









1

Hvem er jeg..



Keld Norman
kno@dubex.dk














Dubex:
(OO A/S)

Dubex:

Dubex:

Familie firma

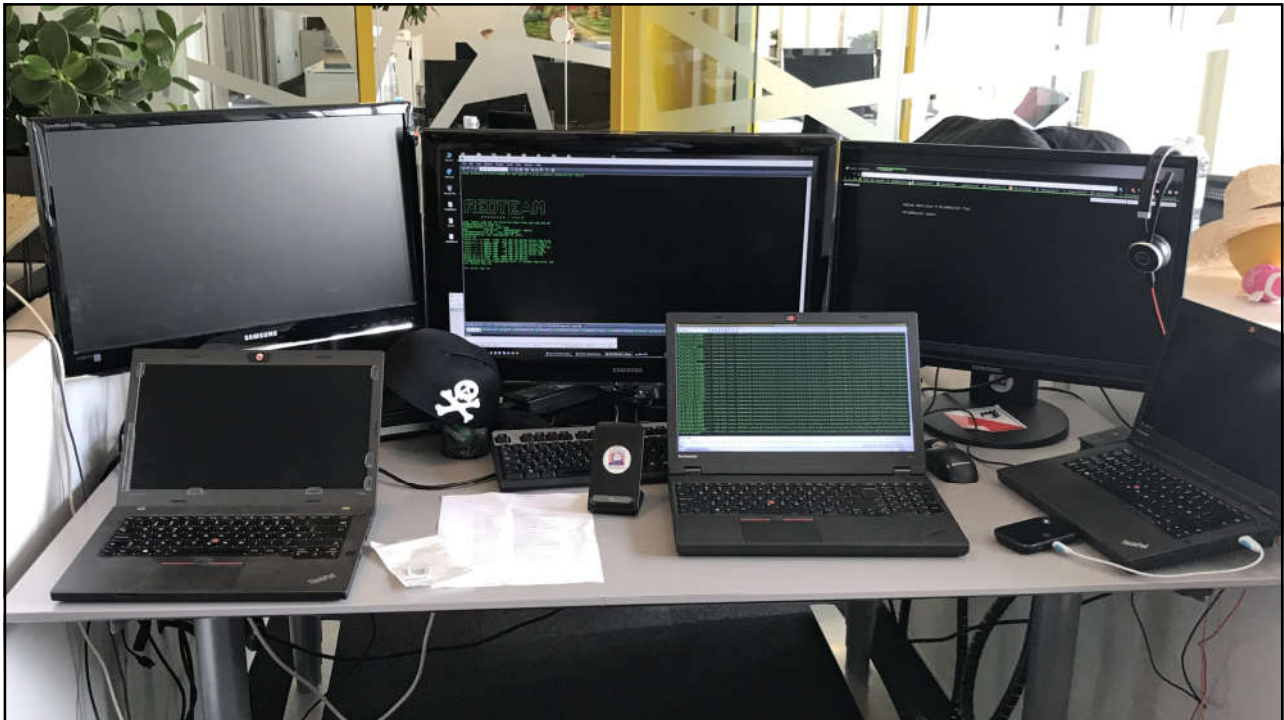


Dubex
Incident
Response
Team

2



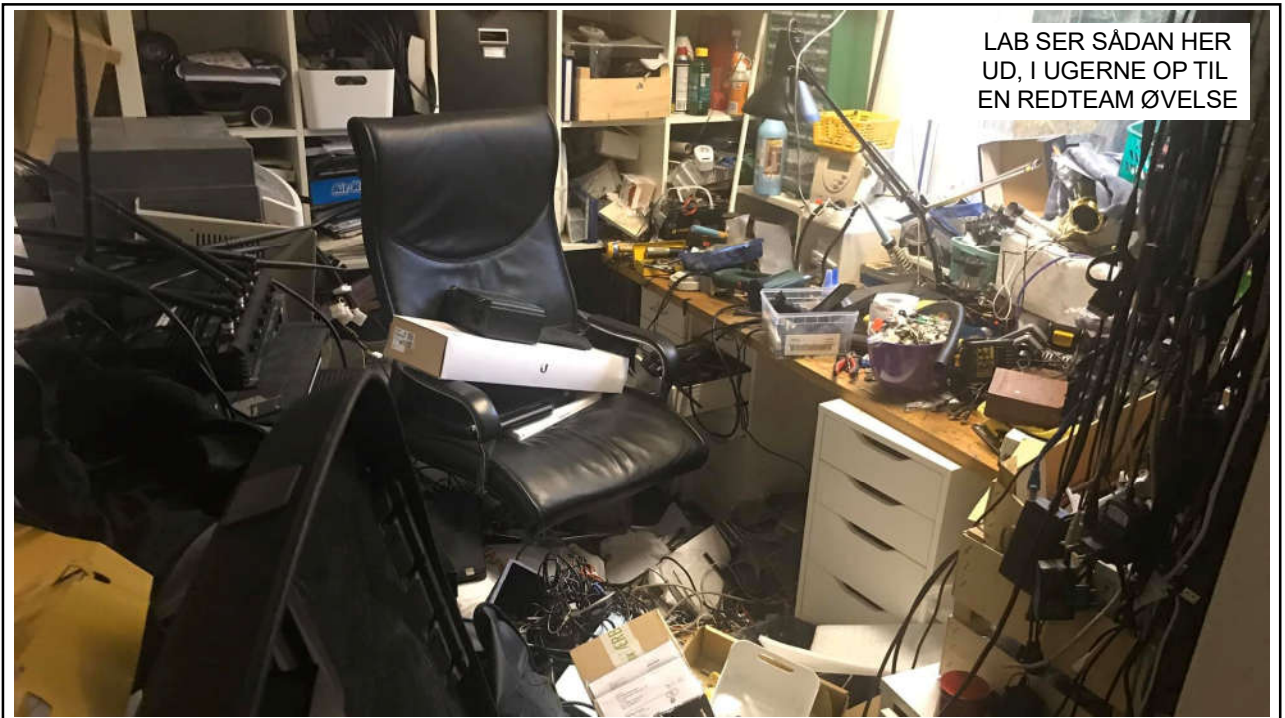
3



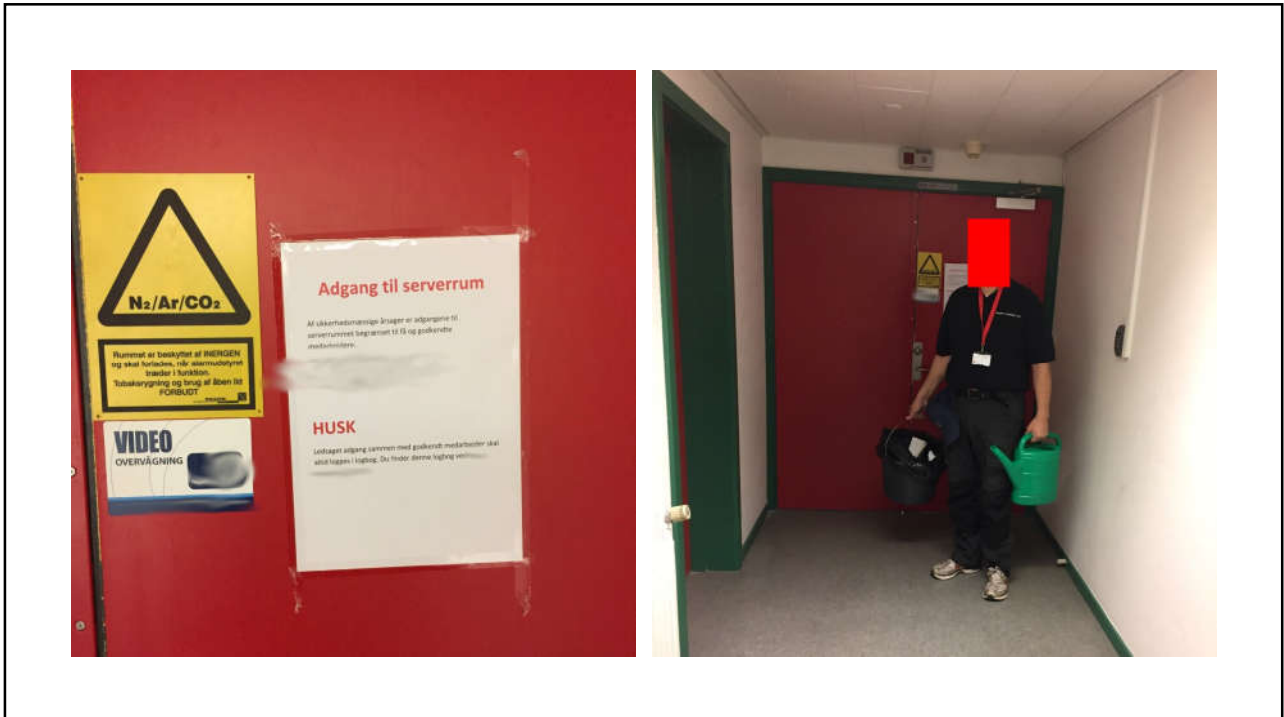
4



5



6



7



8

Ajax Security Team (Group 26, Saffron Rose) Flying **Kitten** Al Qassam Cyber Fighters Andariel APT4 Samurai **Panda**
 APT12 IXESHE (DNSCalc, DynCalc, Numbered **Panda**) APT1 Comment Crew (Comment **Panda**, PLA Unit 61398, TG-8223)
 APT10 Stone **Panda** (CVNX, MenuPass, POTASSIUM, Red Apollo) APT17 Deputy **Dog** (Aurora **Panda**, Hidden Lynx, Tailgater Team)
 BuhTrap APT19 Deep **Panda** (Black Vine, KungFu **Kittens**, Pink**Panther**, Shell Crew) Codoso / Sunshock / Sunshop Group
 APT28 APT15 Vixen **Panda** (GREF, Ke3Chang, Mirage, Playful **Dragon**) **Dragon** OK Charming **Kitten** (Group 83)
 APT18 Wekby (Dynamite **Panda**, TG-0416) Fancy **Bear** (Iron Twilight, Pawn Storm, Sednit, Sofacy, Strontium, Tsar Team)
 Bureau 121 APT29 The Dukes (Cozer, Cozy **Bear**, Cozy Duke, CozyCar, EuroAPT, Office **Monkeys**, Rus2) Byzantine Hades
 APT30 APT33 **Animal Farm** APT Threat ActorsTrend Axiom Hacking Group (Barium, Wicked **Spider**, Winnti Group)
 BLACKGEAR Lazarus Group Carbanak (Anunak, Carbon **Spider**) APT3 UPS (Gothic **Panda**, TG-0110) Conference Crew
 Danti Bronze Butler Darkhotel Chafer Elderwolf (Beijing Group, Sneaky **Panda**) Equation Group
 Energetic Bear (Berserk Bear, Crouching Yeti, **Dragonfly**, Dragonfly, Group 20, Group 24, **Koala** Team) FIN4 Five Eyes FruityArmor
 Gaza Hacker Team (**Molerats**) General Directorate for Electronic Security Government Communications Security Bureau
 Group5 Hellsing Goblin **Panda** (Cycldek) HIDDEN COATIS Hurricane **Panda** Bluenoroff Moafee
 Moonlight Maze National Security Agency National Electronic Security Authority Neodymium No. 91 Office (NK)
 Pacifier APT Patchwork – Dropping **Elephant** (Monsoon APT, Operation Hangover) Promethium Roaming **Tiger**
 Rocket **Kitten** **Sandworm** Team (BE2 APT, Quedagh) Silent Chollima Spring **Dragon** (Lotus Blossom)
 Stealth **Falcon** Strider - ProjectSauron **TigerMilk** Actor Silverworm (Cobalt Gypsy) Titan Rain Tonto Team
 Turla Group (Group 88, KRYPTON, **Snake**, Venomous **Bear**, Waterbug) Unit180 Unit 8200 Zirconium Group

9



10



11



12



13



14

Hackerprogrammerne - Kali, Metasploit og Armitage / Cobalt Strike

Programmet har indbygget en AUTOUPDATE af NYE EXPLOITS (nye hacker metoder)

17

SHODAN Account Bing Take a Tour Login Register

No contracts. No setup fees. Cancel anytime.

