Highlights of Update Cybersecurity: Gamechanger für die Finanzfunktion?
Event date: 12 June 2024
Location: Oeconomicus, Heinrich Heine Universität Düsseldorf

Documentation by: Ardi Kaars
Date of release: 14 June 2024

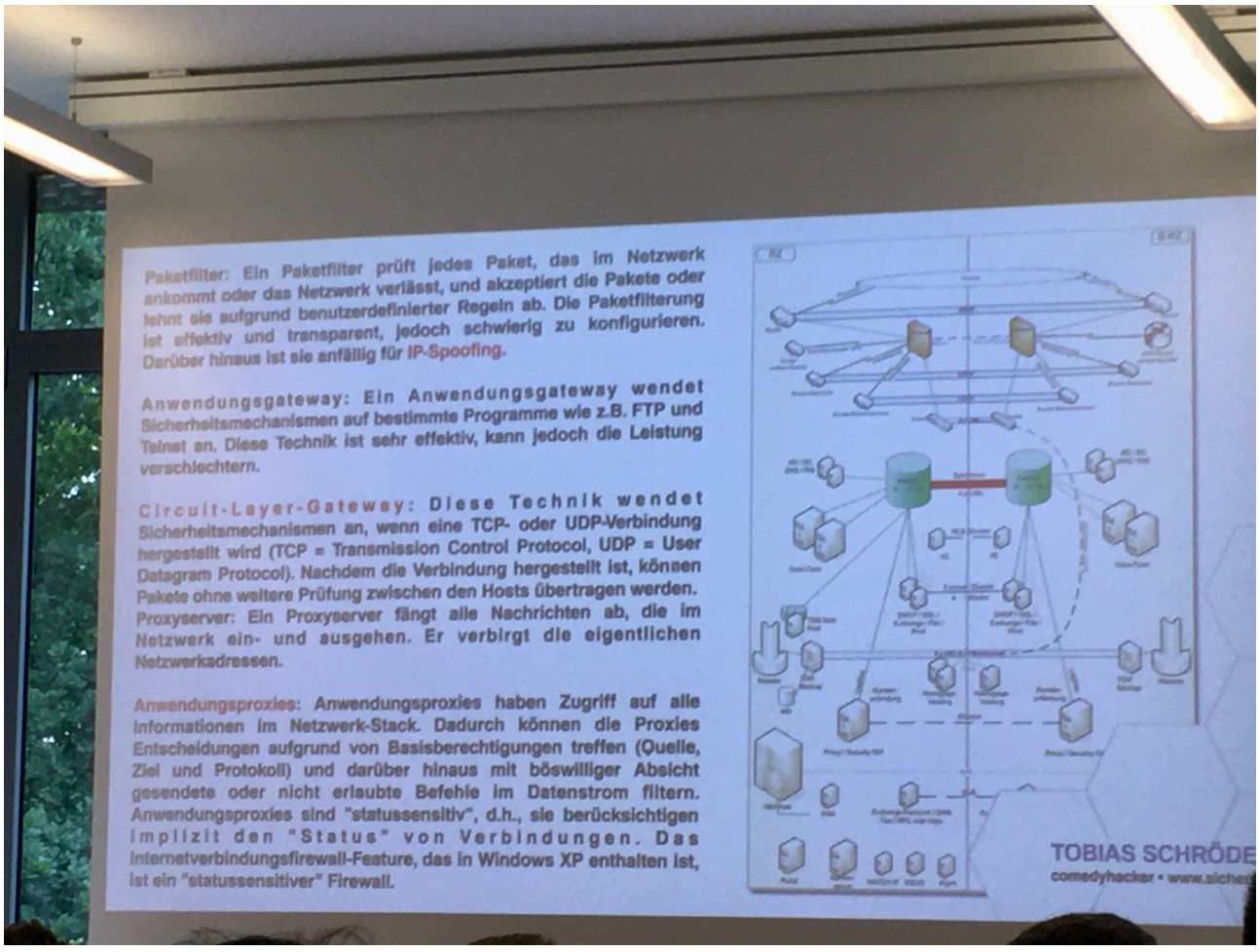
Introduction: About the event itself

Update Cybersecurity: Gamechanger für die Finanzfunktion is an event where perhaps one of the most challenging issues in today's economy is analysed and discussed: How to safeguard digital tools in economic life and firm's decision-making processes? This event, hosted at the Heinrich Heine University of Düsseldorf, analyses trends in cybersecurity through the lens of German experts, yet their insights are very much applicable too on other (European) countries.

