

Cyberangriffe gegen Unternehmen

Attacken, Hintermänner, Gegenmaßnahmen

Bernhard Patsch, Barracuda Networks
Peter Stelzhammer, AV-Comparatives





Auditing / Certifying of IT Security Solutions



Barracuda Networks



Networks



Data

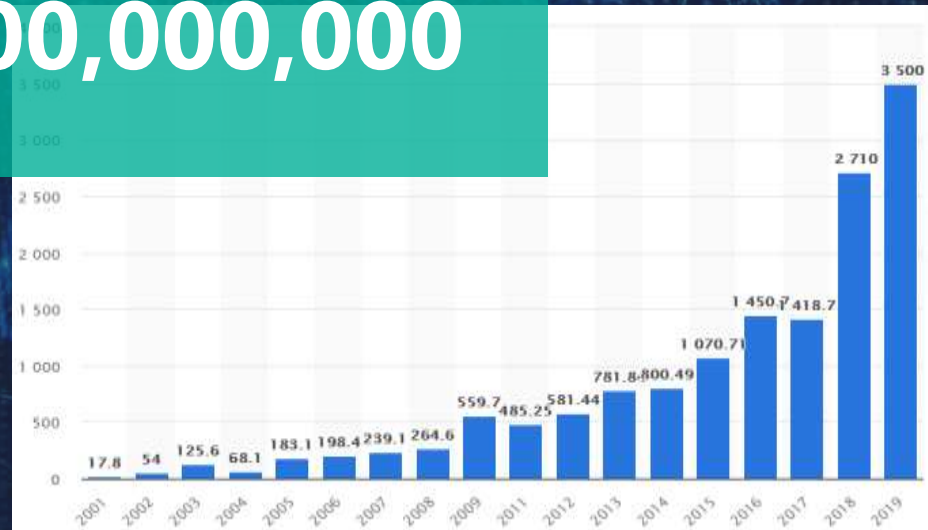


Application

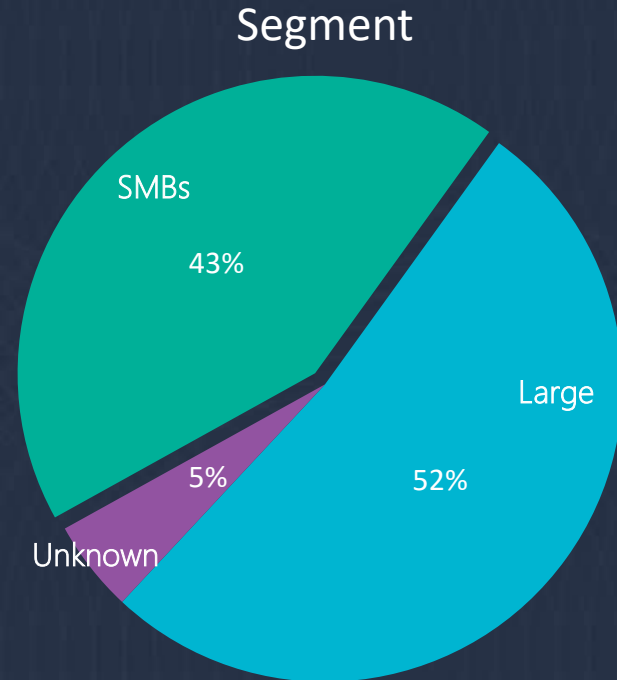
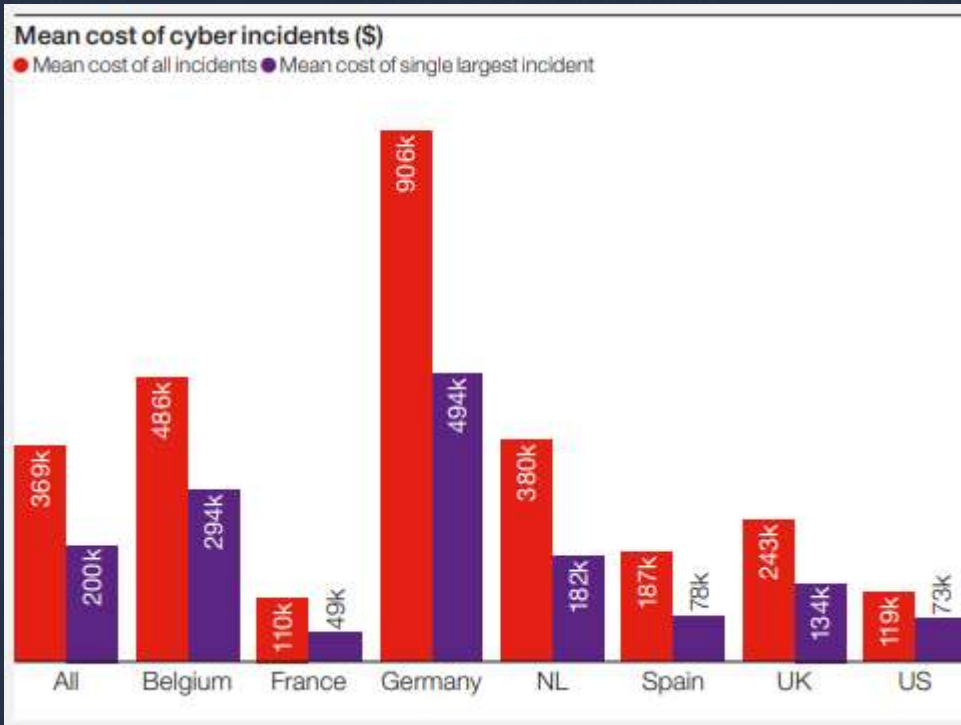