Freelancer	Small Business	Corporate
\$69/month	\$359/month	\$1099/month
<ul style="list-style-type: none"> Up to 1 million results per month* Scan up to 5,120 IPs per month Network Monitoring for 5,120 IPs 	<ul style="list-style-type: none"> Up to 20 million results per month* Scan up to 65,536 IPs per month Network Monitoring for 65,536 IPs 	<ul style="list-style-type: none"> Unlimited results per month* Scan up to 327,680 IPs per month Network Monitoring for 327,680 IPs
<ul style="list-style-type: none"> Access to most filters Allows paging through search results Basic access to the Streaming API Commercial Use E-Mail support 	<ul style="list-style-type: none"> Access to most filters Allows paging through search results Basic access to the Streaming API Commercial Use E-Mail support Vulnerability search filter 	<ul style="list-style-type: none"> Access to all filters Allows paging through search results Basic access to the Streaming API Commercial Use Premium Support Vulnerability search filter Batch IP Lookups Tag Search Filter Complementary Membership Upgrades
1.000.000	20.000.000	

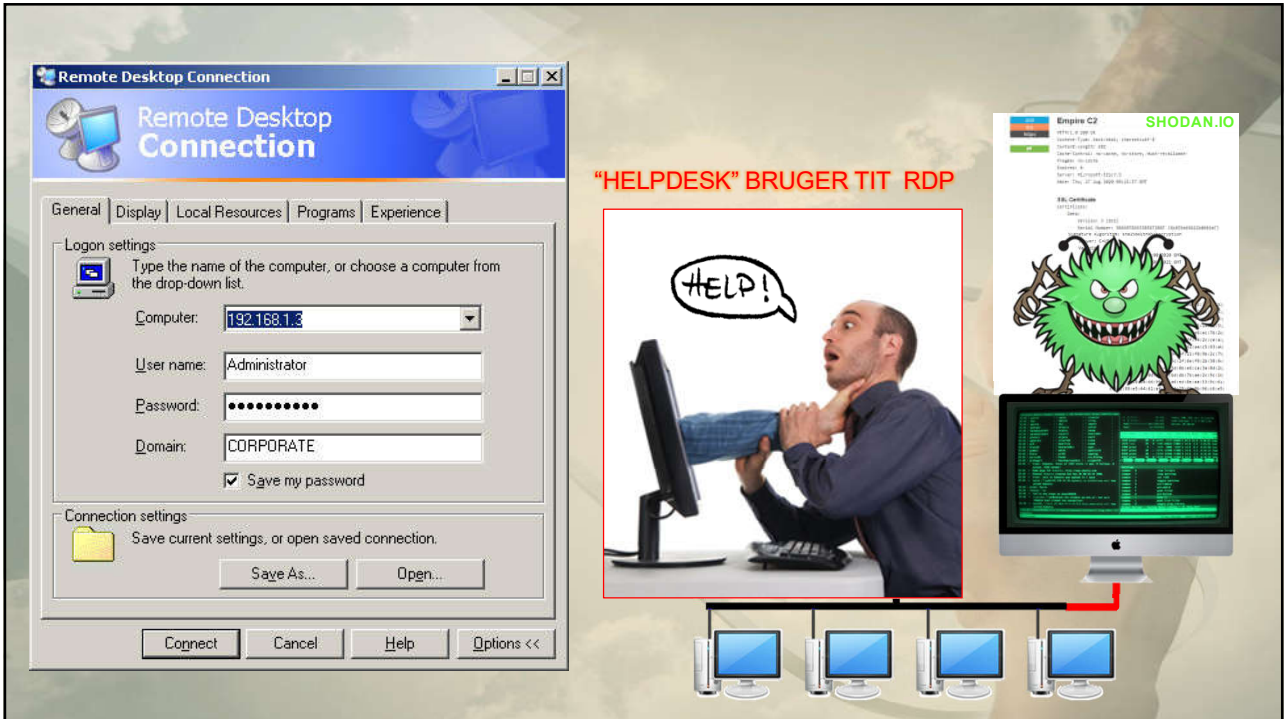
* All API plans are subject to a rate limit of 1 request per second

ROI (%) = $\frac{\text{Profit}}{\text{Costs}} * 100$

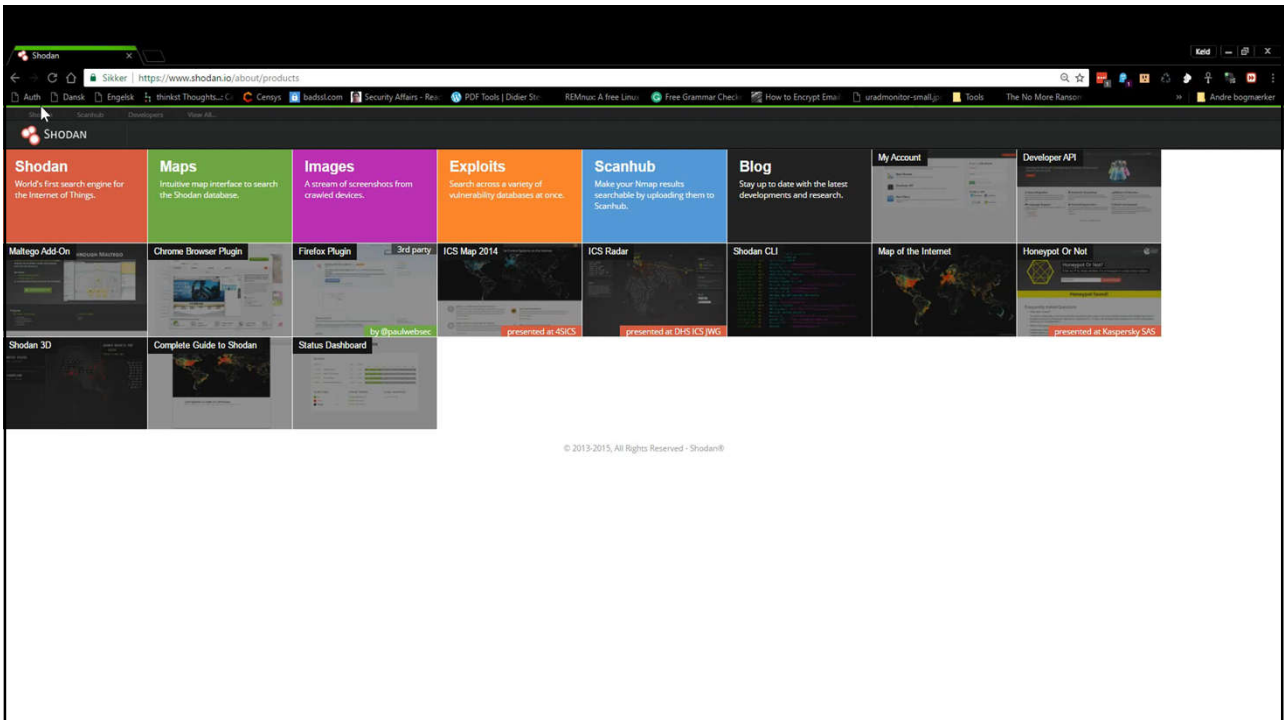
Hver måned får en hacker mulighed for at hacke en milliard potentielle mål

SØGERESULTATER PER MÅNED: 1.000.000.000

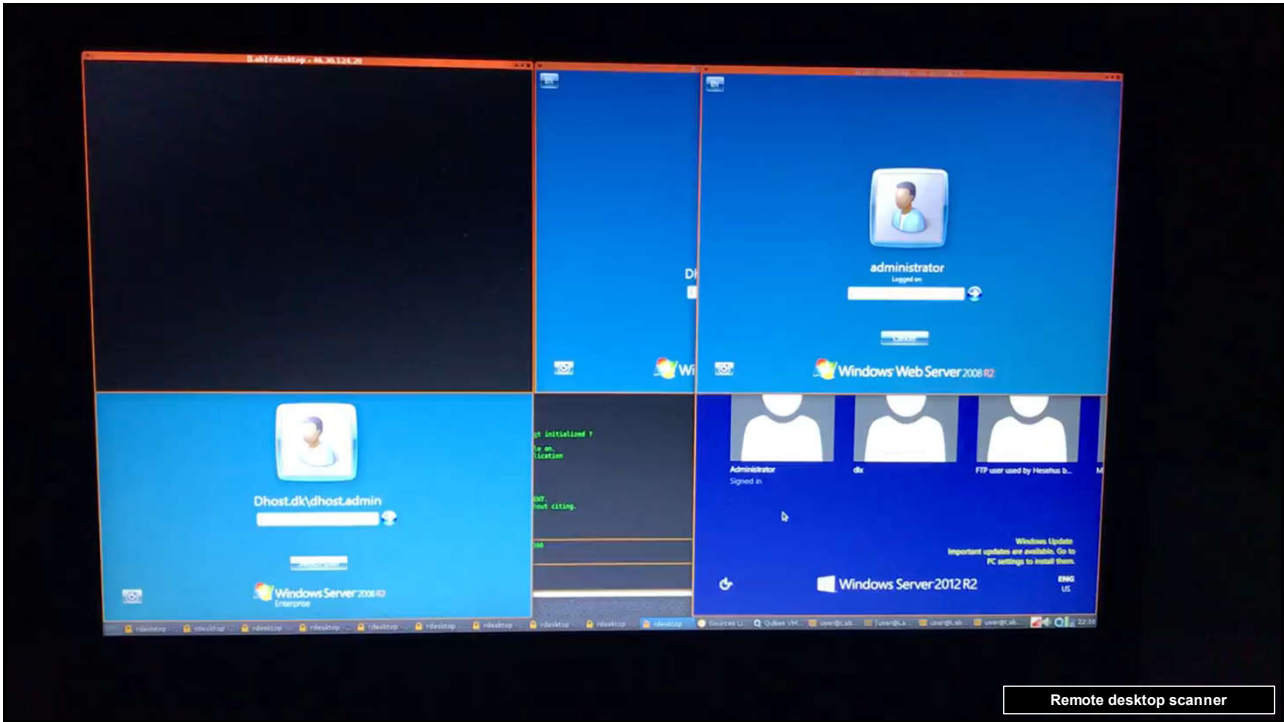
18



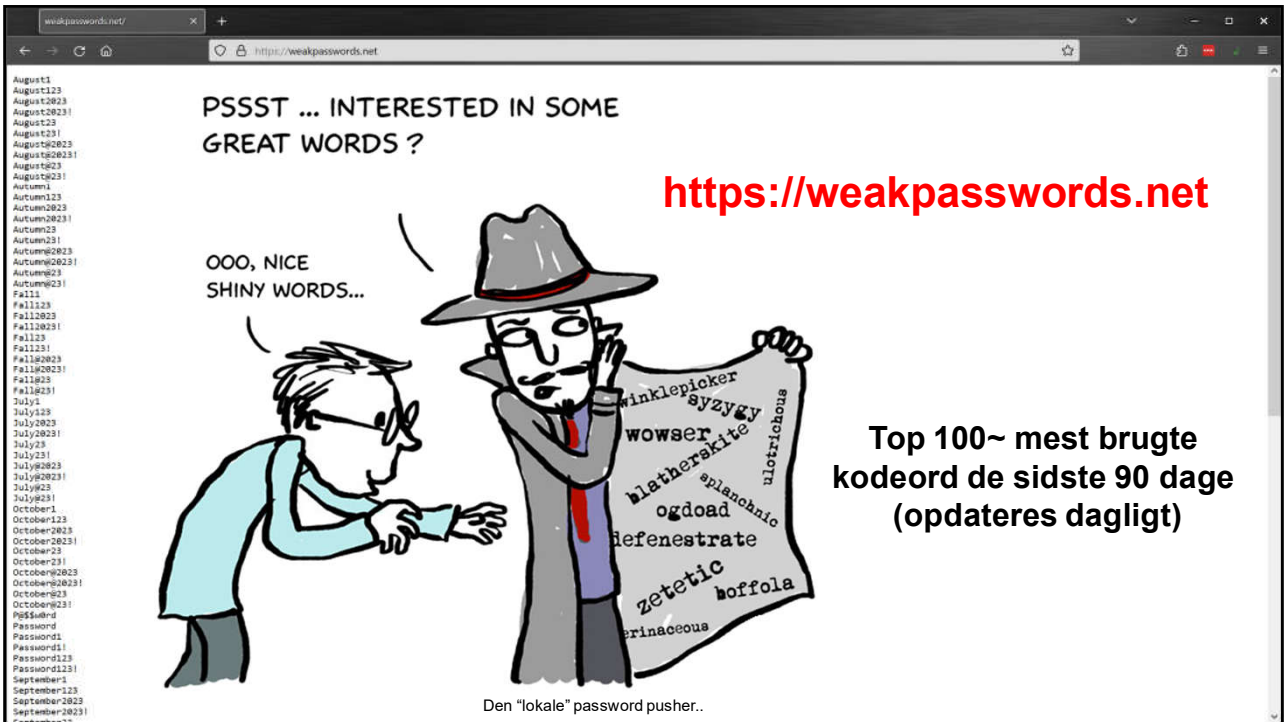
19



20



21



22

Fast RDP Brute GUI v2.0 by Stas'M | rdpthread by ROleg

Stop scan | Max. threads: 1000 | Scan ports: 3389, 3390, 3391 | Enter IP ranges to scan: 129.240.87.1-129.240.255.158

Scan timeout: 2000 | Thread timeout: 60000

Statistics: 397 Hosts left, 0 Good, 0 Bad, 0 Error, PP5: 19

IP-address	Port	Status	User	Password
129.240.87.10	3389	Guessing user and pass... (2%)	Åååååååååååå	123456
129.240.87.13	3389	Guessing user and pass... (3%)	Åååååååååååå	12345678
129.240.87.15	3389	Guessing user and pass... (2%)	Åååååååååååå	1
129.240.87.17	3389	Guessing user and pass... (0%)	Åååååååååååå	admin
129.240.87.18	3389	Guessing user and pass... (2%)	Åååååååååååå	12345
129.240.87.21	3389	Guessing user and pass... (3%)	Åååååååååååå	1234567
129.240.87.25	3389	Guessing user and pass... (1%)	Åååååååååååå	qwesad
129.240.87.26	3389	Guessing user and pass... (2%)	Åååååååååååå	12345
129.240.87.32	3389	Guessing user and pass... (3%)	Åååååååååååå	1234567
129.240.87.33	3389	Guessing user and pass... (2%)	Åååååååååååå	zxcvbnm
129.240.87.34	3389	Guessing user and pass... (2%)	Åååååååååååå	123
129.240.87.43	3389	Guessing user and pass... (2%)	Åååååååååååå	asdfghjkl
129.240.87.44	3389	Guessing user and pass... (2%)	Åååååååååååå	12345
129.240.87.45	3389	Guessing user and pass... (2%)	Åååååååååååå	123456
129.240.87.47	3389	Guessing user and pass... (2%)	Åååååååååååå	123
129.240.87.52	3389	Guessing user and pass... (2%)	Åååååååååååå	12345
129.240.87.56	3389	Guessing user and pass... (2%)	Åååååååååååå	12
129.240.87.58	3389	Guessing user and pass... (2%)	Åååååååååååå	12345
129.240.87.70	3389	Guessing user and pass... (2%)	Åååååååååååå	1

Scanning now: 129.240.94.2 | Active threads: 1000

https://github.com/raddyfiy/Fast-RDP-Brute-GUI-v2.0-by_Stas-M--Official

23

SHODAN | Explore | Developer Pricing | Enterprise Access | Contact Us

Industrial Control Systems

Spotlight

ZERES Wind Turbine
ZERES Wind designs & manufactures wind energy systems for small wind turbine markets designed for powering homes farms or businesses with clean energy.
[Explore](#)

PIPS Automated License Plate Reader
The PIPS AutoPlate Secure-ALPR Access Control System catalogs all vehicles entering or exiting an access point to a site or facility.
[Explore](#)

What Are They?
In a nutshell, industrial control systems (ICS) are computers that control the world around you. They're responsible for managing the air conditioning in your office, the turbines at a power plant, the lighting at the theatre or the robots in a factory.

