openHPI Course: Cyberthreats by Malware

Emotet

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

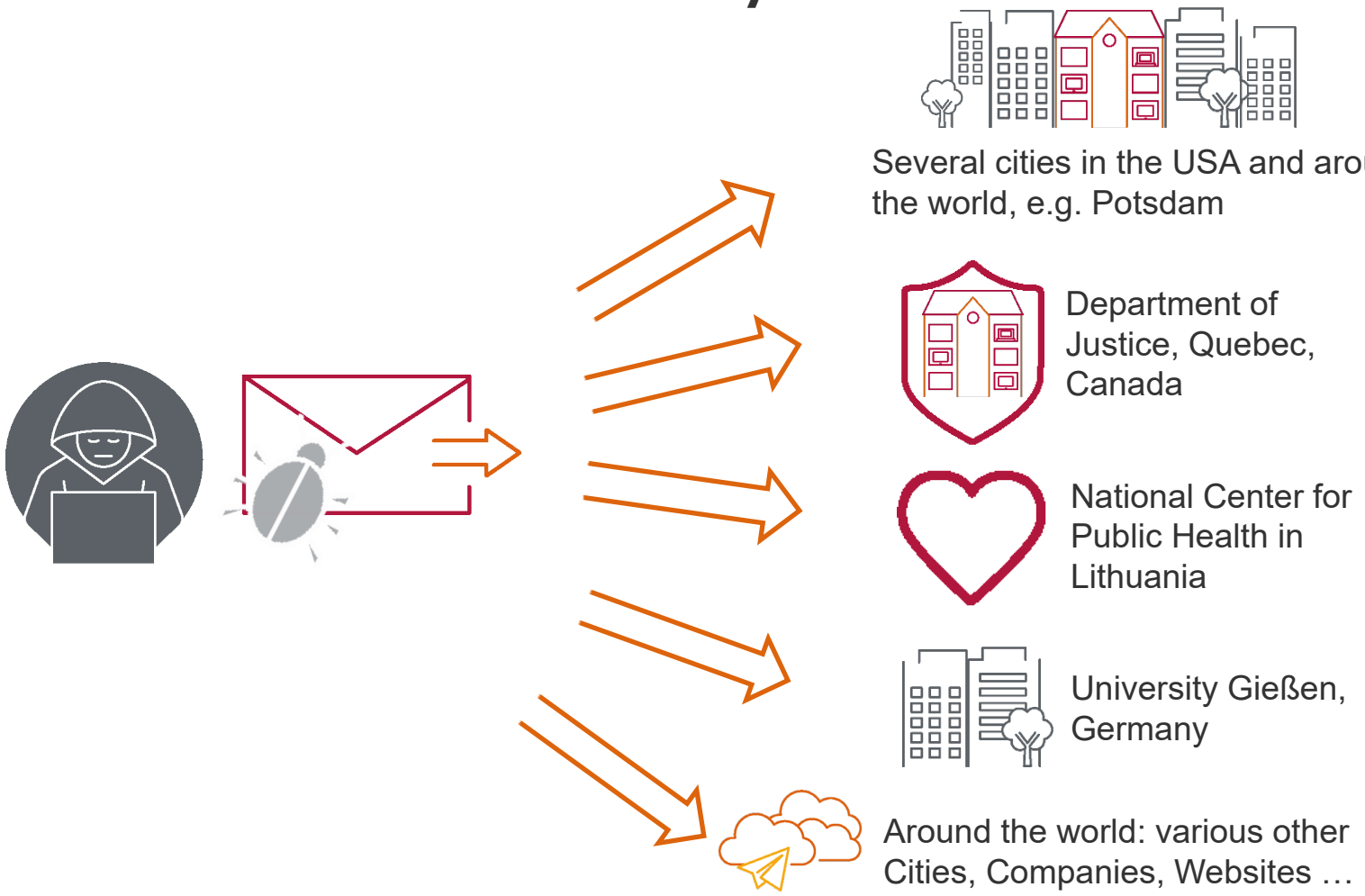
Emotet in The News

Over the past years, Emotet has produced news headline in various fields with severe results

- It accounts for 7% of malware infections globally based on Check Point‘s Global Threat Index from December 2020
- So far, Emotet has managed to infect various institutions around the world

Emotet in The News (2/2)

Emotet infections over the last years:



Emotet – a Prominent Virus Example

The malware **Emotet** is classified as a virus

- Needs interaction from the user to infect a system and spread further
- Usually **spread via emails** with malicious attachments or **links to malicious URLs**
- Has to be actively accessed / opened by user …

Emotet – The Actions it Takes

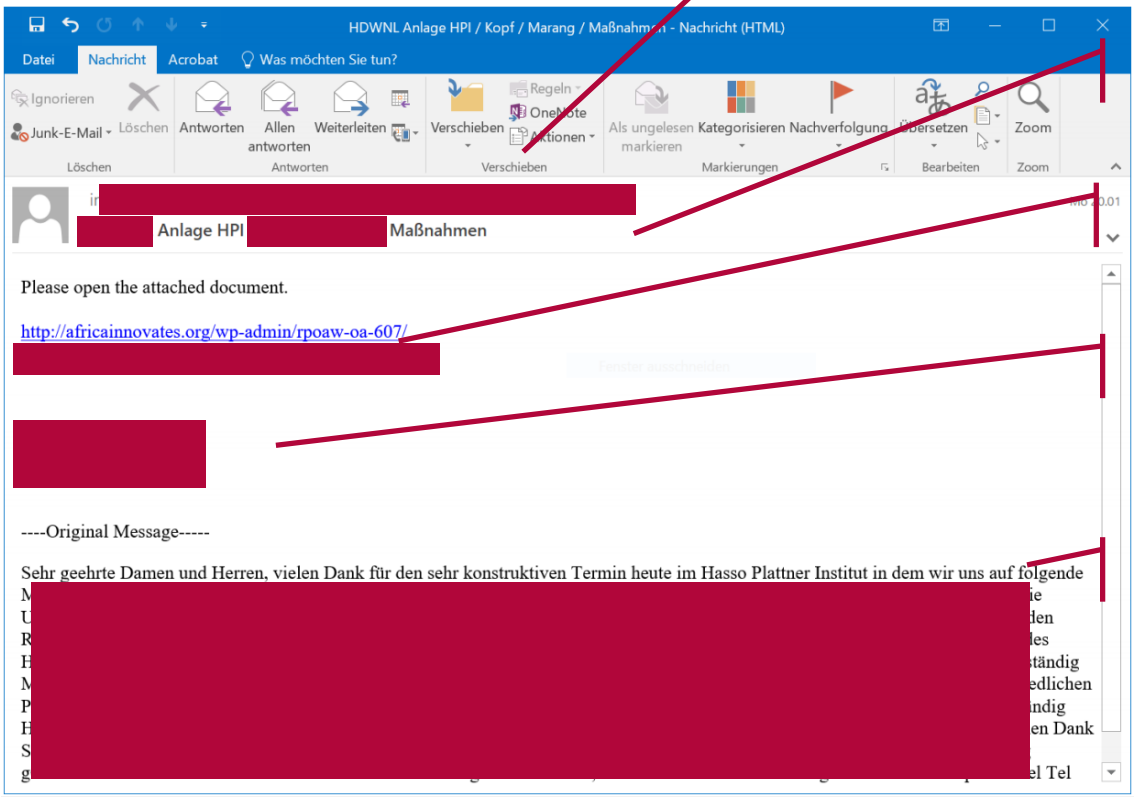
- In regard to the actions taken by the malware, Emotet could not be specifically classified
- It serves as a staging malware and will thus be used to deliver further kinds of malware to a target system
- Those can be various:
  - trojans
  - ransomware
  - scareware
  - keylogger
  - …

Why is Emotet So Dangerous?

Compared to "usual" spam emails…

- Emotet spam emails are particularly dangerous because they appear to be very realistic
- Upon infection, Emotet collects **data** from the user's email account
  - with whom the user communicates
  - which are the current topics that the users communicates about? (**email subjects**, **email contents**)
- Emotet then uses such kind of information to send further emails from infected email accounts to other users
- Spam emails from Emotet therefore look really realistic

Examples of Emotet (1/2)