Strictly confidential, no photos, no recording

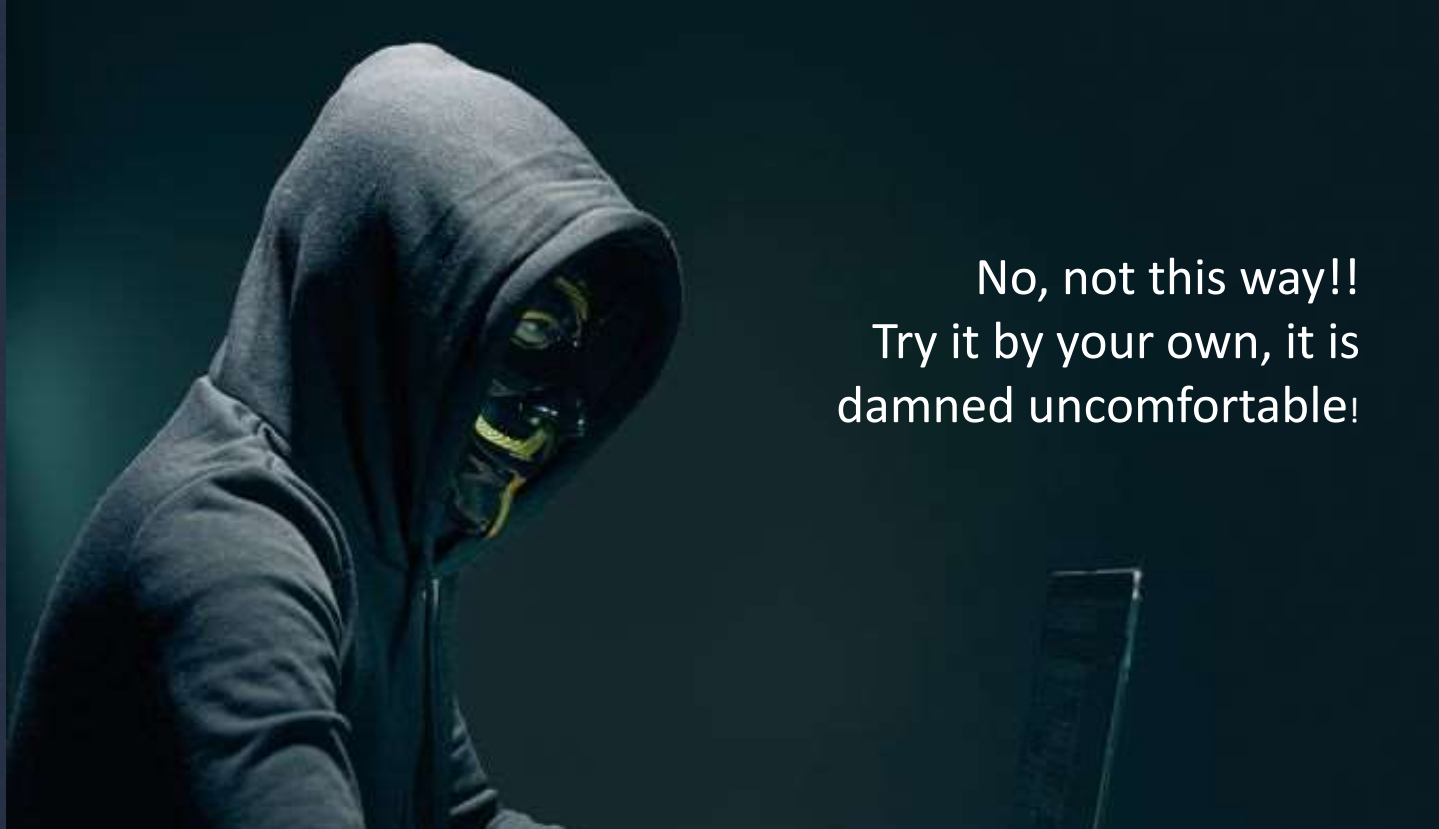
\$ 3,500,000,000,000











No, not this way!!
Try it by your own, it is
damned uncomfortable!

How does a hacker look like?





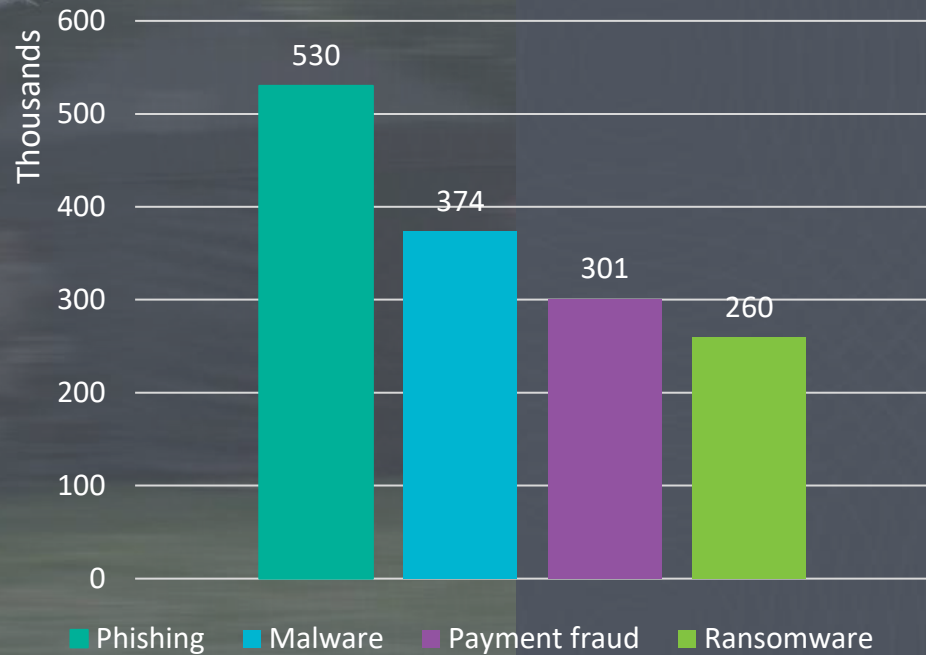
**CyberCrime is not only violence in the cloud
It is also physical violence**



Threats



Top Threats



Phishing

Gesendet: Montag, 29. Juni 2020 um 11:11 Uhr
Von: "Bank Austria - UniCredit..." <rezqkqlz@beacker.de>
Betreff: PostBox : IT Service ID : MKA4XN



Sehr geehrter Kunde,

Wir informieren Sie, dass wir Probleme in unserer Datenbank haben.
So überprüfen Sie Ihre Telefonnummer,
Klicken Sie auf "Login" und Sie erhalten eine Benachrichtigung mit Ihren