Common Terms

- ICS: Industrial Control System
- SCADA: Supervisory Control and Data Acquisition
- PLC: Programmable Logic Controller
- DCS: Distributed Control System
- RTU: Remote Terminal Unit

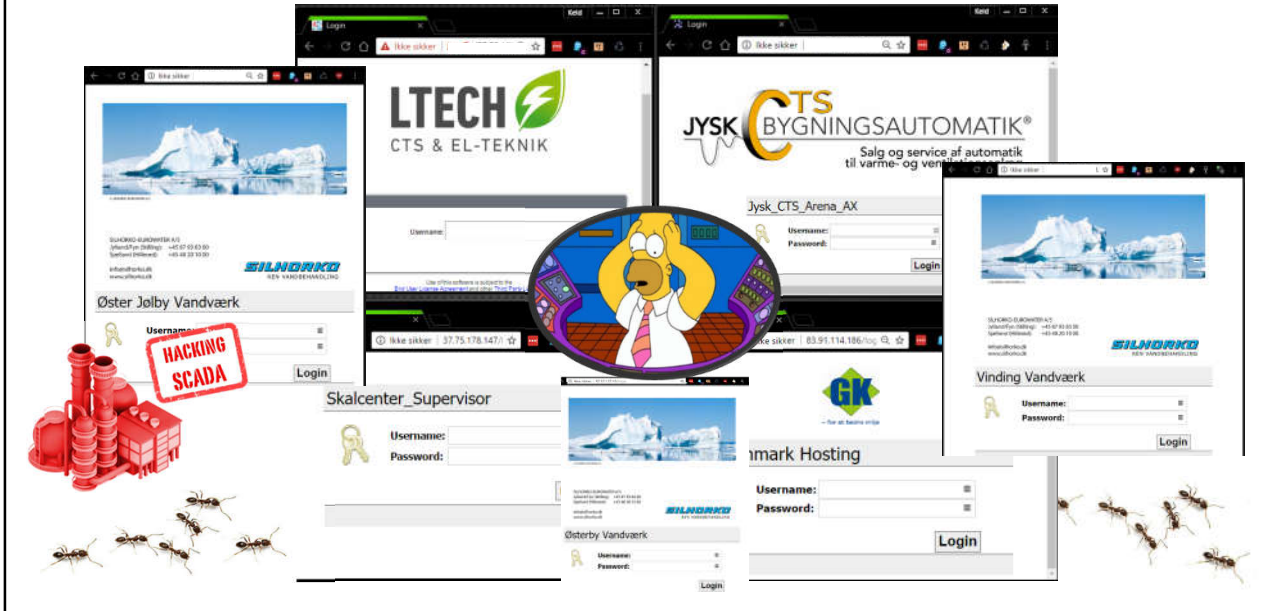
Protocols
The following protocols are some of the languages that the industrial control systems use to communicate across the Internet. Many of them were developed before the Internet became widely used, which is why Internet-accessible ICS devices don't always require authentication - it's not part of the protocol!

- Modbus**
Modbus is a popular protocol for industrial control systems (ICS). It provides easy, free access to the control system without requiring any authentication.
[Explore Modbus](#)
- SIEMENS S7**
S7 (S7 Communication) is a Siemens proprietary protocol that runs between programmable logic controllers (PLCs) of the Siemens S7 family.
[Explore Siemens S7](#)
- dnp**
DNP3 (Distributed Network Protocol) is a set of communications protocols used between components in process automation systems. Its main use is in utilities such as electric and water companies.
[Explore DNP3](#)

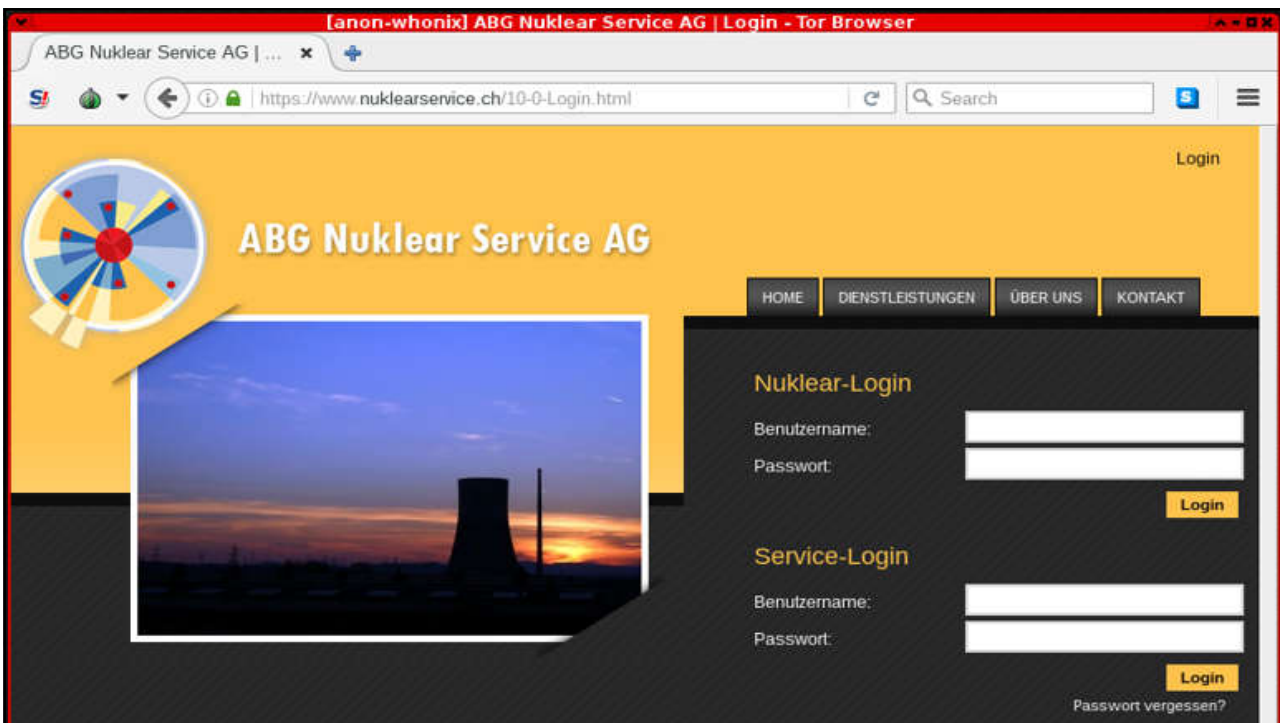
24

Der er massere af "KONTROLPANELER" online..

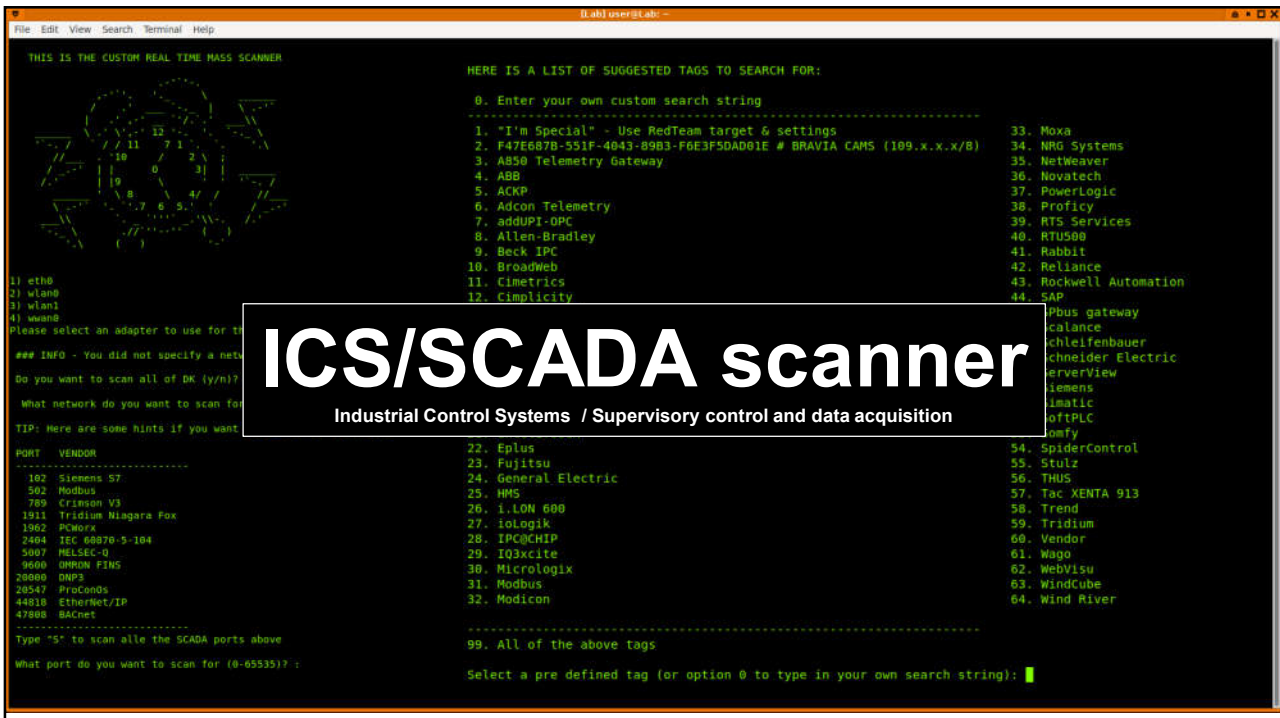
Prøv evt. selv at søge på shodan.io efter: Niagara country:"dk"



25



26



```

THIS IS THE CUSTOM REAL TIME MASS SCANNER

HERE IS A LIST OF SUGGESTED TAGS TO SEARCH FOR:

0. Enter your own custom search string
-----
1. "I'm Special" - Use RedTeam target & settings
2. F47E687B-551F-4043-89B3-F6E3F5DAD01E # BRAVIA CAMS (109.x.x.x/8)
3. AB90 Telemetry Gateway
4. ABB
5. ACKP
6. Adcon Telemetry
7. addUPI-OPC
8. Allen-Bradley
9. Beck IPC
10. BroadWeb
11. Cimetrics
12. Cimplicity
-----
33. Moxa
34. NRG Systems
35. NetWeaver
36. Novatech
37. PowerLogic
38. Proficy
39. RTS Services
40. RTU500
41. Rabbit
42. Reliance
43. Rockwell Automation
44. SAP
-----
45. sibus gateway
46. salance
47. schleifenhauer
48. schneider Electric
49. serverView
50. Siemens
51. iematic
52. softPLC
53. omfy
-----
54. SpiderControl
55. Stulz
56. THUS
57. Tac XENTA 913
58. Trend
59. Tridium
60. Vendor
61. Wago
62. WebVisu
63. WindCube
64. Wind River
-----
99. All of the above tags

Type "5" to scan all the SCADA ports above
What port do you want to scan for (0-65535)? :

Select a pre defined tag (or option 0 to type in your own search string): █

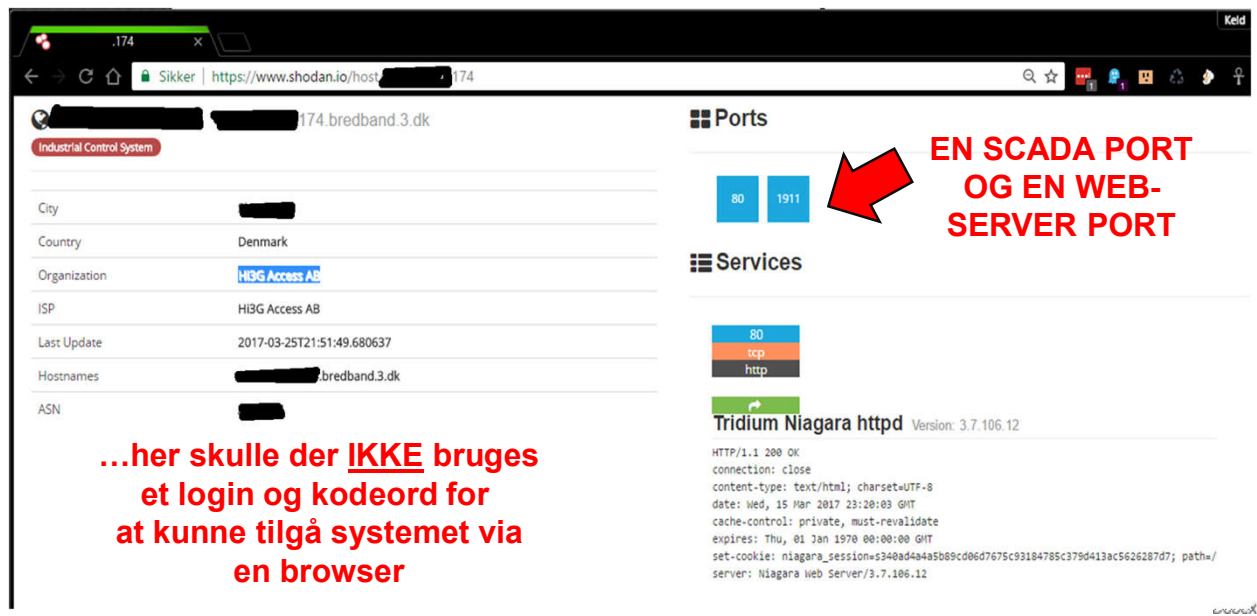
```

ICS/SCADA scanner

Industrial Control Systems / Supervisory control and data acquisition

27

Et andet eksempel..