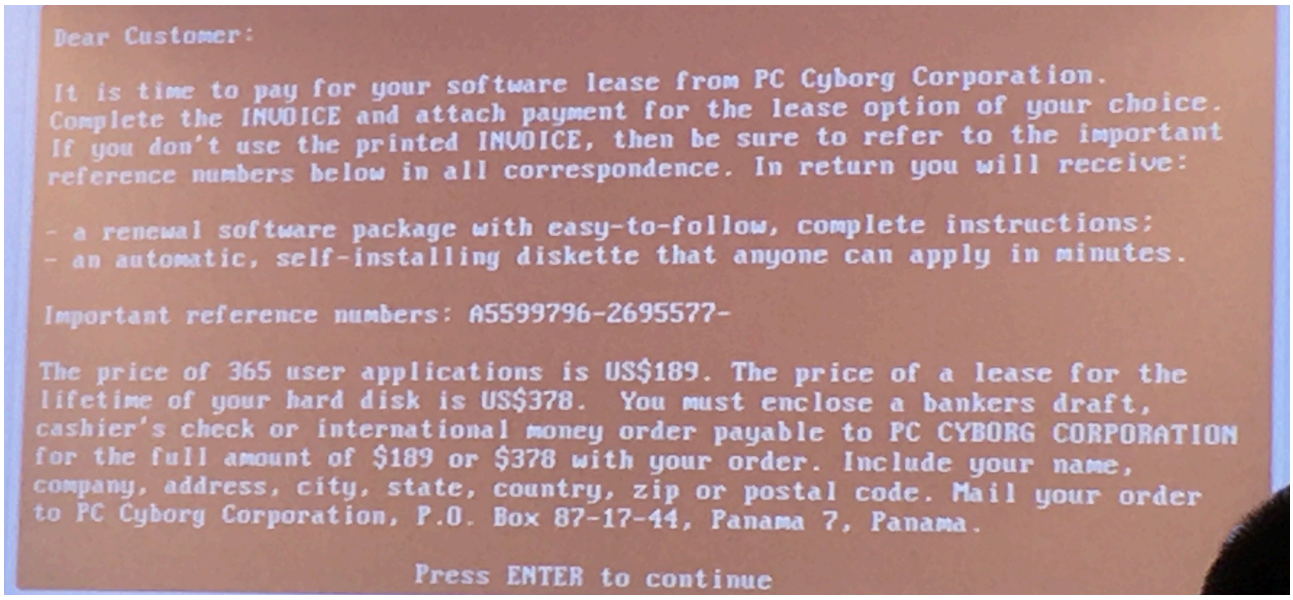
In this document, I have zoomed in on one speaker that I found particularly interesting. Mr. Tobias Schrödel, who held a presentation on the Darknet offered a plethora of information and things to watch out for as a company, but also as a private citizen. There are no direct quotations, yet covered topics and answered questions have been documented below with utmost care and accuracy based on my own notes, careful listening and a final review. Moreover, I have included several photographs that capture important (sub)topics. The information has been documented with explicit permission of the speaker.

I. 14:30 - Cyber@attacken verstehen und abwehren (To understand and shield off Cyber@attacks) by **Tobias Schrödel (Comedyhacker, Munich)**