<https://banking.bankaustria.at/wps/portal/retail/de/login/login>

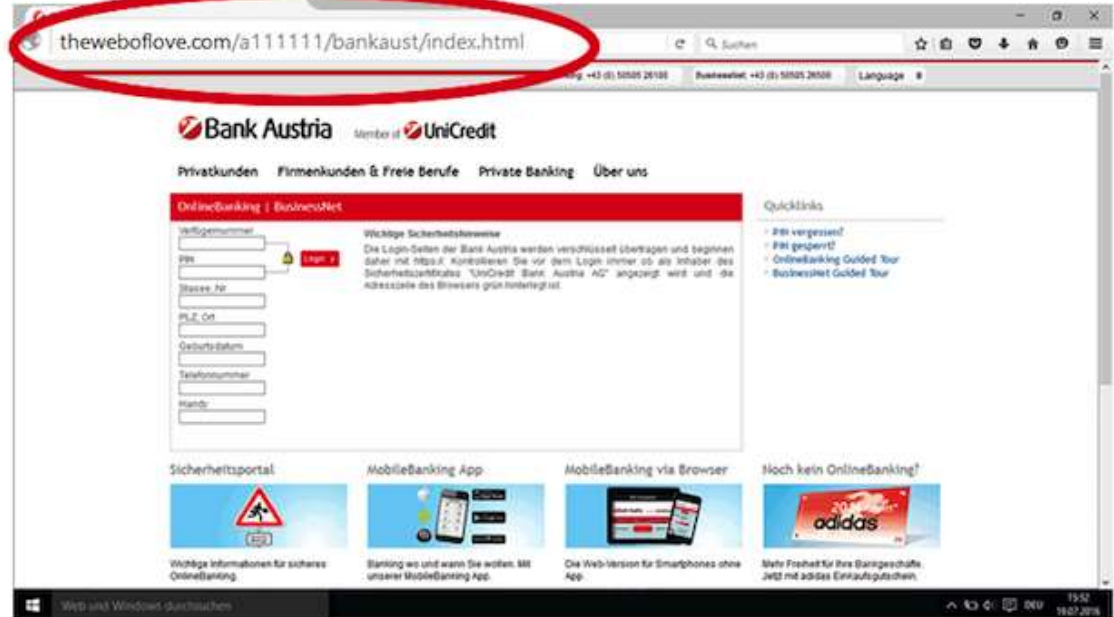
Vielen Dank für Ihre Aufmerksamkeit

Freundliche Grüße.

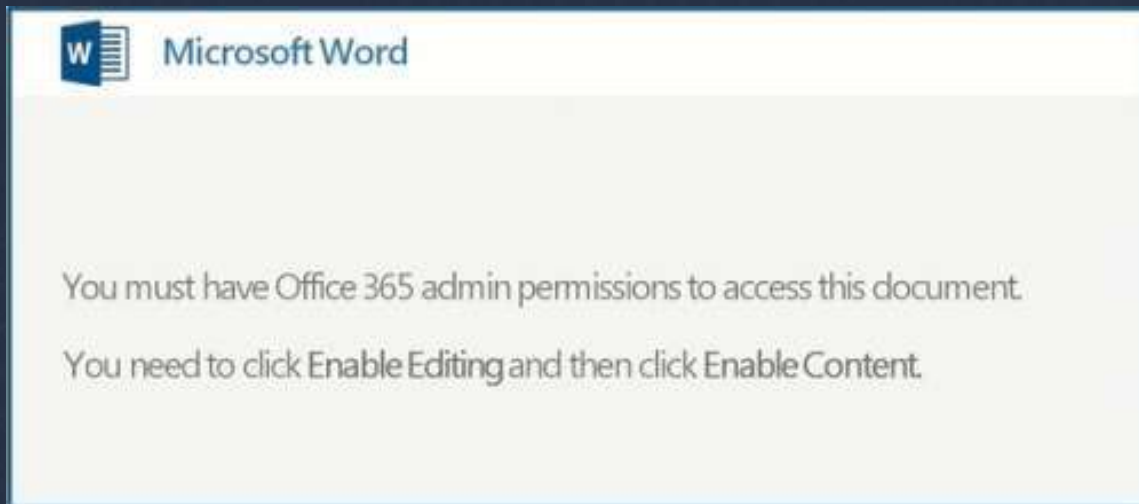
Ihr ElectronicBanking-Team
UniCredit Bank Austria AG

<http://www.bankaustria.at>

<https://mobile.bankaustria.at>



Phishing





CEO - FRAUD

Yes, it works - in Innsbruck as well as international!

HOW CEO FRAUD IMPACTS YOU

THE START

Attackers see if they can spoof your domain and impersonate the CEO (or other important people)



Bad guys often troll companies for months to gather the data necessary in pulling off a successful attack

THE PHISH

Spoofed emails are sent to high-risk employees in the organization

●●● To: Finance Department
Urgent wire transfer request!
Please send \$100,000 to new acct #987654-3210.

