IPMA GLOBAL **BEST PRACTICE WEEK**

VIRTUAL EVENT

Cyber Threats –
A peek behind the headlines

28.10.2020

IPMA

About me

Bruno Blumenthal

Dipl. Ing. FH in Computer Sciences, CISM, CISA, CISSP

- Expert Security Consultant at TEMET AG, Switzerland
- Working in IT & Cyber Security since 2004

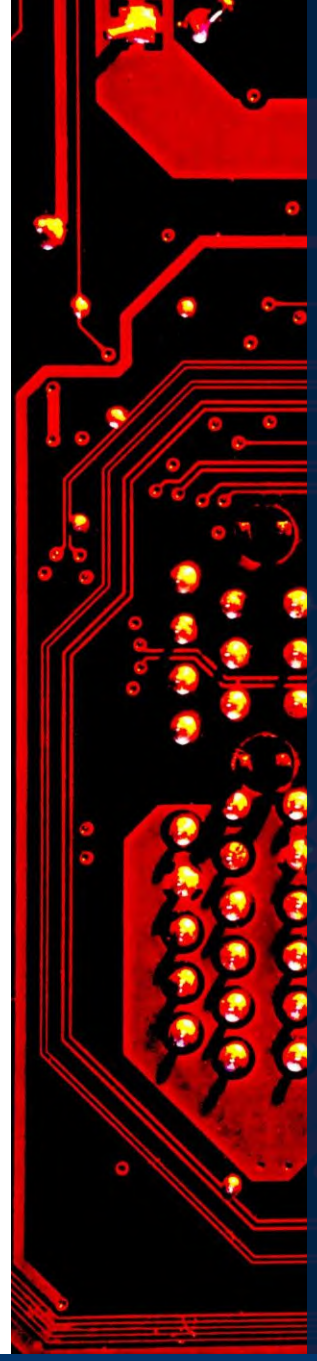
Specialties:

- Information Security Management
- Security Architecture and Strategy
- Risk Management

Contact:

- Mobile: +41 78 859 57 15
- E-Mail: bruno.blumenthal@temet.ch

Agenda



1. 1989 - A first headline
2. Some recent big headlines
3. Another kind of pandemic
4. Recap

1989 – A first headline

March 2nd 1989

The police raids an apartment in northern Germany.

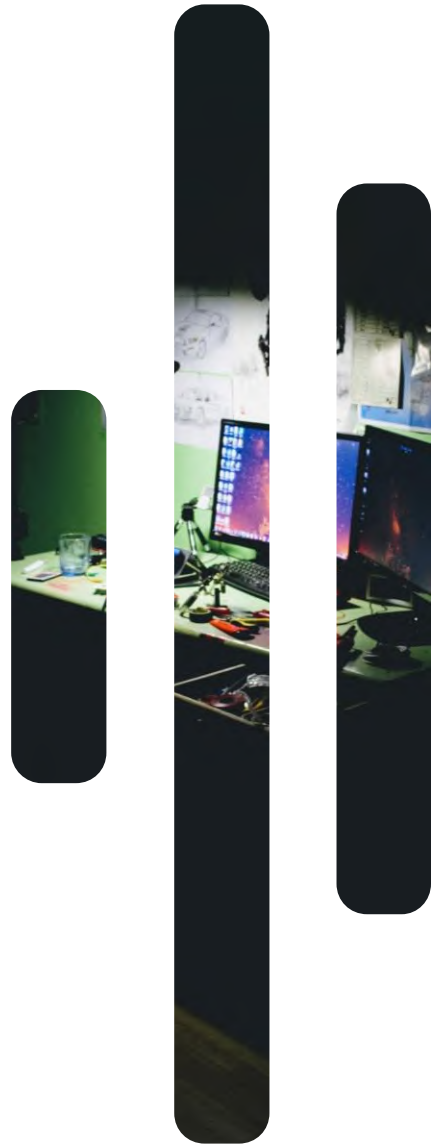
It is the moment the public first learns about events the will eventually became known as

The KGB Hack

The KGB Hack

- The first widely publicized case of a state affiliated cyber attack
- The target were military and scientific institutions but also commercial technology companies in the west
- It was as much political espionage as it was industrial espionage
- It was young German hackers acting on behalf of the KGB
- They did it for money and drugs, not ideologies
- 75 missing cents and a file named SDInet.doc led to their capture