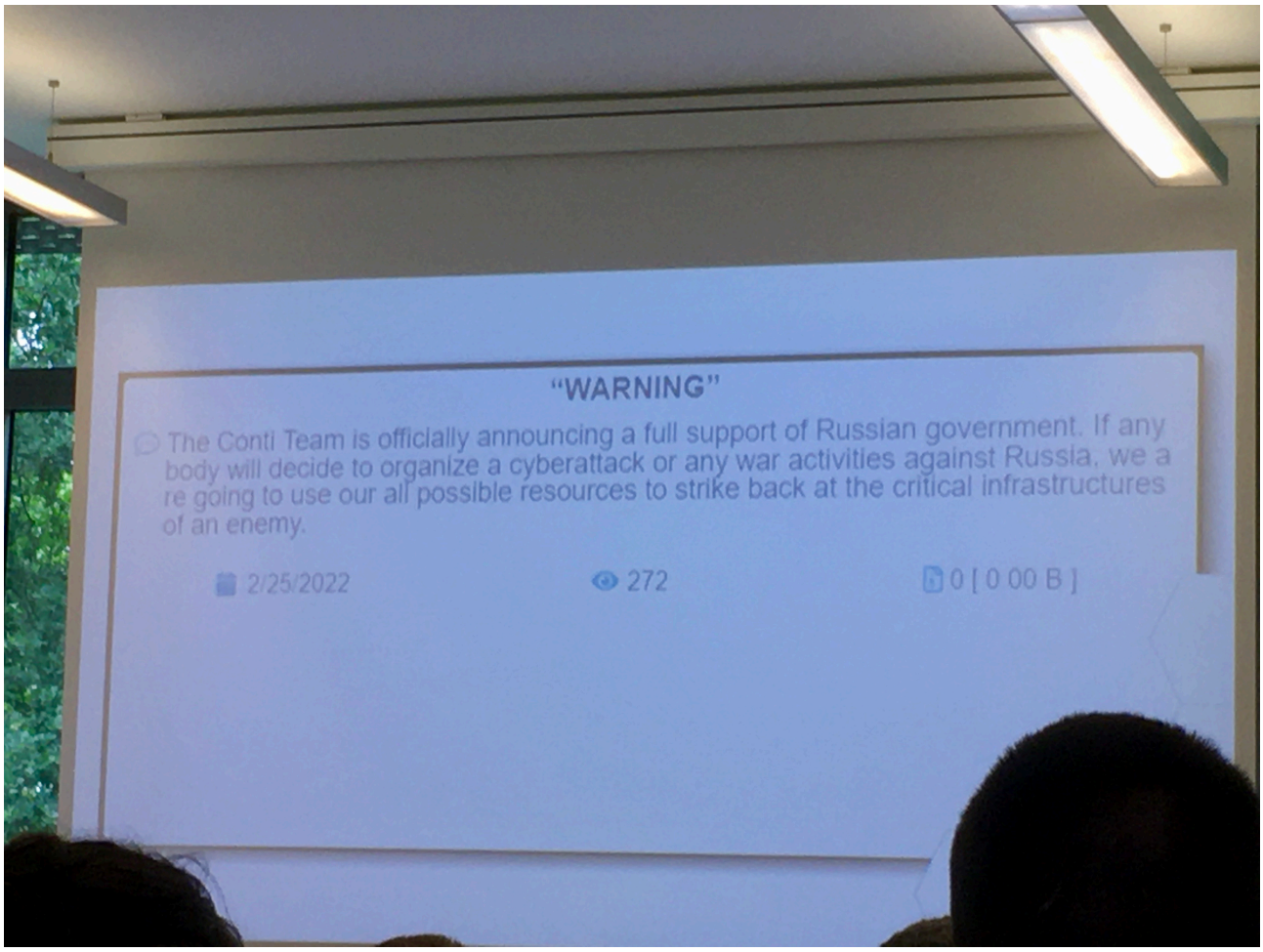
- Today's lecture will focus on Darknet
- You need to understand tech to catch up and outsmart criminals
- The theme of now is ransomware -> This is a two-sided sword -> When criminals take our data, we no longer have access to it and neither do the police, FBI etc.
- Revenue loss due to cybercrime went down from $766 million in 2021 to $457 million in 2022
- Due to what is at stake at a cyberattack such as patents, purchase prices etc., firms sometimes decide to pay the criminals nevertheless
- A typical setup of a firewall can be found on below picture