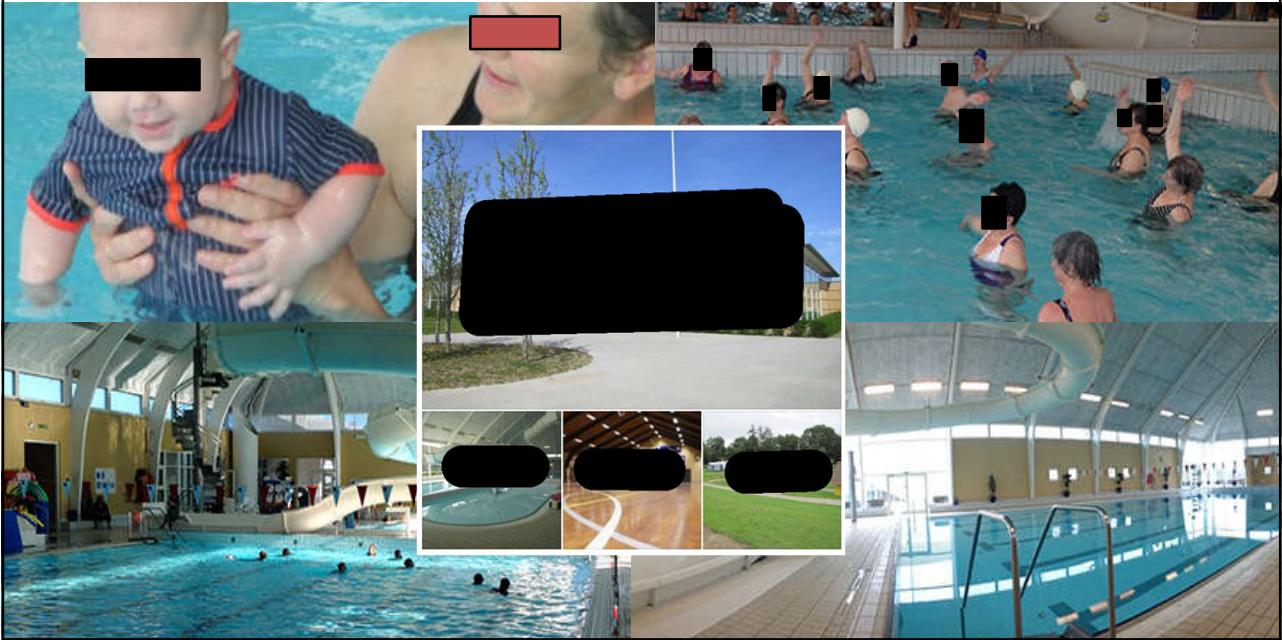


EN SCADA PORT OG EN WEB-SERVER PORT

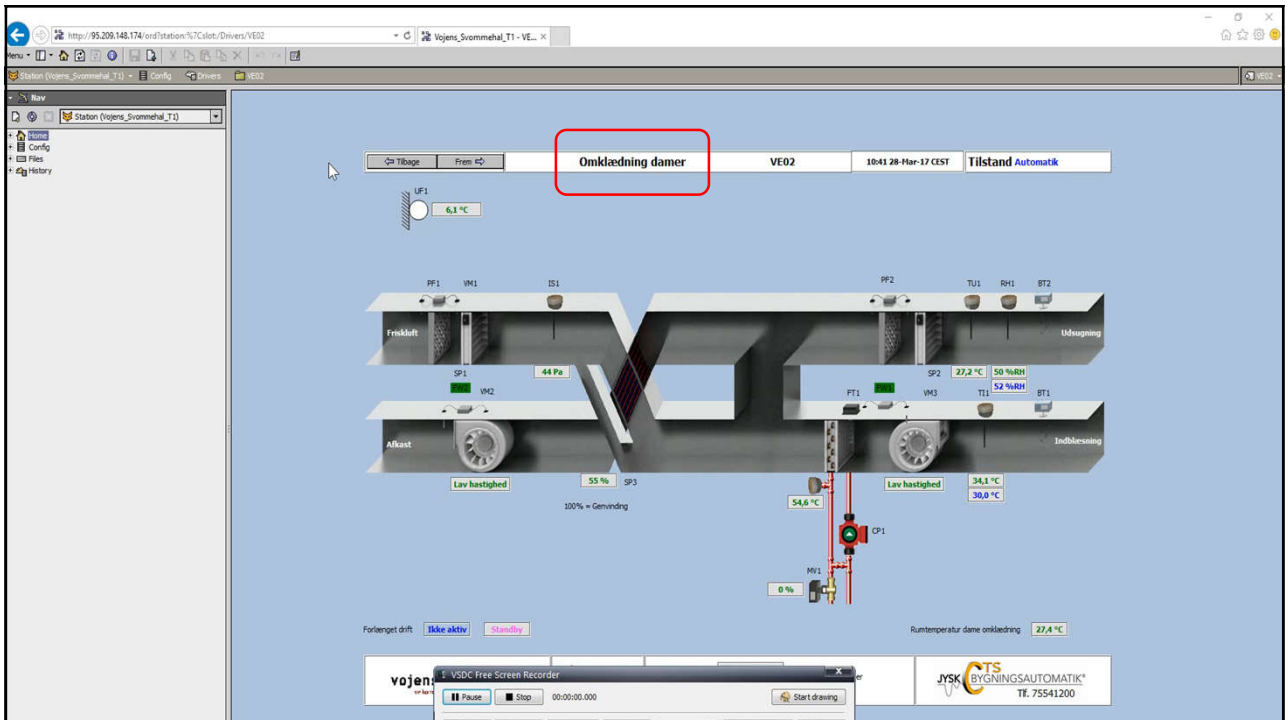
...her skulle der IKKE bruges et login og kodeord for at kunne tilgå systemet via en browser

28

En svømmehal i Danmark..



29

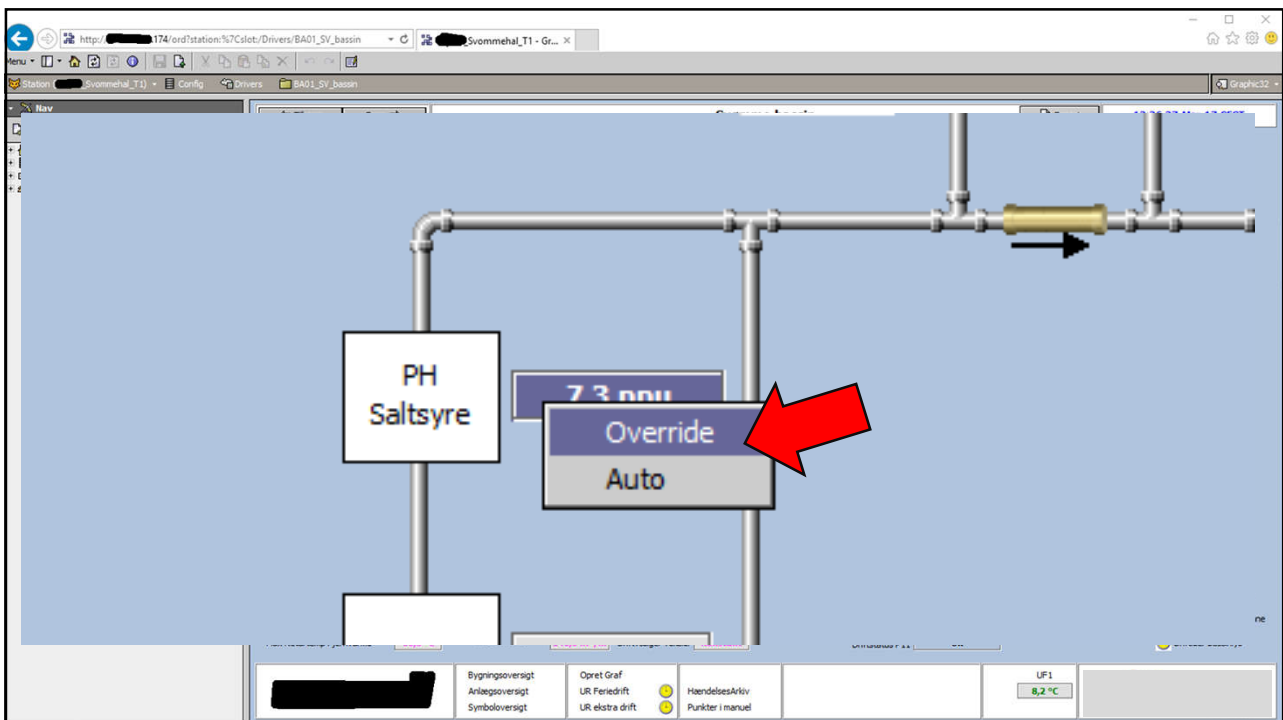


30

Det tyder på at der er en af de ICS/SCADA'er der er kommet online..



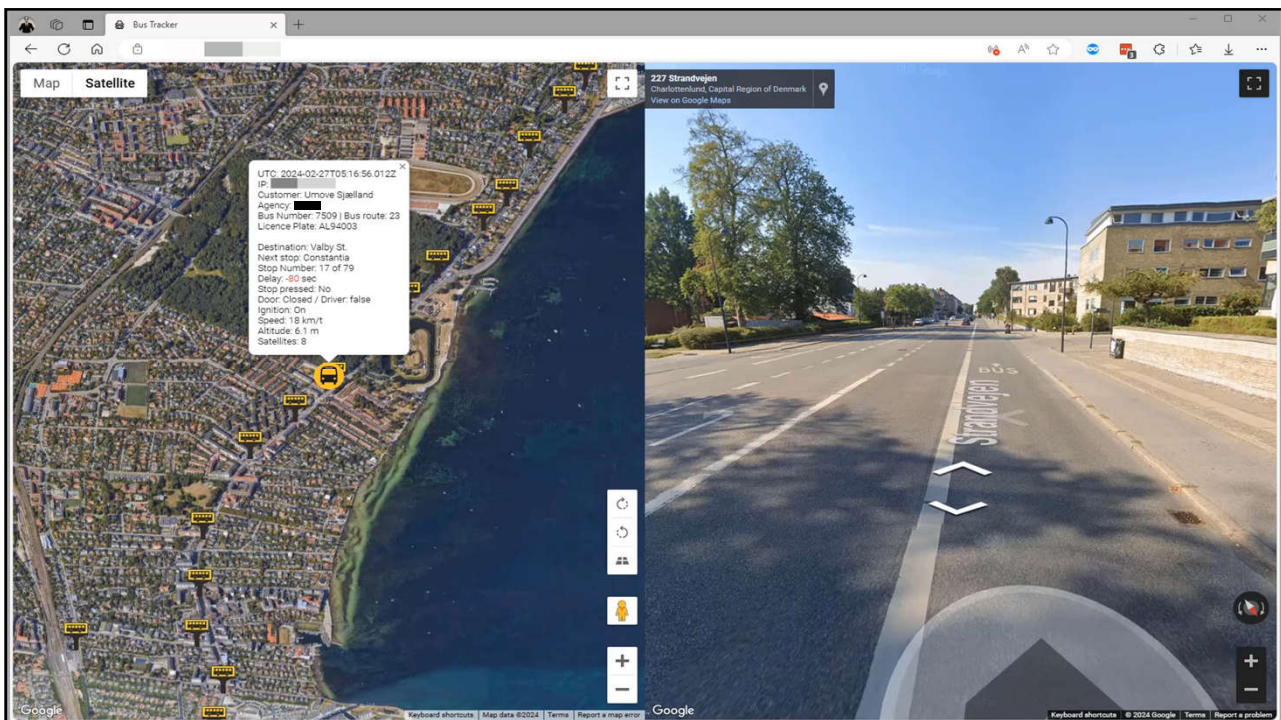
31



32



33



34

The screenshot shows a web browser window with the URL <https://sikkerpa nettet.dk>. The page features the logo 'Sikker på nettet.dk' and navigation links for 'Home', 'Knowledge base', and 'About sikker på nettet.dk'. The main heading reads 'LEARN MORE ABOUT YOUR WEBSITE'S SECURITY IN JUST 10 SECONDS'. Below this, there are three test sections: 'Test your website', 'Test your email', and 'Test your connection'. A large red arrow points to the 'Test your website' section, which includes a text description, a 'Your website domain name' input field with the example 'www.eksempel.dk', and a 'Start test' button.

35

The graphic has a dark green background with a pattern of falling binary code (0s and 1s). The text is in a light green, monospace font. At the top, it says 'DER FINDES ANDRE MÅDER AT FÅ ADGANG PÅ..'. In the center, the main title is '0-DAG SÅRBARHEDER' in a large, bold font, with 'EXPLOITS' written below it in a smaller font. At the bottom, it says 'Hvis man har penge nok..'. The overall theme is cybersecurity and zero-day exploits.

36

zerodium

HOME BOUNTIES FAQ SUBMIT EVENTS CONTACT

ZERODIUM Payouts for Desktops/Servers*

Windows
macOS
Linux/BSD
Any OS

RCE: Remote Code Execution
 LPE: Local Privilege Escalation
 SBX: Sandbox Escape or Bypass
 VME: Virtual Machine Escape

Up to \$1,000,000	Win RCE Zero Click
Up to \$500,000	Chrome RCE+LPE
Up to \$250,000	MS Outlook RCE
Up to \$200,000	VMware ESXi VME
Up to \$100,000	Safari RCE+LPE
Up to \$80,000	VMware WS VME
Up to \$50,000	USB LPE
Up to \$10,000	Antivirus RCE

37

ZERODIUM Payouts for Mobiles*

IOS
Android
Any OS

FCP: Full Chain with Persistence
 RCE: Remote Code Execution
 LPE: Local Privilege Escalation
 SBX: Sandbox Escape or Bypass

13,4 millioner DKK (iPhone exploit)

16,8 millioner DKK (android)

Up to \$2,500,000	Android FCP Zero Click
Up to \$2,000,000	iOS FCP Zero Click
Up to \$1,500,000	WhatsApp RCE+LPE Zero Click
Up to \$1,000,000	iMessage RCE+LPE Zero Click
Up to \$500,000	WhatsApp RCE+LPE
Up to \$200,000	SMS/MMS RCE+LPE
Up to \$100,000	Code Signing Bypass

38



verizon Data Breach Investigation Report

81 %

af alle digitale indbrud sker med stjalne eller "dårlige" kodeord

(Note: A small image of a person's face is partially visible behind the percentage sign.)

39



KODEORD

Gode kodeord og to faktor..

(Note: A question mark icon is in the top right corner of the slide.)

40

Den mest brugte kodeordspolitik:



Settings

Your info

KELD NORMAN
DUBEX\kno

- Brugerens rigtige navn må ikke indgå i koden
- Minimum 8 karakterer
- Mindst 1 lille og 1 stort bogstav
- Mindst 1 tal + 1 special tegn

41

Den typiske password adfærd

8 / 10 / 12


Hvis passwordet skal være på minimum otte tegn

...er det oftest kun på otte tegn



Ref.. Fra forsvarrets efterretningstjenestes kodeords vejledning 2016

42



**Skal passwordet indeholde et stort bogstav,
bliver det store bogstav typisk anbragt
som det første bogstav i passwordet**

A lle_mine_k0der_starter_med_1_stort_bogstav

43

Mon du har tallet 0 eller 1 i dit kodeord ?

min1k0de **P@ssw0rd2019**

Hvis passwordet skal indeholde tal, bliver disse ofte angivet mellem 0 og 99 eller som årstal og gerne placeret til sidst.