- This case is in many regards still a blueprint for modern day cyber attacks and cyber defense



The anatomy of the KGB Hack

Offense

- It wasn’t a one off attack, but a very persistent and patient operation
- They didn’t attack directly, but moved laterally
- It was a nation state attacking, but the targets were also civilian
- The hackers were not yet professionals, but none the less for hire

Defense

- Coincidence and a curious individual started the hunt
- Logs and decoys helped catch em, but first they had to be produced and created
- The hunt was international and law enforcement was not prepared

Some recent big headlines

The Bangladesh Bank Heist

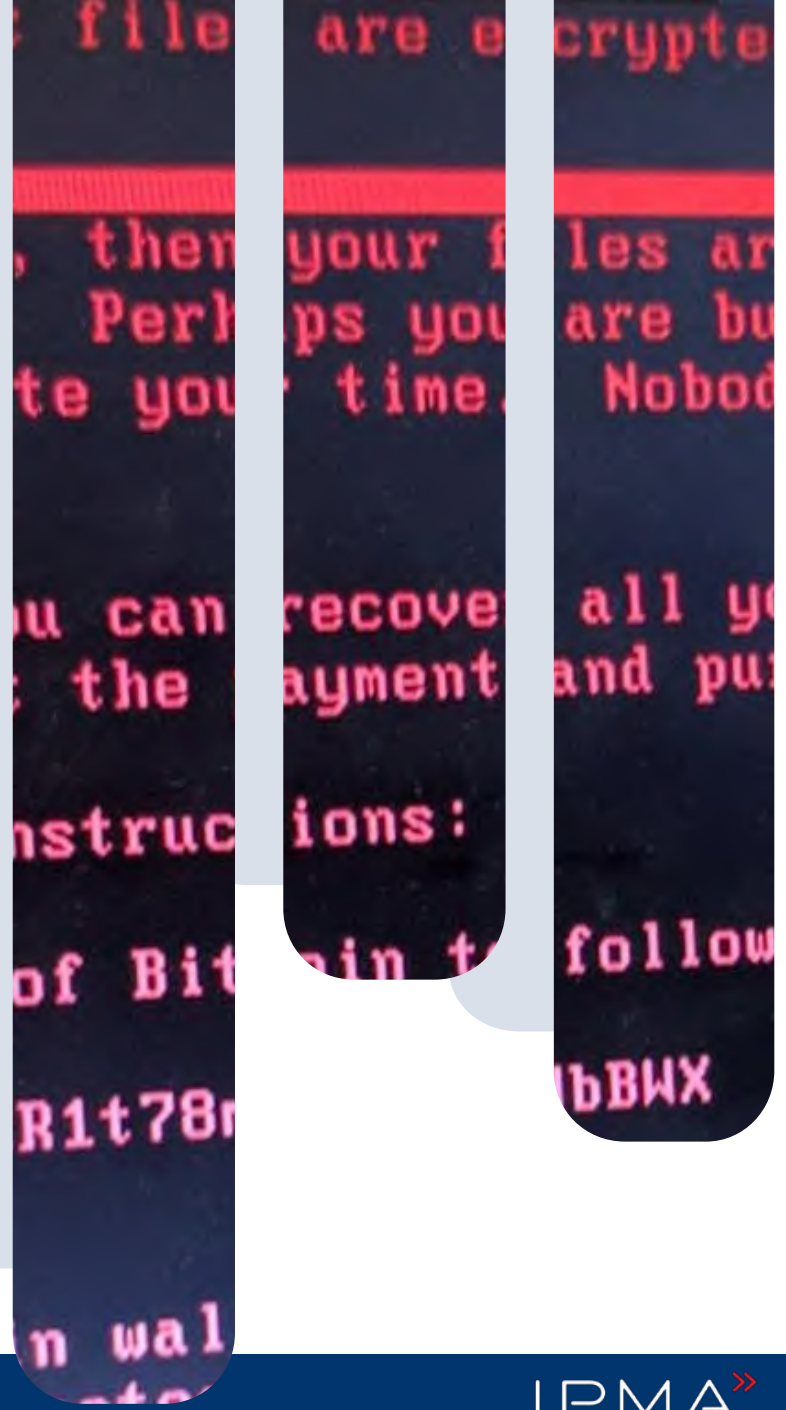
- It was early 2016 and North Korea needed money
- Why not rob a bank?
- They tried it, the 21th century style
- And aimed for 1 Billion US$
- It took month of planning failed partly because of a typo
- But they still managed to get away with ~80 mio US$