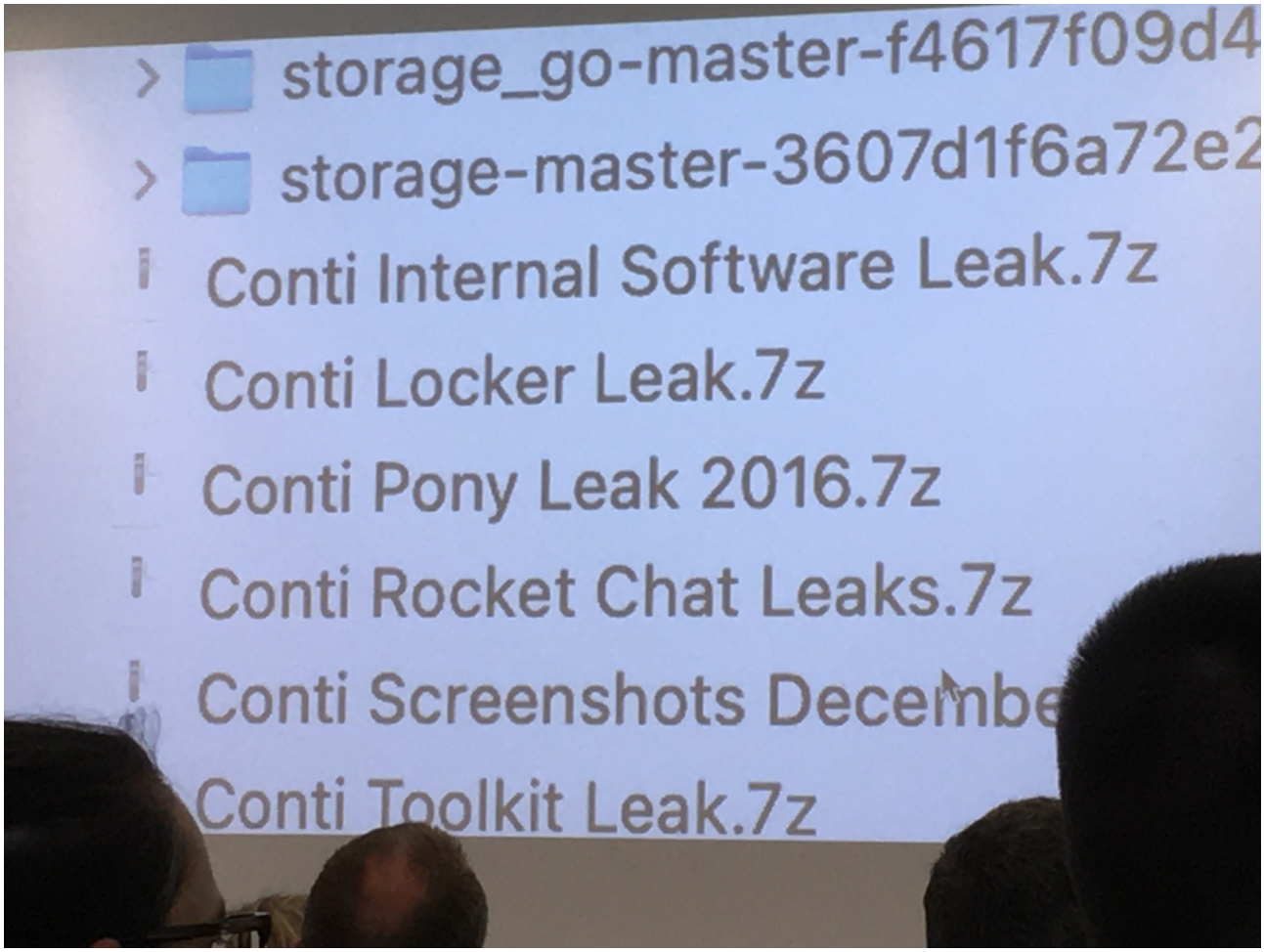
- Yet, cybercriminals cannot use high-speed tech, and that is their disadvantage -> oftentimes finishing a cyberattack takes weeks or months of internet activity
- See below picture for one of the first viruses ever (1998)



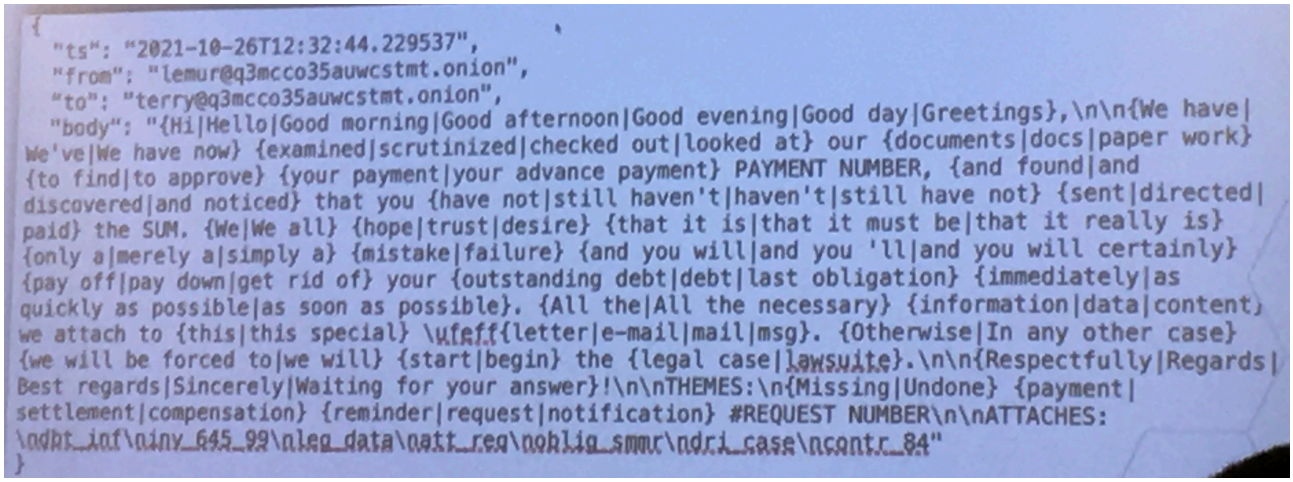
- The $457 million figure was derived from Cryptowallets
- In Russia, there is no prosecution for attacking non-Russian entities
- One Russian gang specialised into that was Conti Group -> This one is no longer active -> They sent a message one day after the Ukraine invasion (see picture below)