●●● To: CFO
Please pay this time-sensitive invoice. I'm on vacation and will be unavailable, no need to respond. - Your CEO

●●● To: Human Resources
I need a PDF copy of ALL employee W-2s for the IRS ASAP!

THE RESPONSE

Target receives email and acts without reflection or questioning the source



I better get this payment to the new account!



It's from the CEO, I'll take care of this for him!



Sounds important, I'll send these right away!

THE DAMAGE

Social engineering was successful, giving hackers access to what they were after

Causing fraudulent wire transfers and massive data breaches




THE RESULT

The fallout after a successful attack can be highly damaging for both the company and its employees


Resulting damage:

- ✓ Money is gone forever in most cases and only recovered 4% of the time
- ✓ CEO is fired
- ✓ CFO is fired
- ✓ Lawsuits are filed
- ✓ Intangibles - tarnished reputation, loss of trust, etc.

So... Think Before You Click!



jdoe@so1idxyz.com
jdoe@solidxyz.com



jdoe@so1idxyz.com
jdoe@solidxyz.com

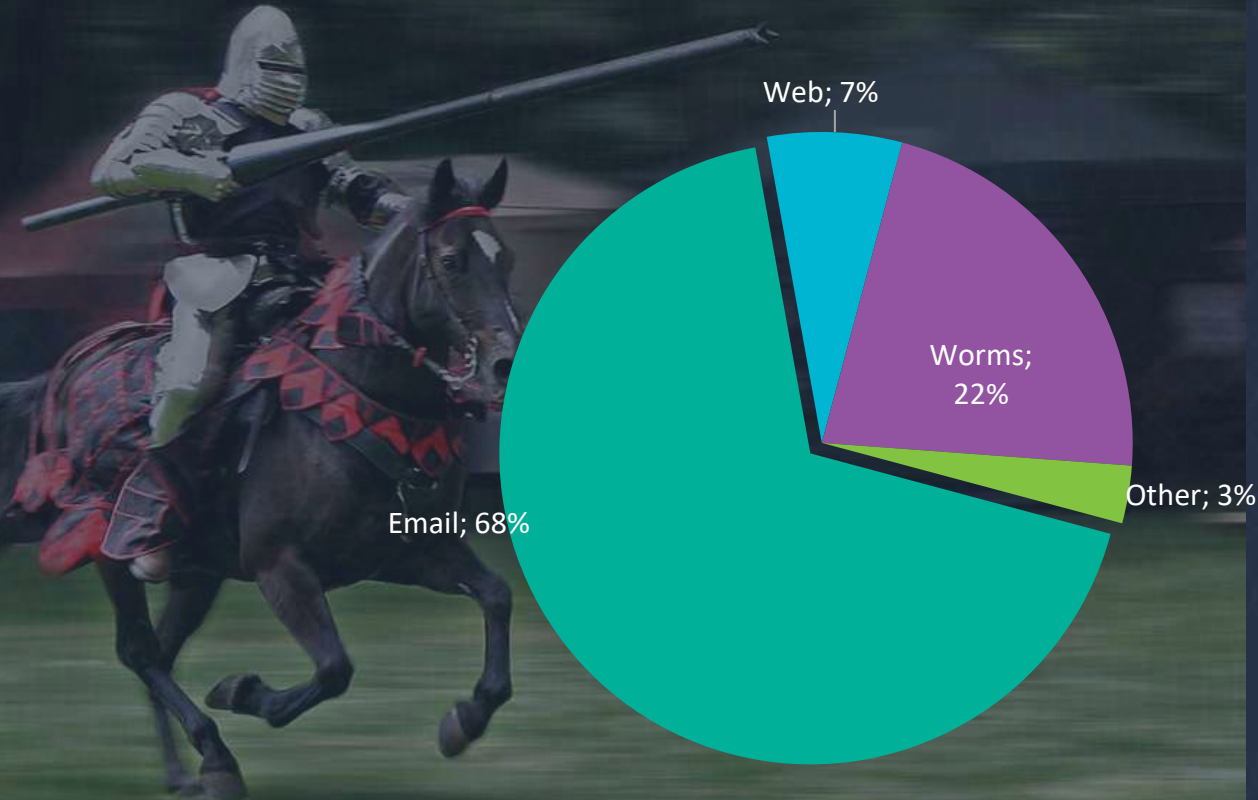
jdoe@so1idxyz.com
jdoe@solidxyz.com



It may seem too obvious, but Ubiquiti Networks lost a total of \$46,700,000 due this exact method.