How to digitally rob a bank

- Find an account with sufficient balance, like the account of the bank itself at the federal reserve
- Take over the machine where legitimate SWIFT transacation are created
- Prepare accounts to deposit the looted money
- Disable the physical audit log printer
- Wait for a long holiday weekend
- Mimic the normal behaviour of employees
- Launder the money through a high roller casino

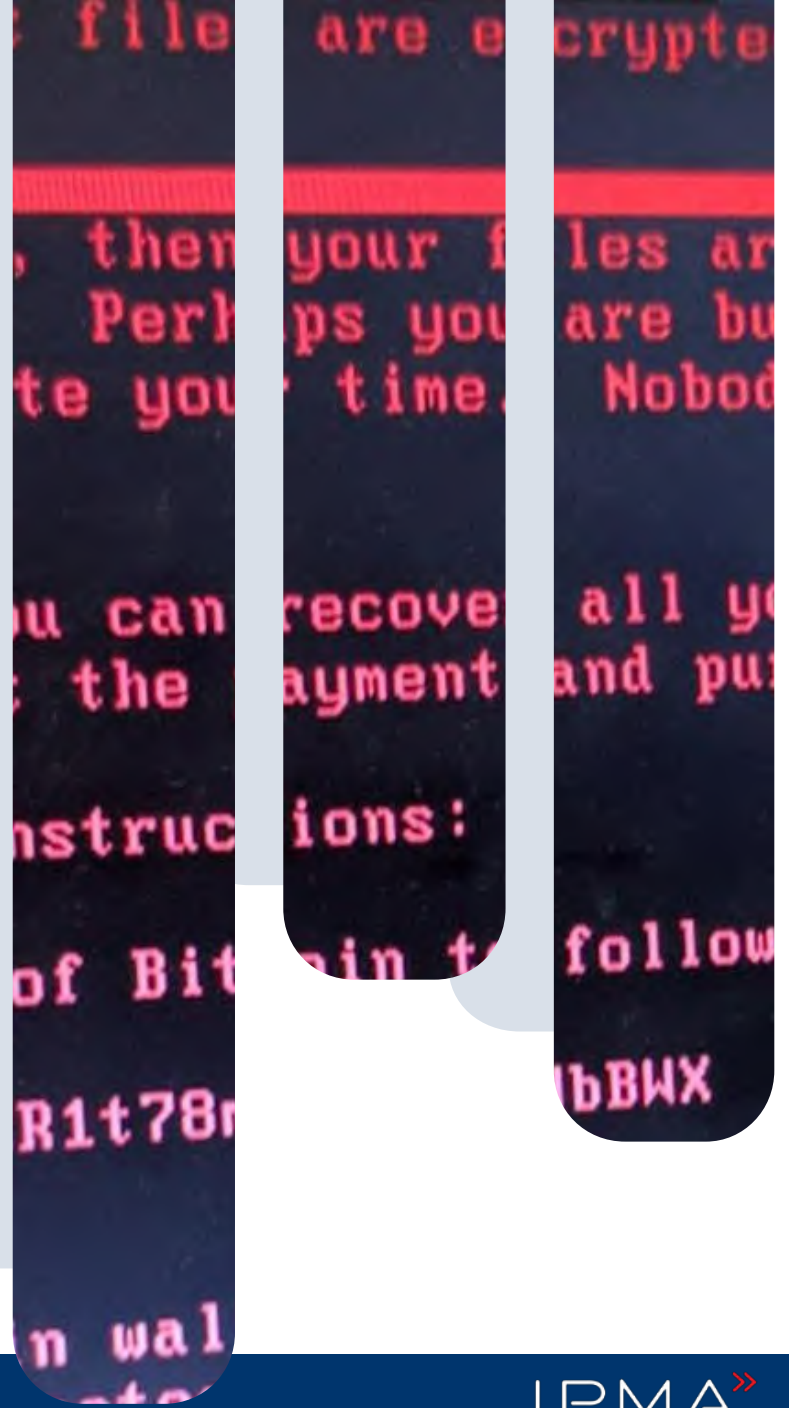
NotPetya

- Summer 2017 Russia is at war with the Ukraine
- Russia already used means of cyber attack in the conflict
- They decides to directly target Ukraines economy
- They targeted broad, maybe too broad
- In the end we saw worldwide collateral damage
- Several billion US$ in economic damage worldwide
- Who got affected was uncontrollable by the attacker