Hijacked user's email account as sender of the email

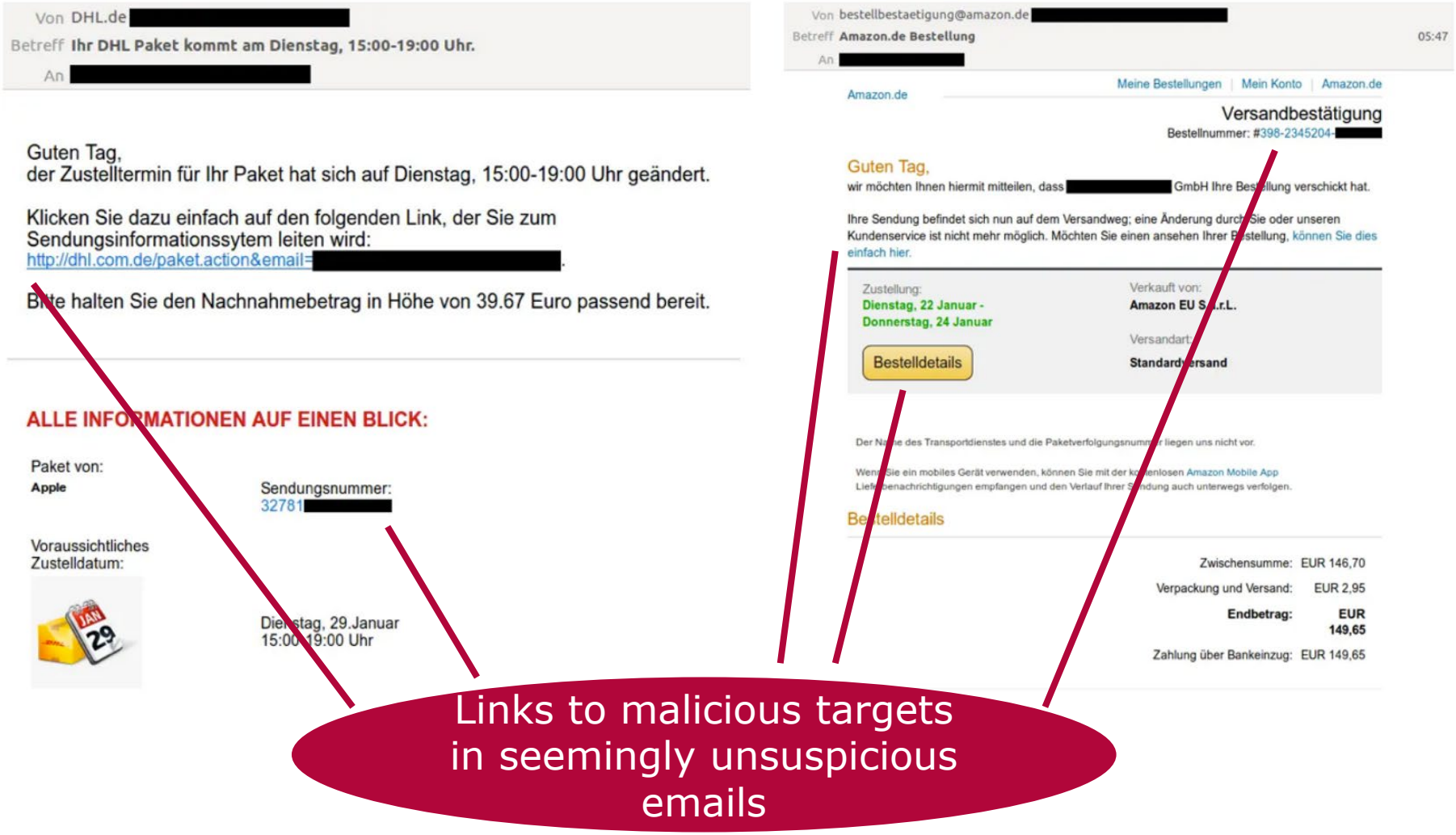
Subject of a previous email

Attached, malicious link

Email signature from the hijacked user

Content from the previous messages in the conversation

Examples of Emotet (2/2)



How Can You Recognize Phishing Emails?

- Be suspicious of mails that you do not expect
- Missing personal salutation (just: ”Hello“ or “Dear customer“)
- Wrong language, e.g., “you use Amazon” in English but received email is in German)
- Typos or misformattings (no more in well-crafted phishing mails)
- Apparent sender address is not consistent with real (technical) sender
- **Strange link targets**: move the mouse pointer over a link or image button in the email and wait for a tooltip to appear. The tooltip will contain the real link target.
  Do not click the link if the the URLs are **different**