<https://www.nbcnews.com/tech/security/ubiquiti-networks-says-it-was-victim-47-million-cyber-scam-n406201>

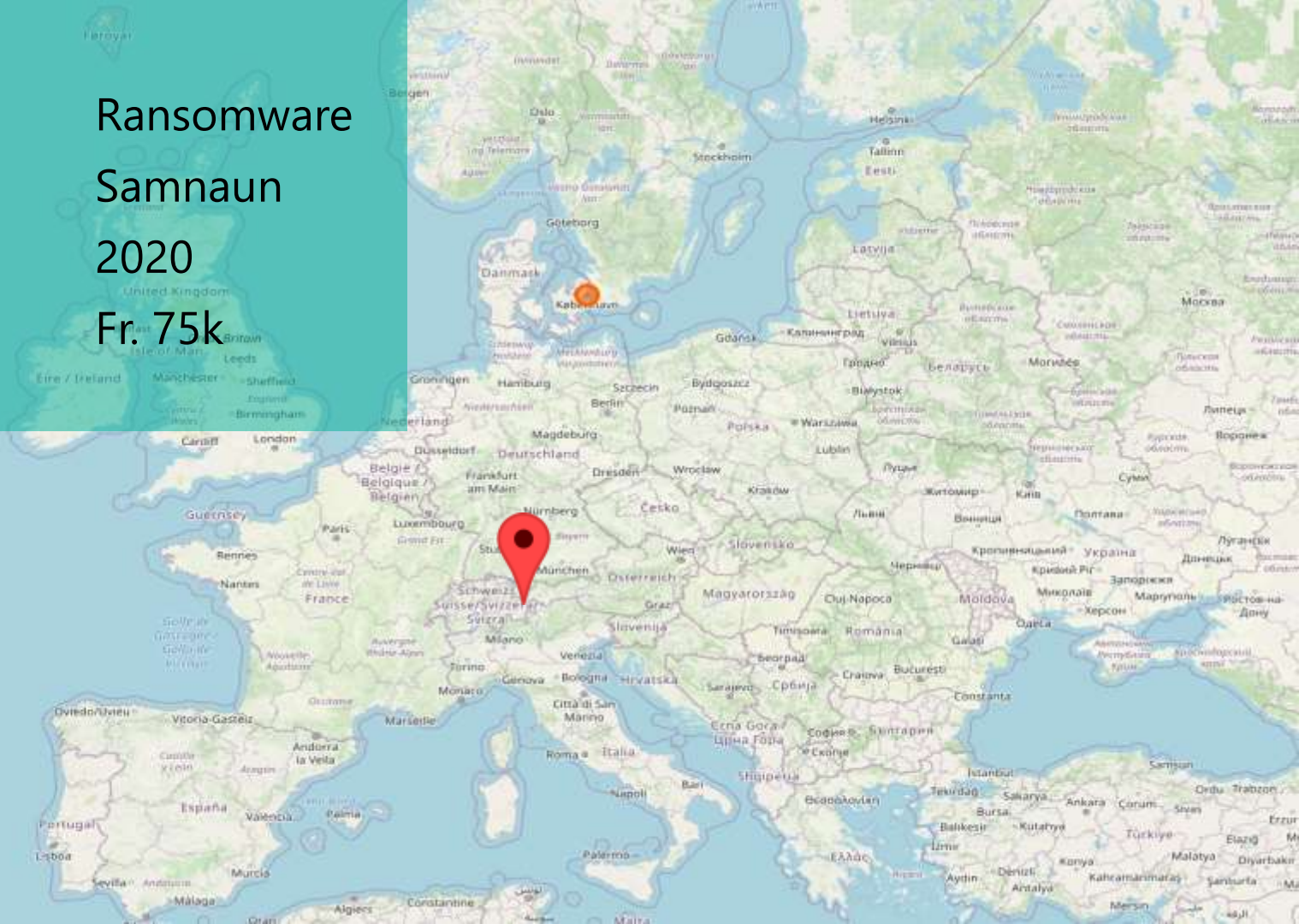