- The Conti Rocket chat leaks is one of the most notorious ones -> Providing a treasure of information on Conti Group's last six months of correspondence, see below

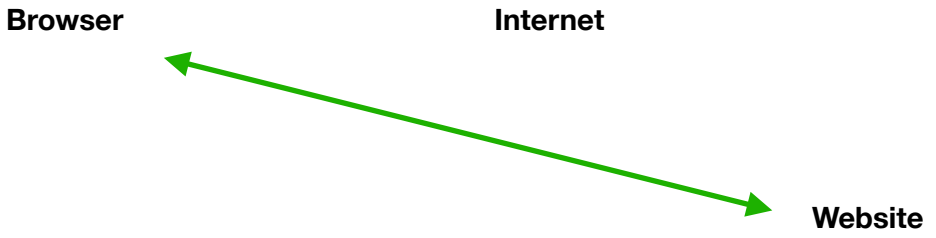


- They have the processes in place for conducting their operations, but are not always using the right tools (SRP for example)
- They decided to leave the medical sector untouched
- Every target of theirs became codified, see below picture

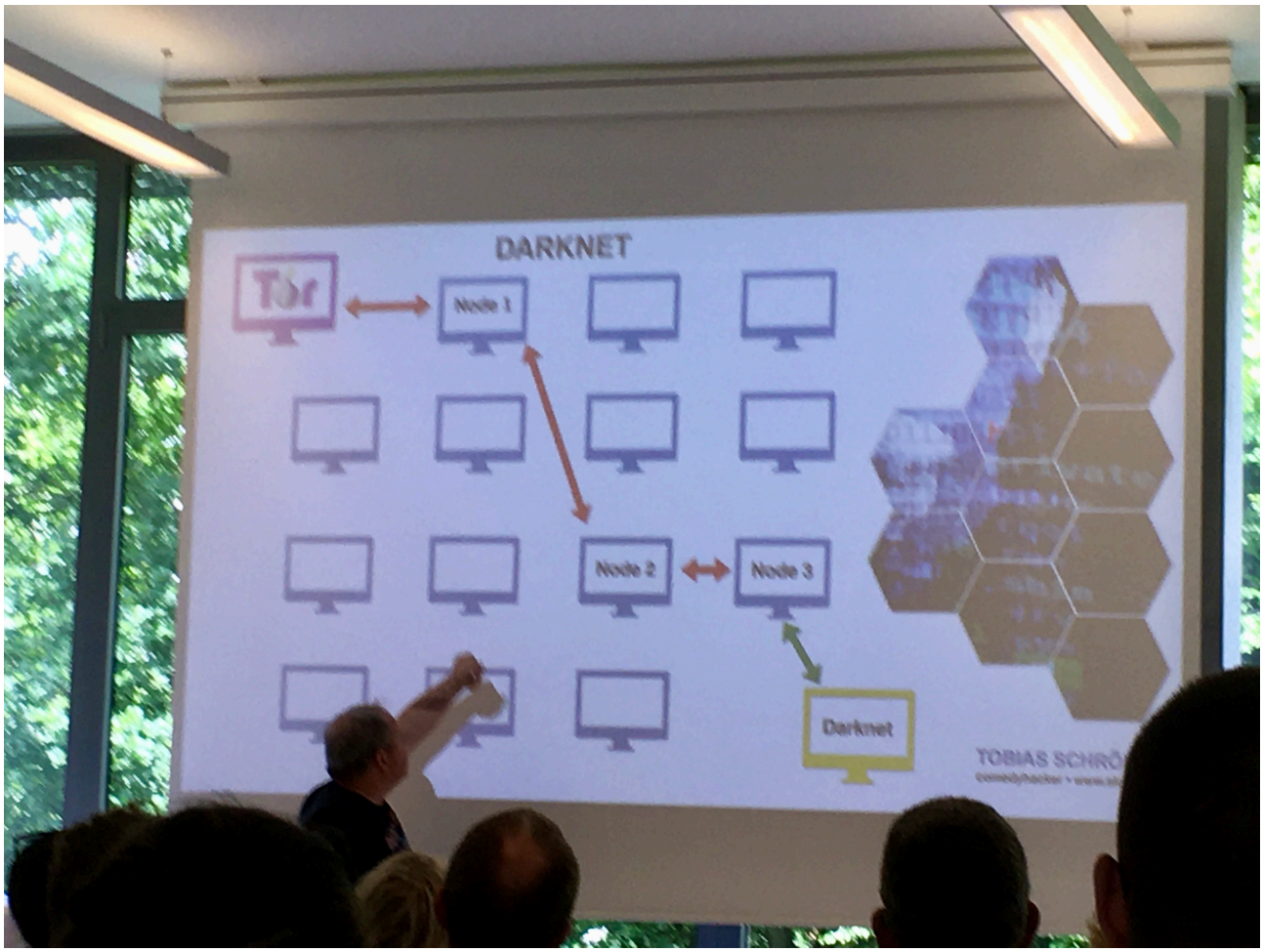