How to cripple an economy

- Find a software ubiquitous in the target economy, like a tax reporting software
- Hack the software vendors network
- Insert a backdoor into the software update capability
- Push your attack software through the update mechanism
- Let your malware spread
- Destroy the data of the victims



Olympic Destroyer

- February 2018 opening ceremony of the olympic winter games
- In the datacenter of a contractor computers start to fail
- The official App stops working and the Active Domain DC’s go offline
- After initial cleanups the compromise repeats itself over and over again
- The well trained incident response plan prevents the worst case
- But who is behind the attack, what was the goal?
- It’s false flags all the way down, sort of

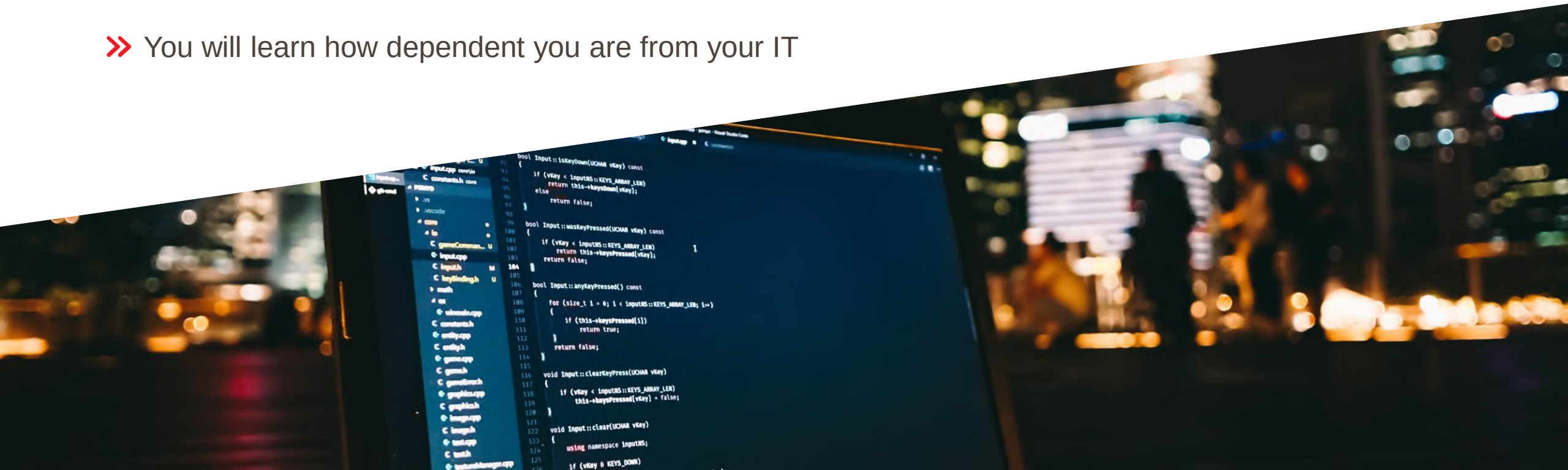
How to mess with attribution

- Think of a likely attacker
- Consider possible wrong leads
- Study your scapegoat's modus operandi and tools
- Integrate their code snippets into your tools
- Change metadata and other info embedded in the attack tools
- Don’t falsify too many flags, unless confusion is your goal