**Det er også almindeligt at ændre bogstaver med tal.
"e" bliver f.eks. til "3", "o" bliver til "0" osv.**

1

44

!@-.#\$%&*=?

Kravet om specialtegn løses i mange tilfælde ved at bruge ét.

Snabel-a ("@") og udråbstegn ("!") er nogle af de mere populære.

Hemmelig1.

V@ndmand!

!-@#\$\$%&*=?.

Mink0de!

45

Vinter2024!

Skal passwordet ændres med faste mellemrum,

er der mange brugere, der anvender cykliske ord
i form af ord for årstider, kvartaler, måneder osv.

(der vælges tit et kodeord som er næsten identisk med det tidligere)

46

H@nsJens1!

MinK@tBing0

Vuffe123!

Passwordet er det samme som brugernavnet eller en del af det.



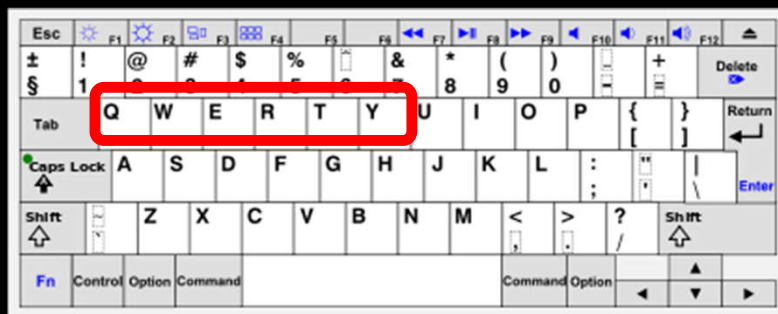
Passwordet består af navne på familie, venner, husdyr osv.

(og ting der er omkring folk når de skal "finde på..")

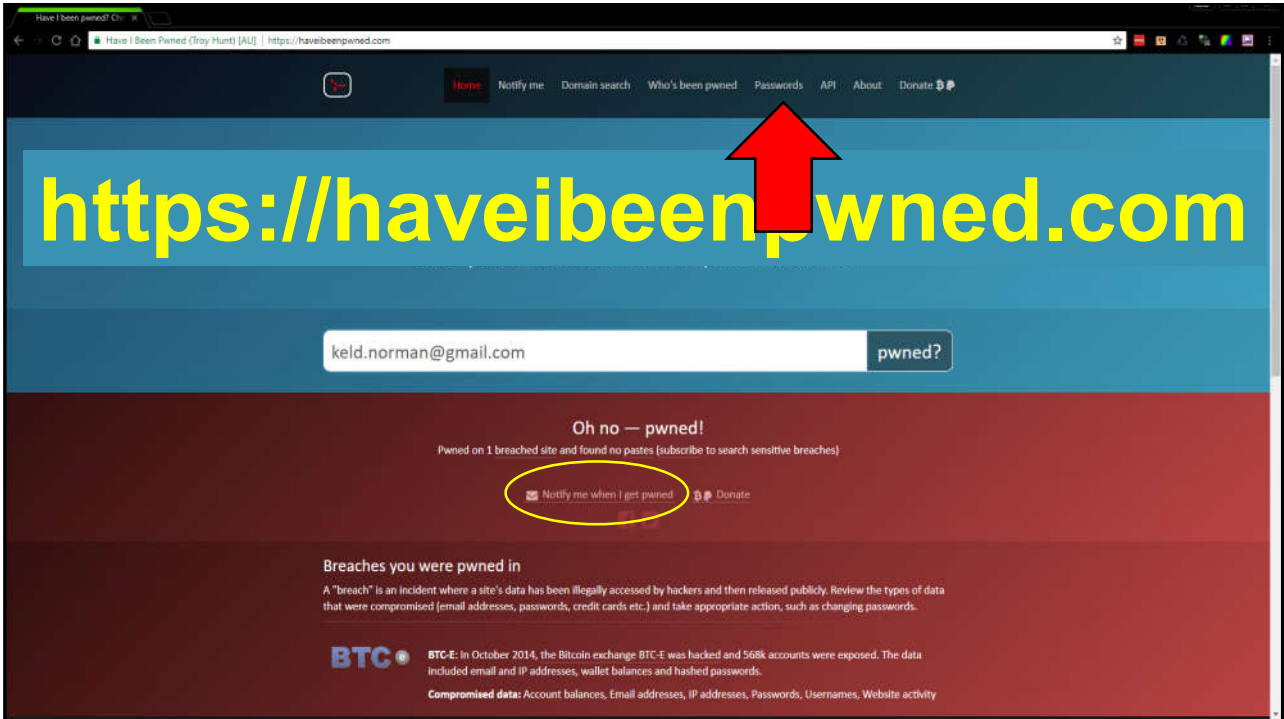


47

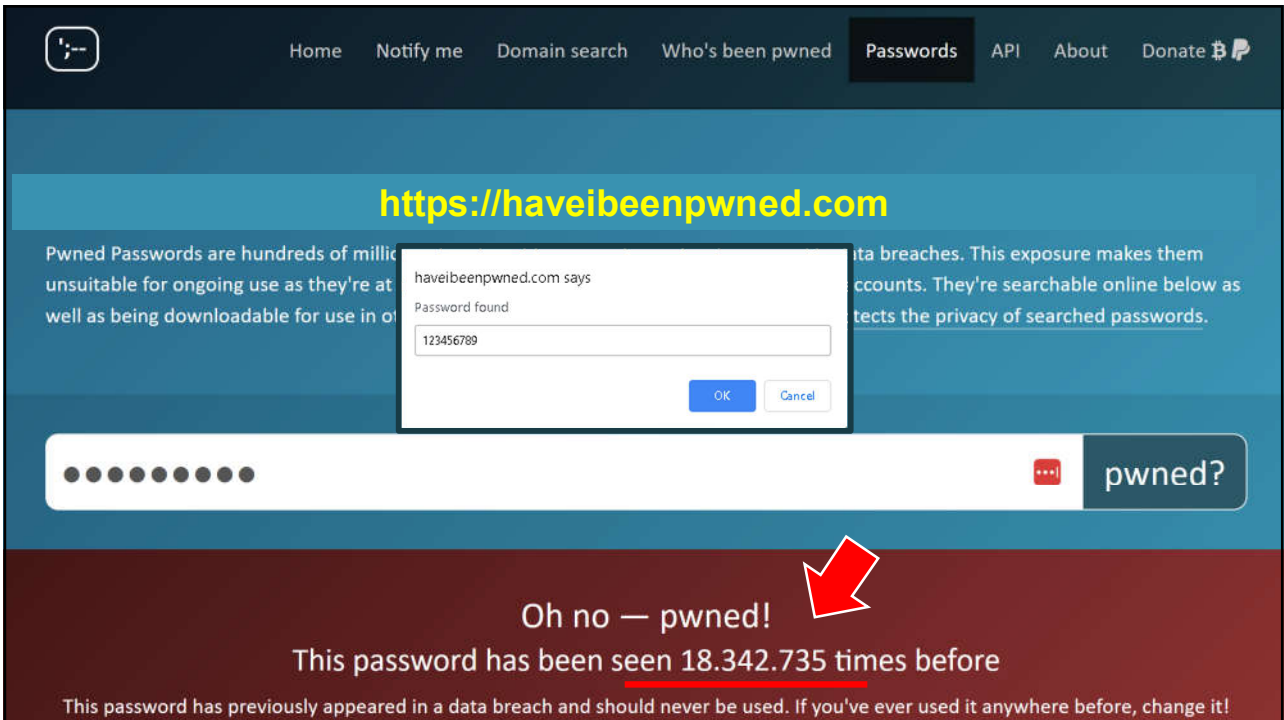
De mest brugte passwords er bl.a. "123456", "password", og bogstavrækker som f.eks. "qwerty", der følger rækkerne på tastaturet.



48



49



50

abcvebu AGENT007 alaska29 Amanda03 amanda13 anders32 annaliva annamoni Anni2013 anni84km asdfghjk bandholm bbaukb6x beauty08 blaavand Borgen88 brandes8 buddinge caroline ceaoghd2 celine02 chrissie cogiwoxy dedeno46 dederyfi emi2005 emi6881 etsuko77 fahajve famuni03 fefabe66 flemming frankrig ganisu97 gaxusyxy glimmer7 gotami17 gyjinyxy hannah15 hanserik havfruier	henry111 hesse193 hinnerup icecream IngridSN isetta61 jesogras Johannes julebyg JvBCLD18 Karina82 kathrine KATHRINE kaxyzufe KIWIKAVA Kodeord4 laageder laageder labepawa LahJ7832 larsen66 larsen67 lena2222 lime1543 lj2501ej lu05za06 mandag14 maradona mari1234 MartinMa mathilde Memonax18 merkur17 mike1199 missekat MITOCLDE momogobo natdragt nebbiolo Nicoline nijivomy nina0504	nokasywa novumavy odin0990 okokdada ope11993 Oxambo2 palmaa07 perlelaj permasse petecozo plu2nium poll_ttp qgw92vdt qipyzode radikale rb05wour sangbog8 sanjamus satan666 satuba00 sebaldu8 snuske02 sodavagid spiritus Stoffer3 surinat surozi tage5237 tekirico thorkild Thorkild thyramin tidself18 tm8qqsch trunte95 Ulle2007 villamaj villum42 wanyrimu ward0642 Westend.	wMPgTHM2 wobikovu xamoxewy xunaxyca xgugigix Y4AeMImJ yamaha01 yolante Zigg1123 ZiMv85ec Zitrone zxD7qu3 zyjuquxe zypujora 2ko47293 2lerance 2wsx3edc 31234567 31234567 1234567 19081506 19791979 19791979 24051994 21234567 45680108 64402413 Adelsteen Aksel1234 alexander allanblom amela2001 andreas01 annafreja barcelona brasilien BRUXELLES budyxogov camilla13 Carlo2004	chanettea ChanetteA christian cirkeline claus0510 combatlap effektive ezroofig flemming1 fredefup1 gitte1910 greenland henriette Henrik29 huskekage ingeborg2 jamesbond lizzitac jule414 juleferie kalle-ma kalle1311 KARENANNA karijan kejsere kencarina knyrr1975 las1.mysp Linda0316 luxemburg lysestege maskehdman mette 1981 muttebabe nanandchr nyrne2010 oskar0210 OVERgaden papilik84 Peter2304 peter2707	poppylamb postkasse randers91 randers99 rasmussen RESERVEXX ribegaard rosenvold shadow123 SKOLEBUS1 sommersko stenbjerg STENBJERG tante1981 tottenham trilind vinter01 vinter01 vinters01 vinters01 vinters01 10.Januar 12.kar 12.kar 12.kar 1311maria 4040nphw 18981898k amaliestat arsummitog1 barcelona7 Borgen2023! charlotte1 charlottea CharlotteA christoffe elizabeth2 ehedslist Fleischer1 FlemmingKH folketing1	fuller2211 Henrik1976 ilynatasha Kristoffer kviksen777 lars120275 magnus1234 mallorca-y MariannaBJ mikkel1712 moster2234 mozambique mitza2f0am mullepiggen newcastle1 ninaandm7 Preben2014 raunholt06 slov88slov socialisti sommer2011 sommerhus1 sommersko1 SVUMPUKKEL SydOplev18 teeoff2002 trf.lamiya uddannelse upsalagaade UrsusFelix Valdemar19 valmuearmk verdensysel 5d123456tj 2368garden 7848alster 24042404ar Aimeesilas2 charlotte13 christoffer elsborg1410	folketinget garrucha112 guldklumper harrypottter kalinkasmor Linkedin100 marieLouise scooler2000 Seattle1951 sengelampe1 sommerferie sputnik6083 zeusmaximis asmussen1975 bekkasinvej1 frederik1808 genderbender gustavdele12 Liverpool123 Mollyhunden1 palladio9999 rungsted2960 sommerferien strumpetten ummagumma123 131180messenger emmaladwin00 sadaabukhader skoleprut1234 sophiedeliso williamknigge Skopperkaffe5 skoleprut12345 vlad-kovalev2008 AnneliseVossRomme footballaddict9999 smgtasteswickedgood
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

PASSWORD LEAKS
OG MAILS TIL NÆSTE
PHISHING KAMPAGNE

53

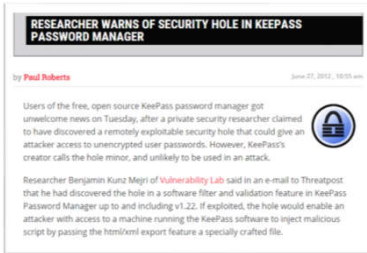
Et Plugin i din browser husker alle dine kodeord (en password manager)

Det er dansk!

54

Risiko og konsekvenser...

PASSWORD MANAGER Hacked



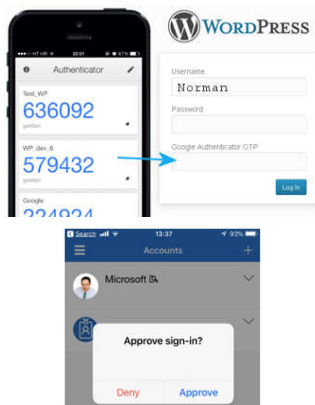
Tænk på..
 Google gmail
 gemmer mange års e-mails.
 Hvad står der i dem?
 ..hvis nu du bliver hacket?

Sendt du banken et
 billede af dit pas?
 Kopi af lønseddel?

Da du søgte om et lån
 for 10 år siden..

55

Brug 2-Faktor login..



2-Faktor ved brug af en applikation



2-Faktor ved brug af papir koder



2-Faktor ved brug af et Token

56

Vidste du at "free wifi" er en sikkerhedsrisiko, selv efter du er logget af ?