- Another Russian gang is Ragnar Locker -> Uses Schadcode
- 99% of their activities consists of things like phishing mails that seem to come from very regular companies -> E.g Siemens but with misspelling such as 'Sienens'
- For Darknet there are three things you need -> i) a TOR browser (can be found on Google for example,) ii) Criminal energy iii) The right clothing ;)

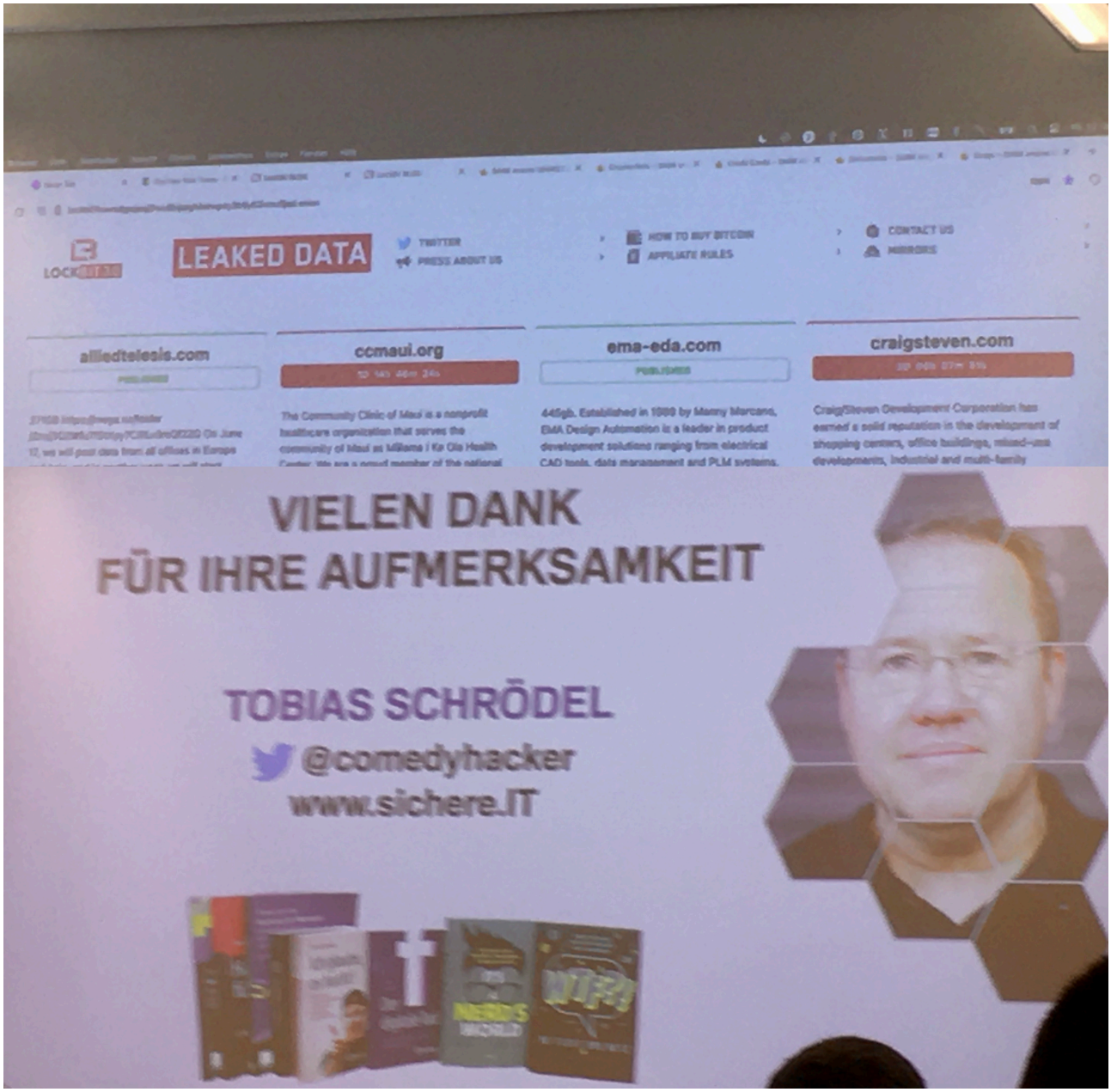
- A normal internet setup looks like this, see below:

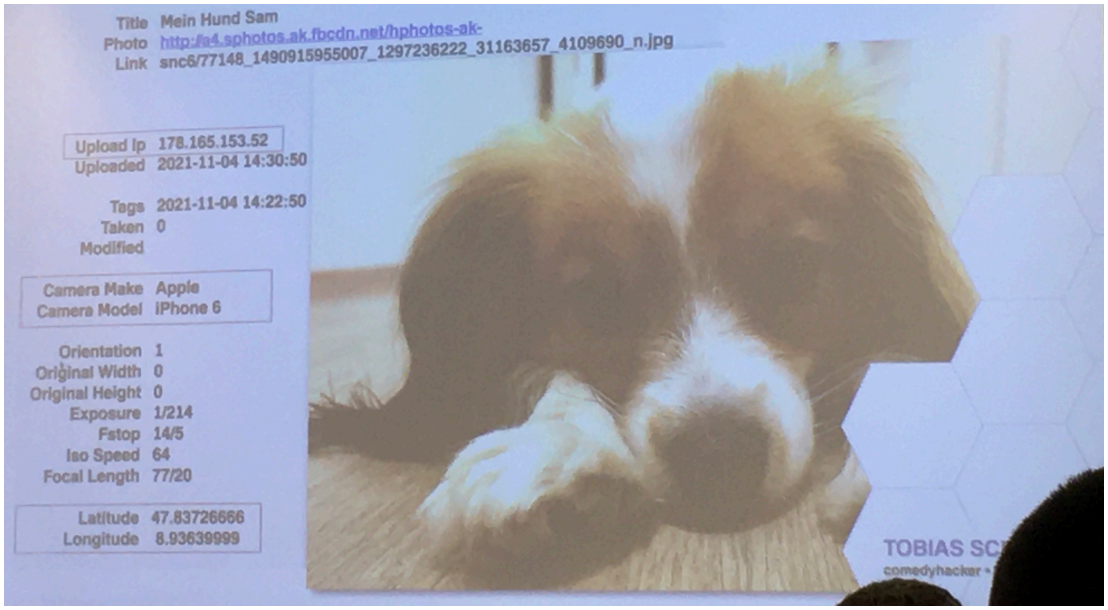


- Darknet has a different setup with more intermediaries, see below (there are a couple of vibrations in the photograph, apologies):