Another kind of pandemic

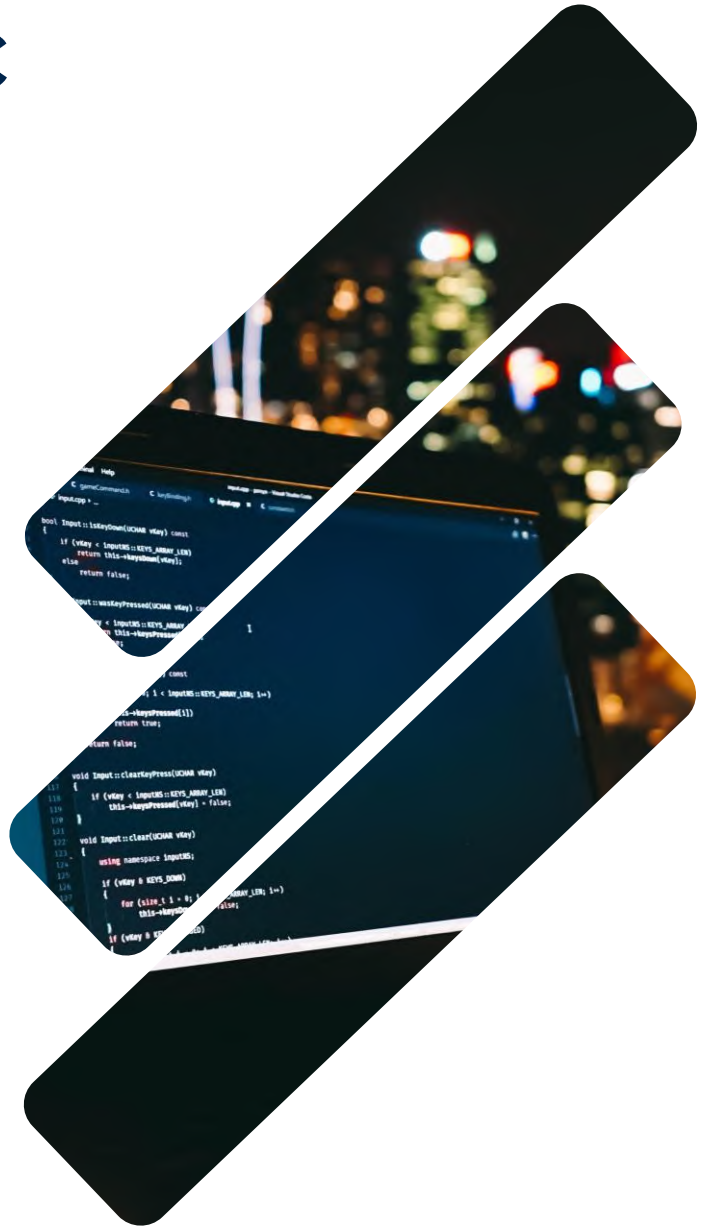
Holding your data for ransom

- Ransomware encrypts your data and systems
- You have to pay a ransom to get it back
- It can bring your business to a complete halt
- You will learn how dependent you are from your IT