57

MAN-IN-THE-MIDDLE



58



59



60



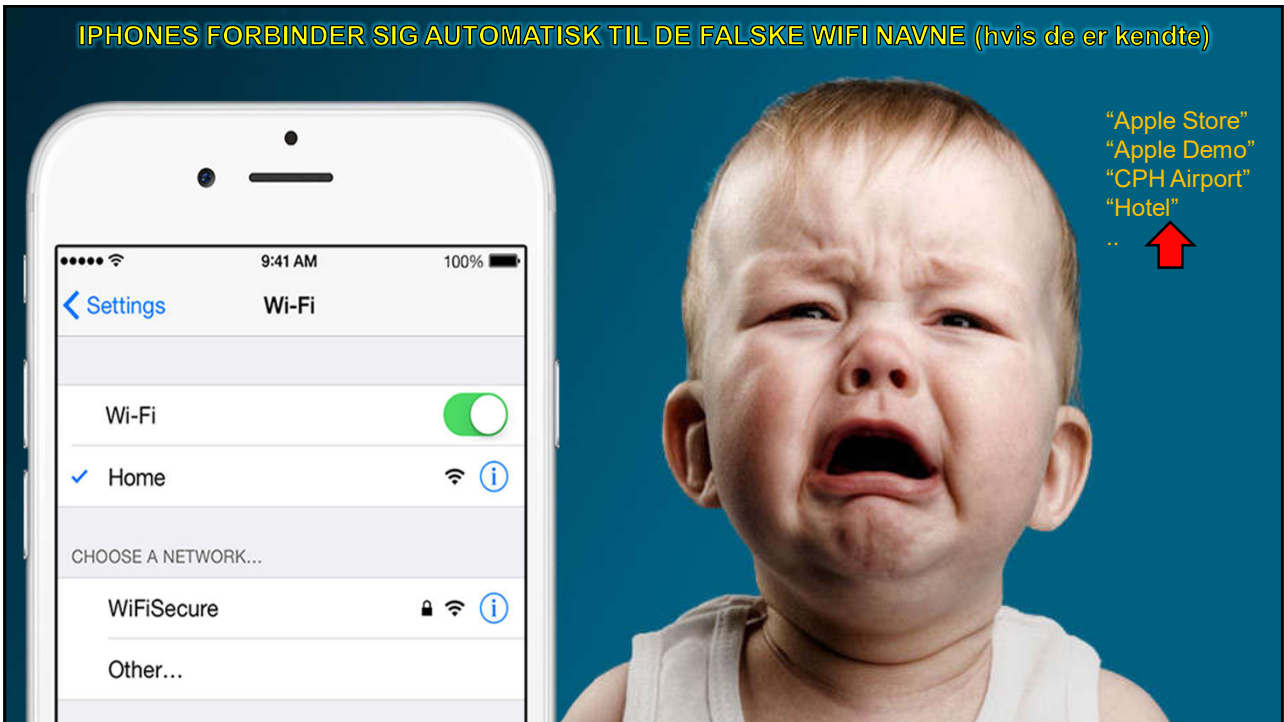
61



62




63



64

Der oprettes automatisk forbindelse til kendte netværk

Men hvis der ikke er nogen kendte (gemte i telefonen) netværk i luften, så kan du vælge..

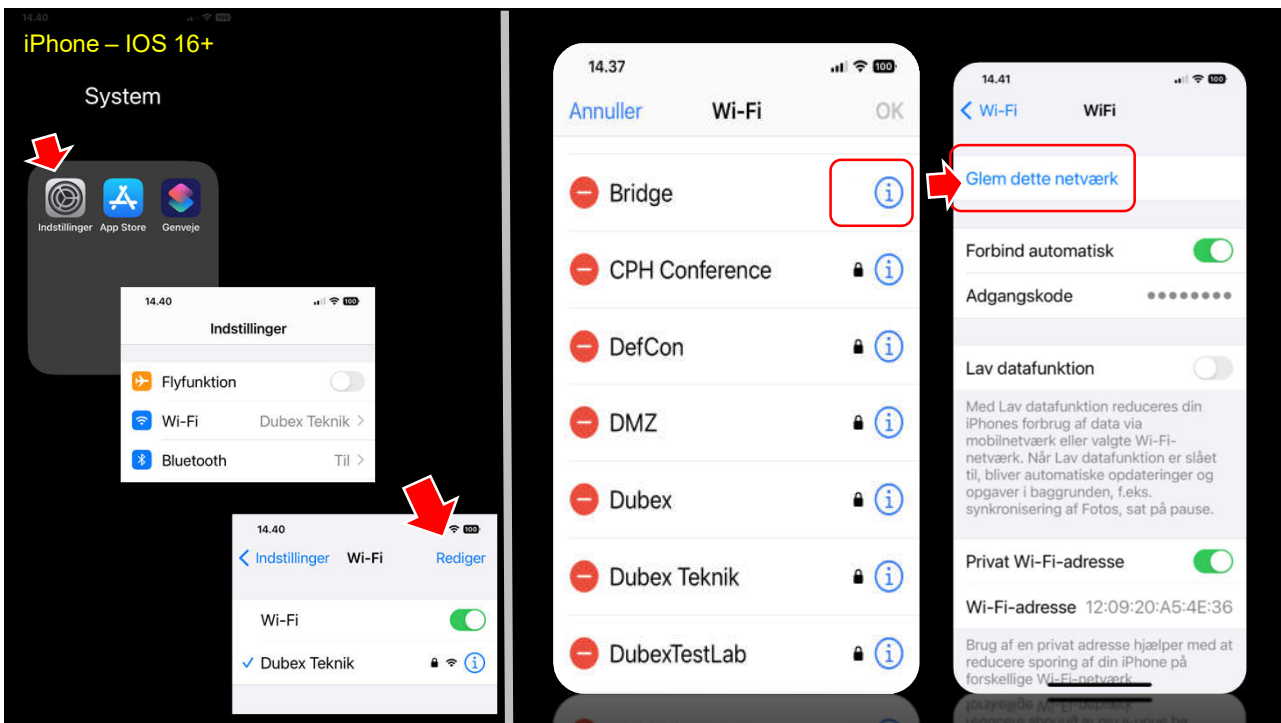


Her sker der ikke noget (ingen pop-up)

Her bliver du **under-**rettet om tilgængelige netværk

Her bliver du spurgt før der oprettes forbindelse til et **NYT** netværk (pop-up)

65



iPhone – IOS 16+

System

Indstillinger App Store Genveje

Indstillinger

Flyfunktion

Wi-Fi Dubex Teknik >

Bluetooth Til >

Wi-Fi

Dubex Teknik

Wi-Fi

Bridge

CPH Conference

DefCon

DMZ

Dubex

Dubex Teknik

DubexTestLab

Wi-Fi

Glem dette netværk

Forbind automatisk

Adgangskode

Lav datafunktion

Privat Wi-Fi-adresse

Wi-Fi-adresse 12:09:20:A5:4E:36

66



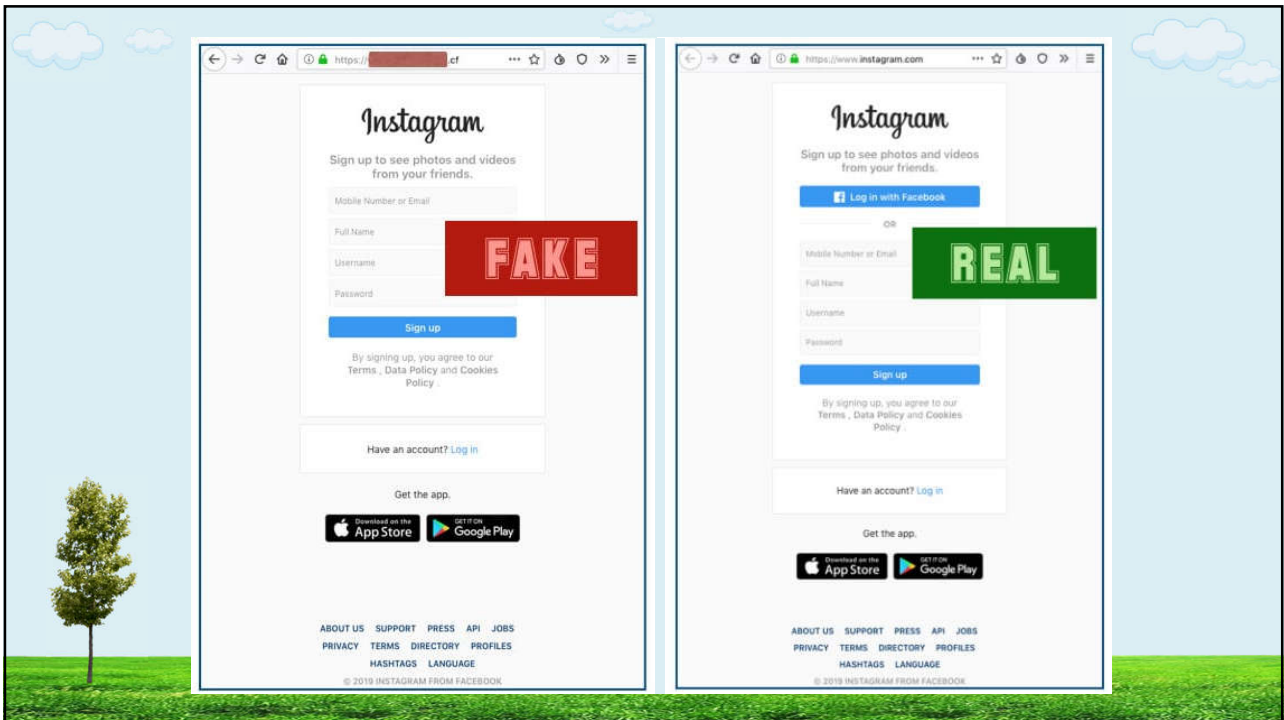
67



68



69



70

Office 365

Arbejds-, skole- eller personlig Microsoft-konto

cfo@dit-firma.dk

Log mig ikke af

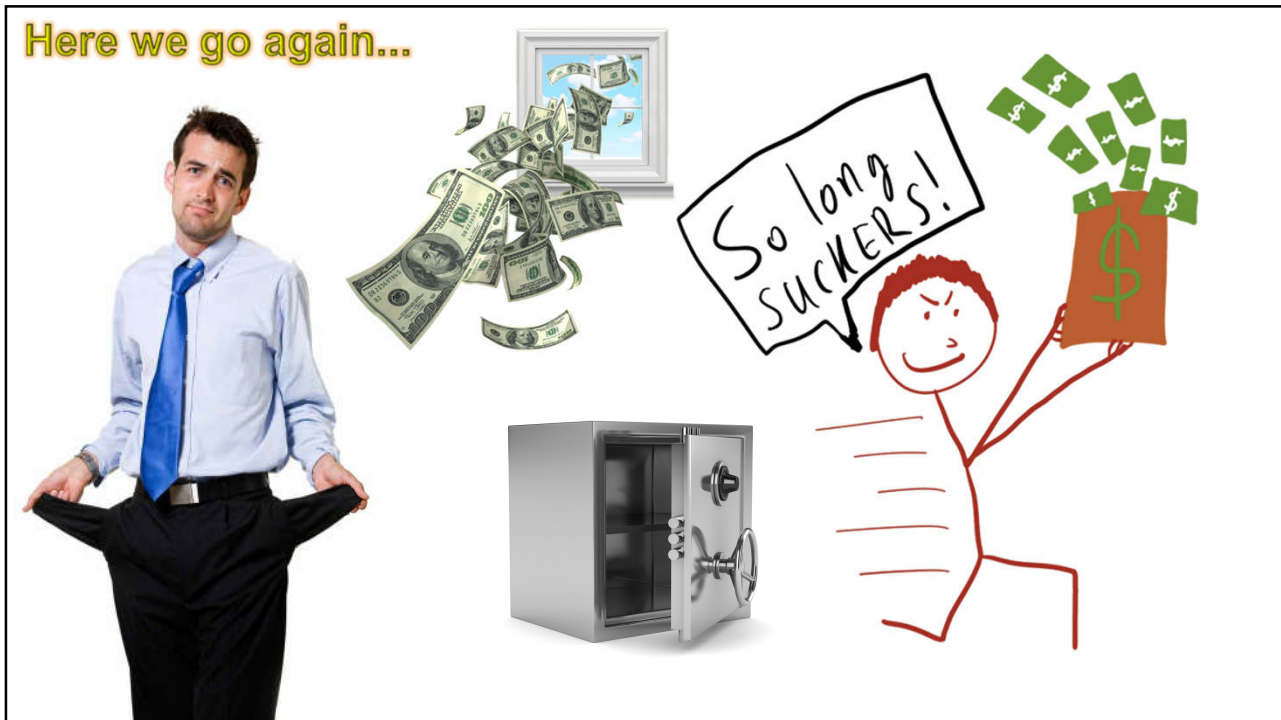
Log på

Can du ikke få adgang til din konto?

EN FALSK OFFICE 365 SIDE STJÆLER DIT BRUGERNAVN OG KODEORD

© 2016 Microsoft
 Vilkår for anvendelse Beskyttelse af
 Microsoft

71



72

Virtual Private Network

vpnTunnel

VPN SIKRE DIN FORBINDELSE MOD AFLYTNING VED AT KRYPTERE DEN OG FORBINDER DIN ENHED TIL ET SIKKERT STED AT SURFE IGENNEM

Dubex

73

Digitalselforsvar.dk

Mit digitale selvforsvar

Selvforsvar

Advarsler

- Svindelmails om NemID og MitID
- Fupbeskeder fra TuGames
- Vær på vagt! Falske Danske Bank SMS'er i omløb
- Spørgeskema og pengepræmie IKKE fra REMA 1000
- NemID: svindelmails og fup-opkald om opdatering af ID-oplysninger i NemID
- Falsk konkurrence
- Transaktionsanmodning er ikke fra Nets
- Pas på, når du shopper skiudstyr på nettet

Digitaliseringsstyrelsen

Svindelmails om NemID og MitID

Opdatér dine ID-oplysninger i NemID

Kære NemID-bruger

I løbet af 2022 og 2023 skal alle med NemID have MitID, hvis du har NemID, kan du bruge MitID til det, som du plejer at bruge NemID til.

Digitaliseringen bliver erstattet af nye over 100. Fordi du skal være sikre og følge med udviklingen, skal du opdatere dine ID-oplysninger i NemID. Det betyder, at du skal opdatere dine ID-oplysninger i NemID.