Attack vectors



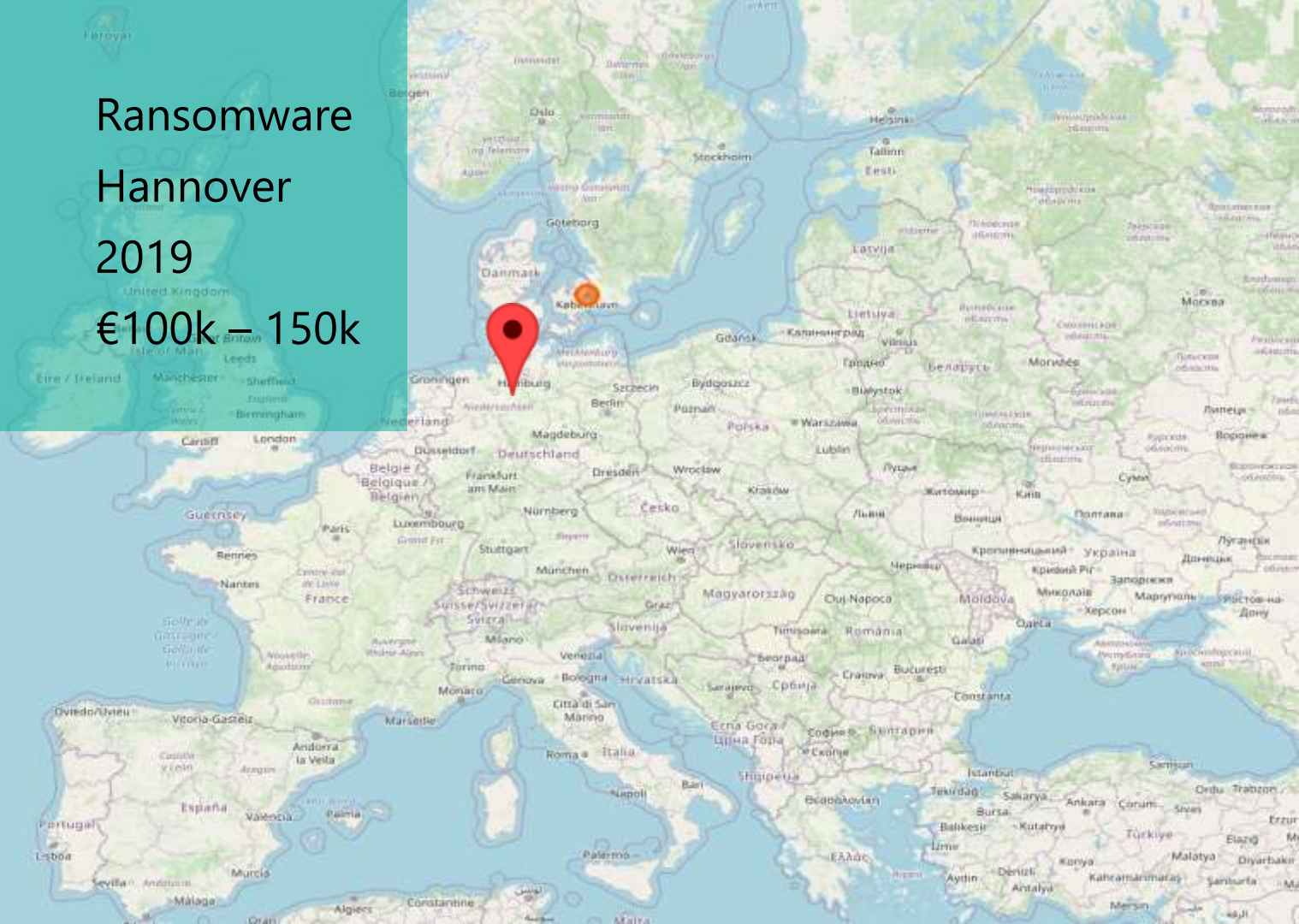
Further risks

Untrusted applications
Browser extensions
USB pen drives
Messenger/Chat
IoT devices

