for "cookies"
 - Significantly impaired the performance of the affected computer
- The user was only able to use the blocked applications and continue working after typing "cookie"

ILOVEYOU-malicious software launched from the Philippines on 5 May 2000

- Sent as an e-mail with the subject "ILOVEYOU" and the attachment "LOVE-LETTER-FOR-YOU.txt.vbs"
- The .vbs (Visual Basic Script) extension was not displayed in Windows systems and affected users opening the malware as a supposed text file
- Infiltrated malware then sent itself to all contacts from the Windows Address Book and overwrote image files
 - Users viewed e-mail as trustworthy because they came from a known contact (from the address book)
- Damage is estimated at 5.5 - 8.7 billion US \$
- An estimated 10% of all Internet users were affected; 50 million infections were recorded in the first ten days

Conficker

Conficker was first discovered in November 2008

- Spiked Windows systems via both
 - vulnerabilities in Windows and
 - attacks on administrator passwords
- Add-ons were loaded to other infected computers via the Internet
- Integrated affected systems in a botnet
- Different types of attack
 - Commands are received over the network and executed without further checking
 - Installed on removable media and abuses "autorun" function
 - Dictionary attacks on admin password
 - Uses file / printer sharing for distribution

Stuxnet worm entered circulation at the end of 2007, but was not discovered until 2010

- Used a variety of previously unknown vulnerabilities in Windows systems and networks
- Subsequently searched for control software from Siemens:
 - Software for the control of technical processes in waterworks, pipelines, factories or nuclear power plants
- Once introduced into the network via removable media (USB stick) only sporadic Internet access is required for communication with C&C server
- Secretly changed settings of the control software
- As a result, Stuxnet caused damage in Iranian nuclear power plants and a delay in its nuclear program

Regin

Regin is highly developed malware discovered in 2012 and mainly used for espionage

- In most cases Regin attacks Windows systems and contains a variety of functions:
 - Stealing access information
 - Remote access to system (control of mouse and keyboard)
 - Recording of data traffic
 - ...
- Also infected systems from mobile operators and could thus influence and spy on the communication
- The high quality of the malware, the complex scope of functions and rumors point to the fact that the attackers were state sponsored

“Kampagnen” Malvertising

Malvertising – Malicious advertising

- An attacker registers with an ad network and distributes malicious advertising
- Malware is then loaded by the malicious ad when it appears to the user
- In October 2015, cybercriminals distributed malware in the so-called “Kampagnen” action
- Affected internet sites were:
 - ebay.de
 - t-online.de
 - arcor.de
 - ...

Ransom32

Ransom32 has been offered as a ransomware service on relevant Internet sites since December 2015

- Malware is simply generated through the website
- Objective: extorting Bitcoins (cryptocurrency) from victims
- 25% of the "revenue" is retained by the developers

The developers use techniques that enable execution on different platforms (e.g., Windows, Mac, Linux)

- In addition to encrypting the user data, ransom32 also contains other functions, e.g. locking the computer

WannaCry

WannaCry is a ransomware that was mainly active in May 2017

- According to Microsoft, NSA discovered the vulnerability in MS Windows, but used it to build an exploit rather than to report it to Microsoft
- NSA informed Microsoft only after the exploit was leaked from NSA by a hacker group
- Microsoft provided patches for this vulnerability in March 2017, but many companies and users didn't apply updates
- Exploit was used by other hacker groups to build ransomware that encrypts data on the computer
- Various companies were affected, for example:
 - Deutsche Bahn □ Honda □ Nissan
 - O2 □ FedEx □ Hospitals in UK