Derfor skal du opdatere dine ID-oplysninger

NemID er i løbet af 2022 blevet udvidet til fupbeskeder. Det er ikke alle regtilladte NemID-brugere, der lever op til de krav, der gælder for MitID, så kan du, at det er udfordret for dig. Har du kun MitID, skal du derfor opdatere dine ID-oplysninger i NemID. Så du kan bruge MitID og NemID er ligesom før, og du er sikker på, at du er sikker.

Derfor er der nogle regler for, hvordan du skal opdatere dit NemID og dit MitID.

Udfør det nu

Opdatér dine ID-oplysninger nemt og hurtigt

Sådan opdatere du dine ID-oplysninger:

opslysninger.

Nyeste phishings rapporteres på siden: <https://phishtank.org>

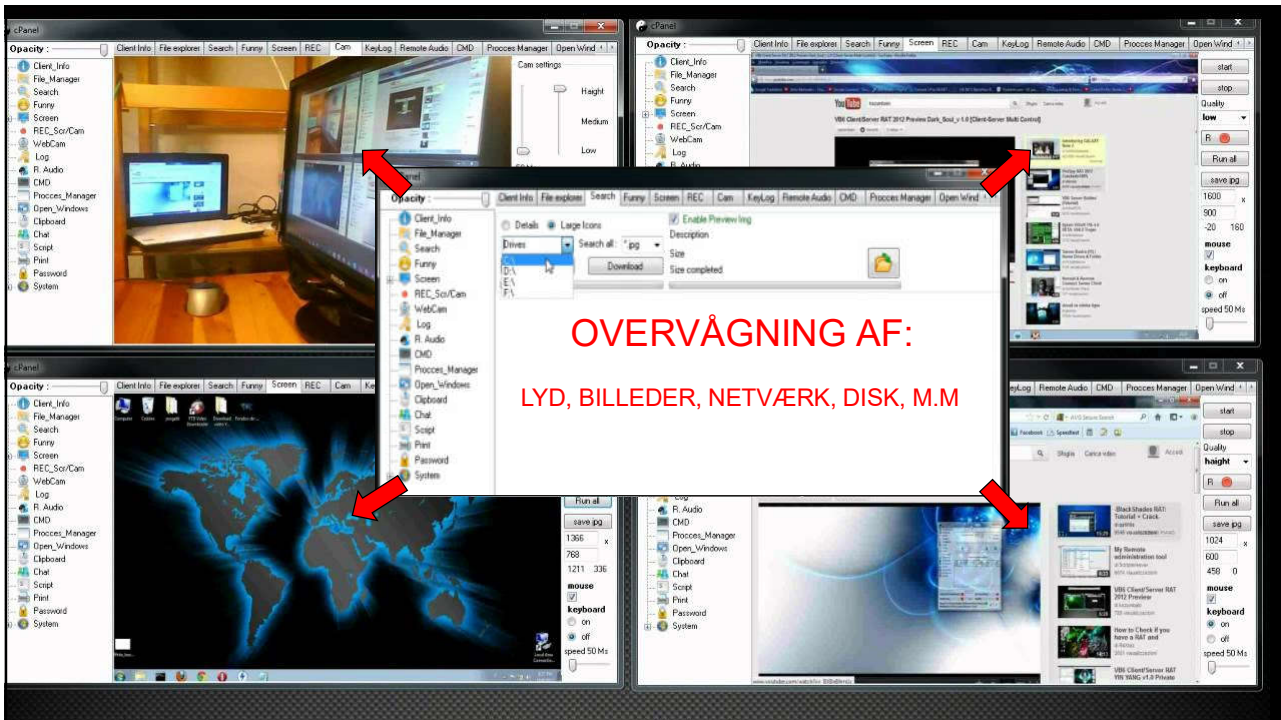
Dubex

74

Hvad gør de når de har fået adgang ?

Dubex:
MANAGING RISK. CHANGING GROWTH.

75



76

File Edit View History Bookmarks Tools Help

Databases Emails Clients Forex Busi X +

p2blcmrur23gmaw4lm36rtka6njclzlaymcmnh4c7ytiuon35eouhyd.onion

USER ACCOUNTS

PERSONAL FILES

WALLETS

PASSWORDS

MNEMONIC SEED PHRASE

NEW UPDATE EVERY DAY! USER ACCOUNTS, PERSONAL FILES, WALLETS, PASSWORDS, MNEMONIC SEED PHRASE, FRESH WORKING COOKIES, AND OTHER

LifeTime - 200\$

FREE SAMPLE: ~30GB

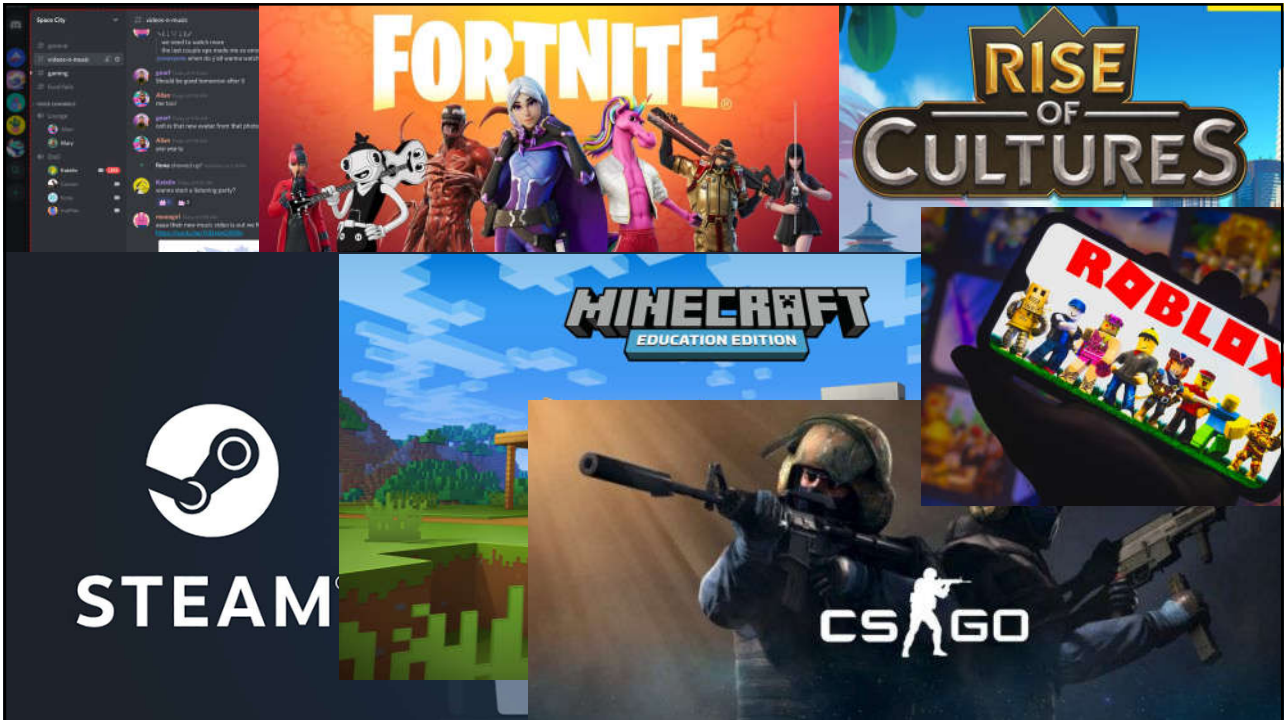
[Magnet Link](#)

[Torrent File](#)