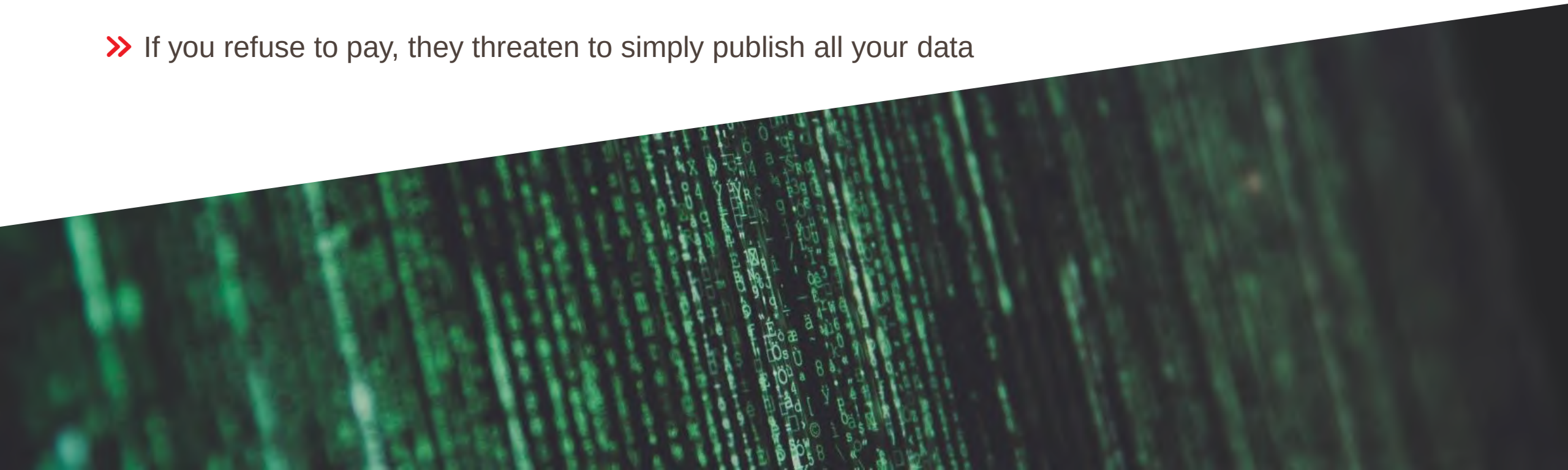
How it became a pandemic

- Ransomware, is the most ubiquitous kind of attack at the moment
- It is so pervasive I didn’t want to mention just one headline
- It’s not new, the first known case happened in 1989
- The first ransomware was called AIDS or PC Cyborg Trojan
- As always with ransom, the money exchange was difficult
- Then Bitcoin came along and changed the game
- Ransomware became the main method to generate money



The evolution of ransomware

- It started focused mainly on individuals, but have moved now to target enterprises
- Companies and public authorities of all sizes are victims
- First the encrypted right away, now the first compromise your whole infrastructure
- If you refuse to pay, they threaten to simply publish all your data



How they get in

- Phishing – broadband and targeted
- The move to the enterprise changed tactics
- RDP became the number one attack vector for
- Combined with Phishing or password stuffing
- But also Software Vulnerabilities
- It’s not just RDP it’s also VPN
- If you don’t want to hack, just buy the access in a RDP Shop

Should I pay?

- No.

- It fuels the problem
- It can make you more susceptible to repeated attacks
- It can even be illegal

Recap

What we learned

- Indirect attacks
- Preparation and long lead times
- Attribution is difficult
- Collateral damage
- Attackers adapt their tactics
- It’s not always about secrets
- Everybody can be a target

- Not all is new in the cybers

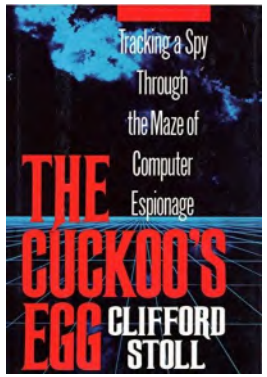
Interesting reads and listens

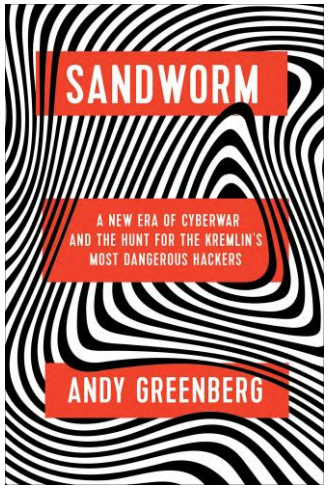
Books:

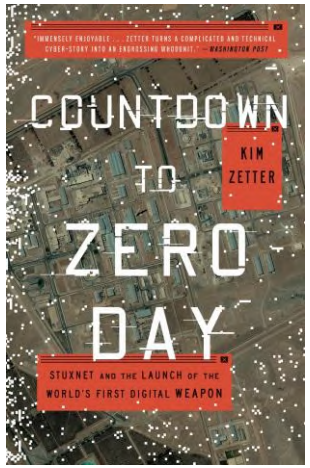
- The Cuckoo’s Egg by Clifford Stoll
- The Hacker and the State by Ben Buchanan
- Sandworm by Andy Greenberg
- Countdown to Zero Day by Kim Zetter

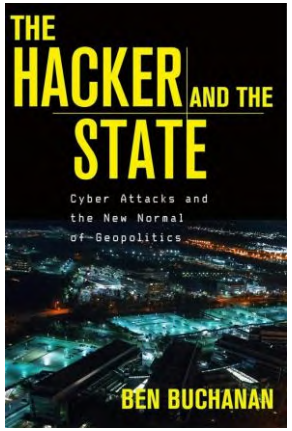
Podcast:

- Darknet Diaries from Jack Rhysider









IPMA

international
project
management
association

IPMA GLOBAL
BEST PRACTICE WEEK

VIRTUAL EVENT

TEMET
end-to-end IT security