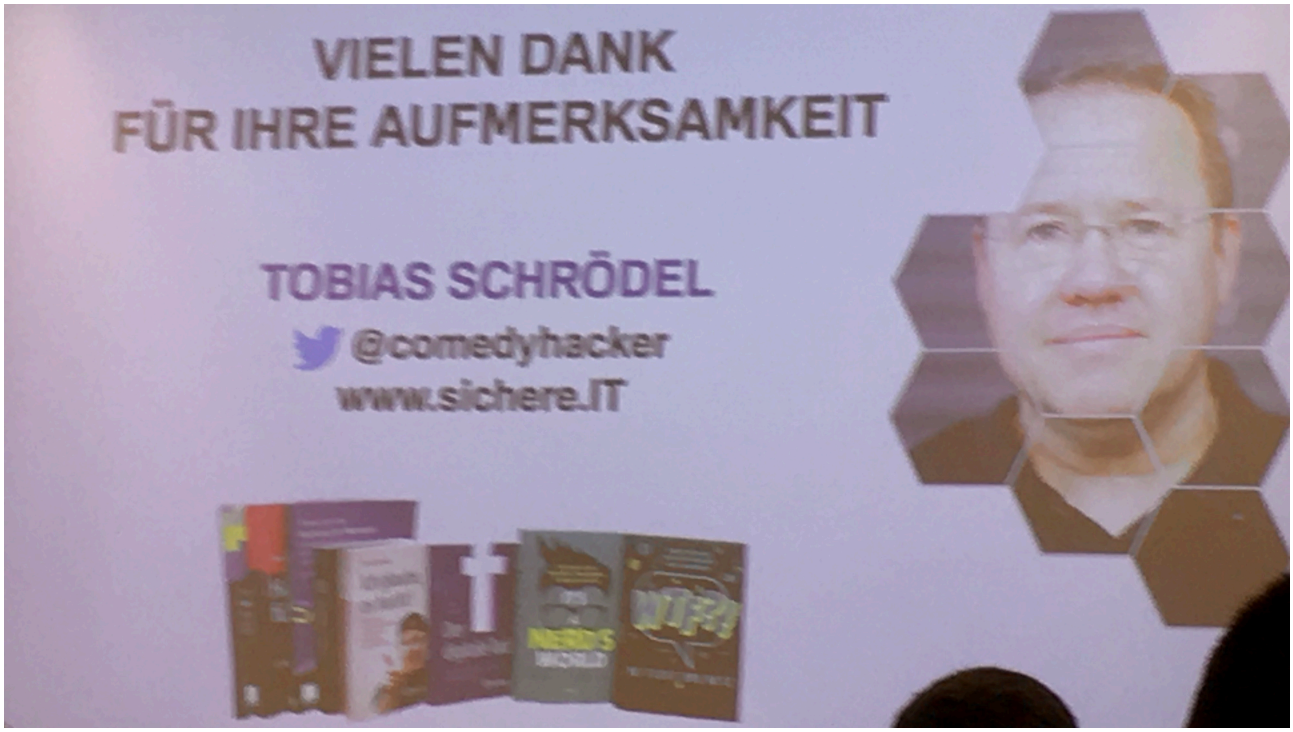


- Darknet cannot be shut down and serves legitimate purposes
- Initially it was meant for the military to send information in a secure manner, yet later on criminals joined in -> This gave Darknet a bad name and reputation
- Darknet is slower than normal internet, as queries need to pass three hubs for encryption
- There are no commercials on the Darknet
- On the next page you can find a picture with leaked data from the Darknet, displaying companies that have been victim of a ransomware attack and in some case a timer indicating how much time they have left to pay off the ransom
- A rather funny case involved a technical problem -> End encryption was not working -> So when ransom was paid, firms received back their data ánd their money :)


LEAKED DATA
TWITTER
PRESS ABOUT US
HOW TO BUY BITCOIN
AFFILIATE RULES
CONTACT US
MIRRORS
alliedtelesis.com
ccmaui.org
ema-eda.com
craigsteven.com
VIELEN DANK
FÜR IHRE AUFMERKSAMKEIT
TOBIAS SCHRÖDEL
@comedyhacker
www.sichere.IT


Title Mein Hund Sam
Photo Link http://a4.sphotos.ak.fbcdn.net/hphotos-ak-snc6/77148_1490915955007_1297236222_31163657_4109690_n.jpg
Upload Ip 178.165.153.52
Uploaded 2021-11-04 14:30:50
Tags 2021-11-04 14:22:50
Taken 0
Modified
Camera Make Apple
Camera Model iPhone 6
Orientation 1
Original Width 0
Original Height 0
Exposure 1/214
Fstop 14/5
Iso Speed 64
Focal Length 77/20
Latitude 47.83726666
Longitude 8.93639999

- So what happens when encrypted data is published? -> Company information will be thrown in the open air on internet -> Yet, hackback is a serious option to consider -> Attacked firm hacks back the cybercriminal, for example with a DDoS
- Another interesting peculiarity is pre-shredded cash, cannot be used in its existing form but when repaired it becomes usable again
- Then something else -> Metadata offers a valuable source of information -> Every picture posted on social media has it and includes things such as date, device, phone number, location, geographical coordinates
- We can also derive this data -> For example, Google Earth can be used to derive the location of a picture based on the metadata description of the geographical coordinates
- That way, a picture of a dog can identify an entire user profile, preferences, way of life, work, hobbies, family
- Spotify can derive with high accuracy when a woman is in her period -> During that time, her playlists change
- Likewise, Uber can derive from travel data which partners cheat on their wives -> Recurring short distance travels to nearby destinations is such a way of estimation
- Silicon Valley has an extremely high number of psychologists and sociologists for market research
- Other useful fact -> You can call anyone from any number if you do it right -> Use Voice Cloning for example
- This led to a case of a Deepfake, which is a serious problem -> In one case, four financial CEOs from Hong Kong have been extorted for €23 million -> Voice cloning plus the usage of a picture to paste it over someone's face at a videocall made this possible -> So be careful



On a final note
The conference offered a clear yet extensive lists of cyber risks to watch out for from a firm's perspective, and captures this serious challenges well. As apparent, there is a serious rat-race within this field between legitimate versus illegitimate parts of the economy, and it has become increasingly clear that we should buckle up. Thank you for reading! For feedback or comments, please send an E-mail to quero@discounted-by-a-lightning-strike.com.

I have no interests to declare other than my attendance as a board member of investment committee Carpe Divitias.