Type: Ransomware
Location: Samnaun
When: 2020
Cost: Fr. 75k



Type: Ransomware
Location: Hannover
When: 2019
Cost: €100k – 150k

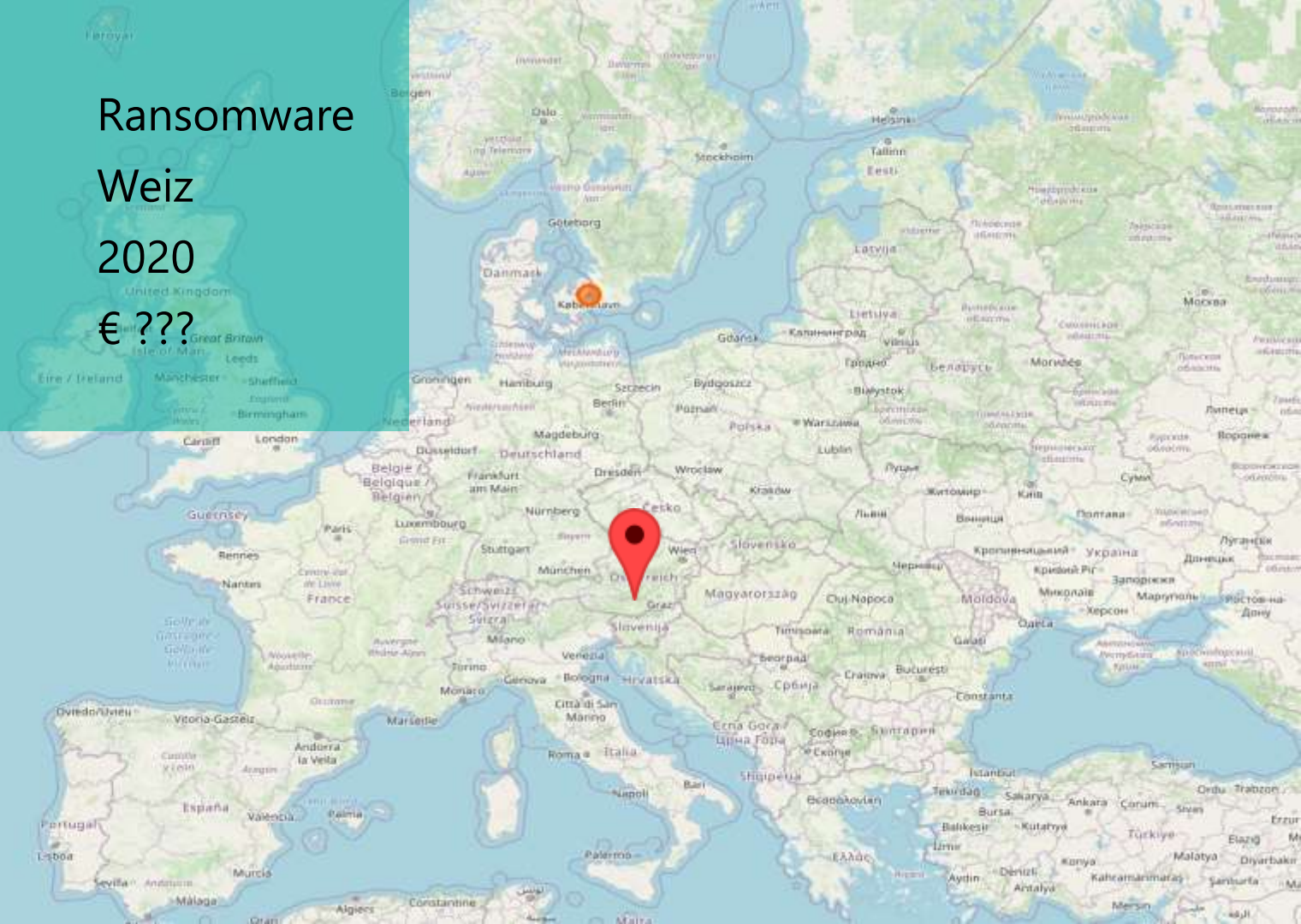


Type: Ransomware

Location: Weiz

When: 2020

Cost: € ???



How to protect

Prepare for attacks

Consult experts

Employee education

Implement several layers of defense

Monitor & detect



Technical measures

Apply updates

Use Virus Scanner

Use different passwords for different accounts

Multi-factor authentication

Backup (3 – 2 – 1, offline!)

Least privilege, separation of duties

Network segmentation



Contact

bpatsch@barracuda.com

contact@av-comparatives.org



Thank You