HER KAN MAN HENTE 30 GB DATA GRATIS SOM EN SMAGSPRØVE

200\$ BUY NOW

77



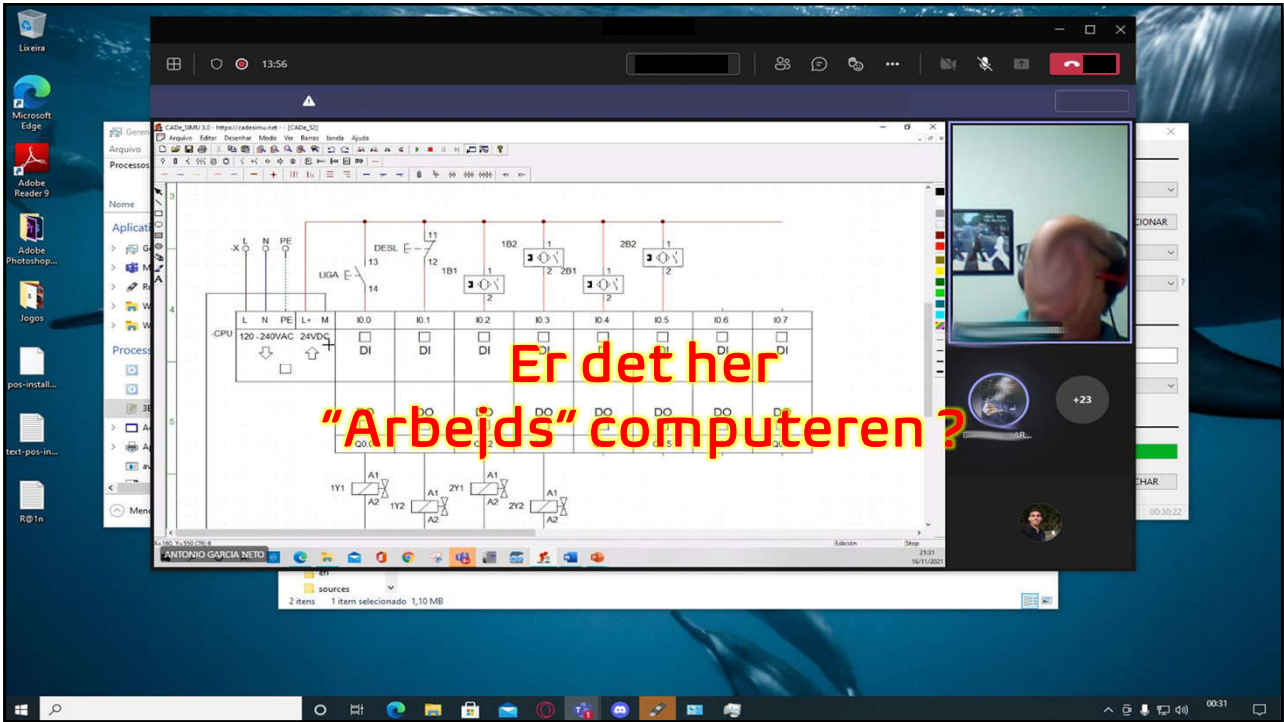
78



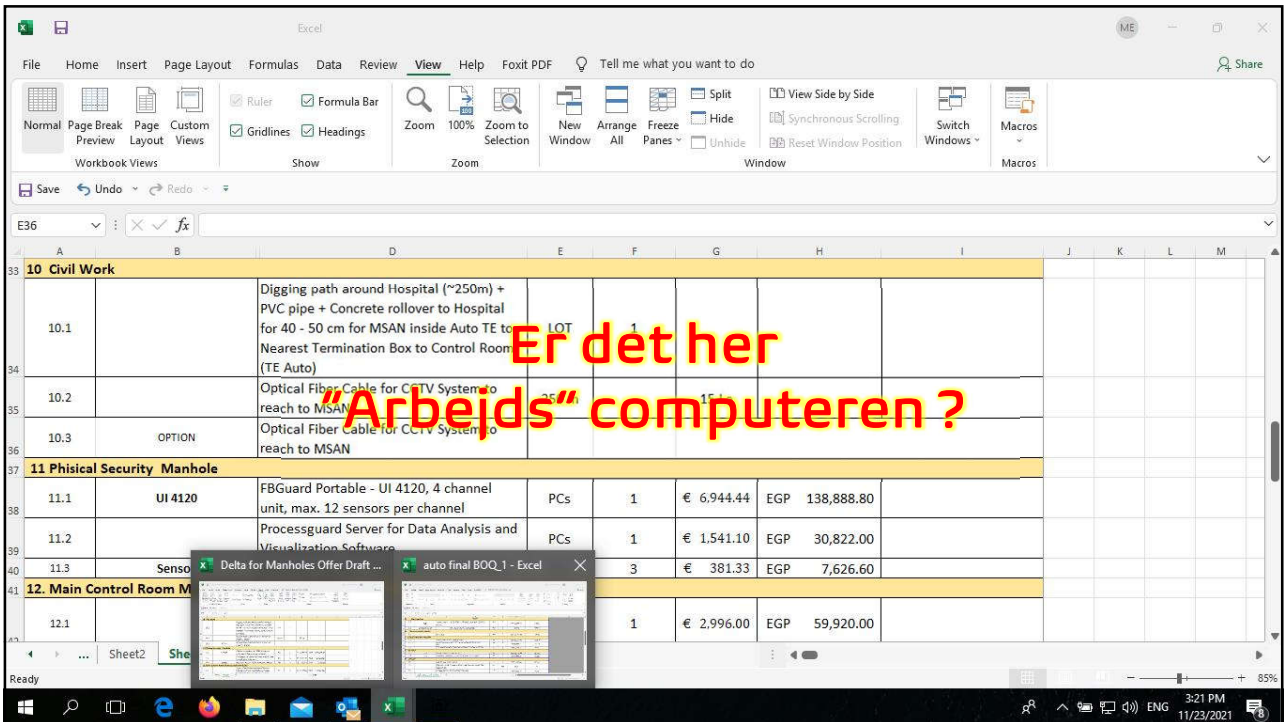
79



80



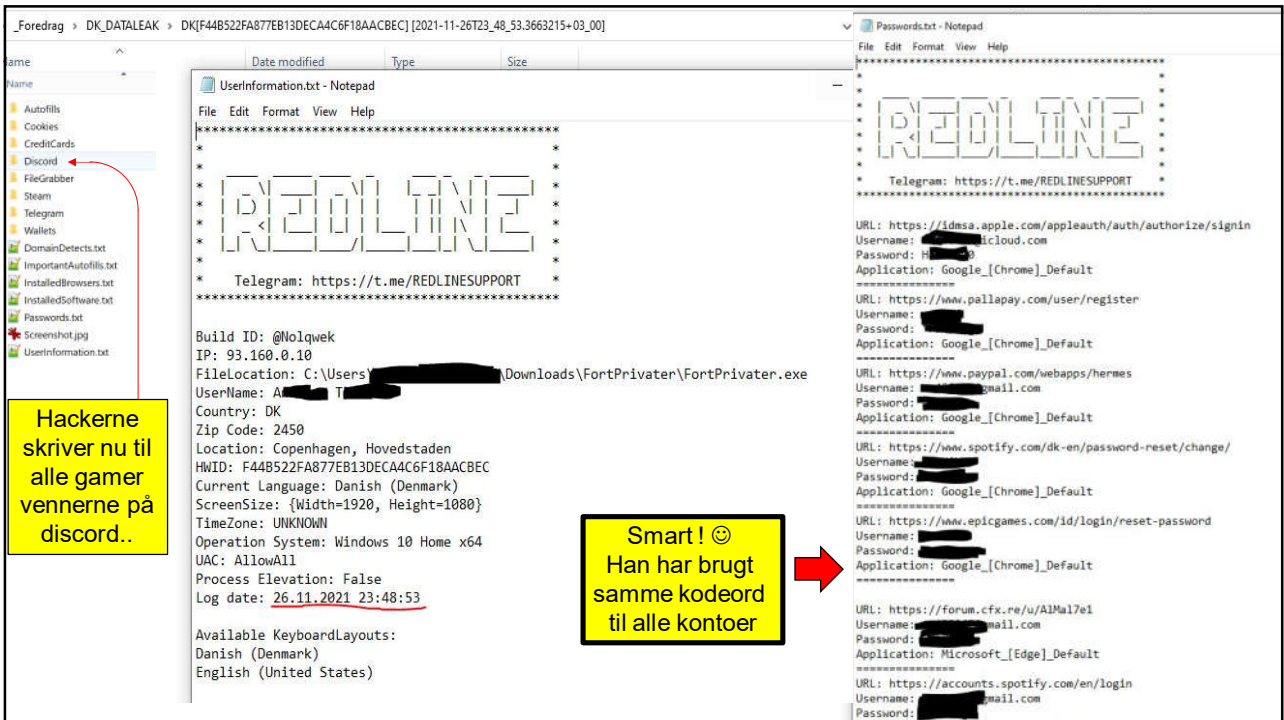
81



82



83



84

Bots til salg



Bot Id	Country	IP Address	Operating System	Ram Usage	Version	Li
36ac61395502e6469b6f70c06018ac3fa	United Arab Emirates	2.50...	Windows XP	0%	v1.0.3	5 Se
aa5f50177c8f545869b9c0517d0916ad53	Pakistan	118.103...	Windows XP	47%	v1.0.3	7 Se
90427a71136d747a5eb9e73deb3a8d394da	Russian Federation	37.122...	Windows XP	52%	v1.0.3	8 Se
966f105119104a42e1ba1f1da212b4c8c17	Russian Federation	37.112...	Windows XP	38%	v1.0.3	9 Se
5ca8ba899fa9040480e50e27d1294b87cdc	India	122.178...	Windows XP	43%	v1.0.3	12 Si
616bf3b788d446469469680456440bebd72	Armenia	46.70...	Windows XP	34%	v1.0.3	12 Si
34fa2862660d84441c8938403ca04b9c3389	Russian Federation	78.110...	Windows XP	40%	v1.0.3	15 Sa
33c3aefc112e1444a8ea9e712a81a075d97a	Spain	87.222...	Windows XP	32%	v1.0.3	15 Sa
7989a9e900f244a8a9f931359114f06f9	India	122.168...	Windows XP	18%	v1.0.3	17 Sa
221d5c8d889e444fb99e91c7a1c2c239a5	France	78.118...	Windows 7	34%	v1.0.3	17 Sa
a4a75d7f6f3bd4d88d84de95725e031feab	India	117.211...	Windows XP	0%	v1.0.3	18 Sa
5c704903005ec6464b7b73999e93a97b0dc	India	27.49...	Windows XP	50%	v1.0.3	18 Sa
0f6c691006a5646bfc3c3dee4d2537dc1f	India	27.97...	Windows 7	48%	v1.0.3	21 Sa
31ea85bc2255f846651821662a960d34411a	Albania	79.106...	Windows XP	27%	v1.0.3	23 Sa
7a399e200c8ca4a81e89e74b6c45c798abe	United Arab Emirates	2.50...	Windows XP	19%	v1.0.3	26 Sa
e30d1f9c99aa7d4d659b398090642119f4	Georgia	46.49...	Windows XP	78%	v1.0.3	29 Si
b249165b0f5c24272bc2ec76c08b40e54	India	122.16...	Windows XP	37%	v1.0.3	31 Si
0dc22af7bb4c34361b31b5be055a01c38	United Arab Emirates	83.110...	Windows XP	0%	v1.0.3	34 Sa
e28b1727f7d94979693665a495c0e25084	Bangladesh	27.147...	Windows XP	35%	v1.0.3	34 Sa
13c098f949e54d233c233821ba1525108	India	117.22...	Windows 7	45%	v1.0.3	34 Sa
57c1d2775bac4ce73883066b164c77a7a2	Malaysia	14.19...	Windows XP	16%	v1.0.3	36 Sa
9736eb5f3a9648920a0e7b2e1657f441	Egypt	41.199...	Windows 7	27%	v1.0.3	46 Sa
91bf825551899497318414005901660db68	Georgia	94.43...	Windows XP	25%	v1.0.3	47 Sa
519d010dd5844fbedb1d36a8460b3c173b	India	114.143...	Windows XP	62%	v1.0.3	48 Sa
57ee758bb70604072822b99ae399eba97	India	117.200...	Windows XP	35%	v1.0.3	49 Sa
94743a3400c194d282ba2bab05ad4d4b312	Unknown	180.234...	Windows XP	0%	v1.0.3	51 Sa
6a2249eece59ad4d90a0967a2c64d61644a	India	117.20...	Windows XP	36%	v1.0.3	52 Sa
189e091d086064632a8da0e8e4eb8a36a26	Vietnam	123.18...	Windows 7	38%	v1.0.3	53 Si
80e4e74e66728141097b97d3473e130be29	India	122.16...	Windows XP	29%	v1.0.3	55 Sa
17d57bee99d944485b9d25d45a7e94d0e	Taiwan	122.11...	Windows XP	62%	v1.0.3	56 Sa

85

Mere end 35 ting en hacker kan bruge din IoT/server/PC til



86

MAIL-BOMB

100 % NEW EMAIL BOMB - COME TRY FOR FREE DEMO -

Buy this listing - you will be given the URL for our online tool. Follow instructions on the site for free demo IF YOU DO NOT PAY YOUR EMAIL IS REMOVED AFTER 5 MINS We spent 1000's on a new server - its superfast - 100 revamped We ask old customers to come back and try us

Sold by **wtfjustwork** - 1561 sold since Nov 17, 2015 **Vendor Level 4** **Trust Level 6**
110 items available for auto-dispatch

	Features		Features
Product class	Digital goods	Origin country	Worldwide
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	Escrow

**EN E-MAIL BOMBE
KOSTER 100 DKK**

Buy this listing - you will be given the URL for our online tool.
Follow instructions on the site for free demo
IF YOU DO NOT PAY YOUR EMAIL IS REMOVED AFTER 5 MINS
We spent 1000's on a new server - its superfast -
100 revamped
We ask old customers to come back and try us

87

SMS BOMBER

**SMS BOMB / FLOOD: 100 or more sms send to your target (Worldwide) !!!
UPDATED - NOW CHEAPER 17.77\$!!!**

NEW (2016-10-07): I FOUND A MOBILE OPERATOR WITH CHEAPER SMS PRICES. PRICE DECREASE FROM 37.77\$ TO 17.77\$!!!
TESTED AND WORKING fine to any International mobile phone number! If you want more than 100 SMS, please order more packages. The
bombing will start during the next 24 hours. Price can't be cheaper as I need to pay the SMS to mobile phone operator. IF YOU ORDER,
PLEASE ENCRYPT...

Sold by **amella75** - 39 sold since Oct 3, 2016 **Vendor Level 5** **Trust Level 4**

	Features		Features
Product class	Digital goods	Origin country	Worldwide
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	Escrow

Default - 1 days - USD +0.00 / item

**EN SMS BOMBE
KOSTER 100 DKK**

Description
Product De
NEW (2016-10-
I FOUND A MOE
PRICE DECRE
TESTED AND W
If you want more
The bombing w
Price can't be cl
IF YOU ORDER, PLEASE ENCRYPT...
1) Target phone number
2) Text message (max. 160 chars)
... using the checkbox right after the notes input.
WARNING: This SMS BOMB attack will freeze or eventually damage your target phone depending on phone brand, version and quantity ordered. Don't use that for a prank!
PLEASE CHECK MY OTHER OFFERS WITH 100% SATISFACTION:
1) DDOS ATTACK with my Botnet: 24 hours on your target
http://alphabaywjrktqn.onion/listing.php?id=199254
2) EMAIL BOMB: Destroy any EMAIL address - Subscription to more than 3K THOUSANDS Newsletters - HUNDREDS EMAILS / DAILY
http://alphabaywjrktqn.onion/listing.php?id=189978

88



89



90

https://canarytokens.org/nest/

CANARYTOKENS.ORG

25 forskellige fælder

Create a Canarytoken.
Deploy it somewhere.
Know. When it matters. ⓘ

Get an alert when an attacker pushes your Azure Entra ID login.

Azure Entra ID login

Get an alert when an attacker visits your URL.

Web bug

Get an alert when an attacker resolves a DNS name.

DNS

Get an alert when an attacker follows your QR Code.

QR code

Get an alert when an attacker loads your MySQL dump.

MySQL

Get an alert when an attacker uses your AWS API Key.

aws

Get an alert when someone opens a fake app on your device.

Fake App

Get an alert when an attacker uses your Kubeconfig.

Kubeconfig

Get an alert when an attacker uses your WireGuard VPN client config.

WireGuard VPN

Get an alert when a log4j logfile is vulnerable to CWV-2021-44-228.

Log4shell

Get an alert when an attacker visits your URL, then redirect them.

Fast redirect

Get an alert when an attacker visits your URL, then redirect them and collect more info.

Slow redirect

Get an alert when a suspicious Windows command is run.

Sensitive command

Get an alert when an image you upload to us is viewed.

Web image

Get an alert when an attacker uses your Azure Service Principal certificate to login with.

Azure login certificate

Get an alert when an attacker browses your PDF document in Acrobat Reader.

Acrobat Reader PDF

Get an alert when an attacker browses your Windows Folder in Windows Explorer.

Windows Folder

Get an alert when an attacker opens your Microsoft Excel document.

Microsoft Excel

Get an alert when an attacker opens your Microsoft Word document.

Microsoft Word

Get an alert when an attacker checks out an SVN repository.

SVN

Get an alert when an attacker sends an email to this unique address.

Unique email address

Get an alert when an attacker accesses your MS SQL Server database.

Microsoft SQL Server

Get an alert when an attacker execute an EXE or DLL file.

Custom EXE / binary

Get an alert (using Javascript) when an attacker clones your website.

JS cloned website

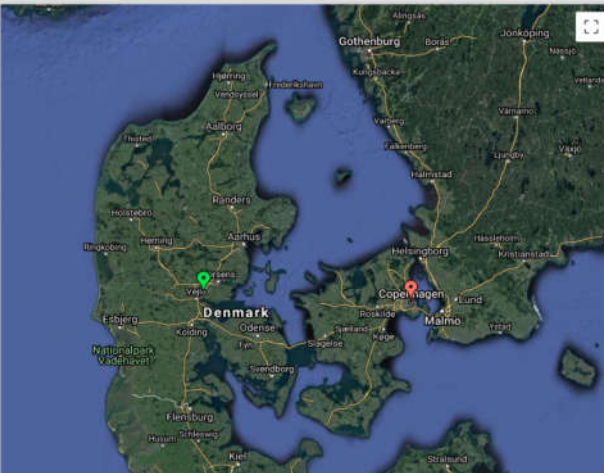
Get an alert (using CSS) when an attacker clones your website.

CSS cloned website

91

Eksempel på data fra en canary token der er blevet aktiveret..

Incident Map



Incident List

Export

Geo Info

Country: DK 🇩🇰

City: Bårkop

Region: South Denmark

Organisation: AS3292 TDC A/S

Hostname: 176-20-222-171-dynamic.dk.customer.tdc.net

Tor

Known Exit Node: False

Basic Info

Memo: Mail til den falske fotograf med billeder

useragent: Mozilla/4.0 (compatible; ms-office; MSOffice 16)

src_data

HOSTNAME: { 'windows_desktopini_access_domain': 'dubex', 'windows_desktopini_access': 'dbxsoew0068', 'windows_desktopini_access_username': 'kno' }

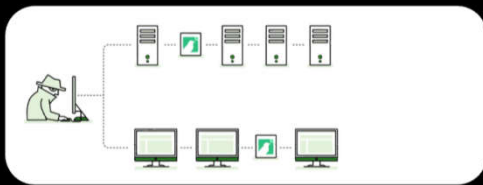
Date: 2021 Apr 10 13:22:10.643544 (UTC) IP: 217.74.215.98 Channel: HTTP

92

Findes også som en appliance og som en virtual server

Emulerer en :

Windows
Linux
Router
Database



<https://thinkst.com> & <https://canary.tools>

Dubex
MANAGING RISK. CHANGING GROWTH.

93

Hvad er det ultimative hacker tool
der findes i dag ?

Tip: Det er noget hackerne har brugt i årtier...

94



Social Engineering Adfærds - manipulation

95

Alle dem med en telefon (i nærheden af mig) – tag den op og se på den..

Vil nogen i en virksomhed der oplevede det her tro deres telefon var blevet hacket ?

Wi-Fi Password

Do you want to share the Wi-Fi password for "Honeywell" with Honeywell?

Share Password

Hvis "IT-Afdelingen" ringede til dig efterfølgende ville du så gøre hvad siger for at "redde firmaet" ?

- Kan du lige logge ind med din 2-factor her og bekræfte..
- Kan du installere det her VPN tool for at vi kan hjælpe dig...
- Kan du fortælle mig hvad din kode er så vi kan checke..

96

Social Engineering kan omgå næsten alt it-sikkerhed..

The diagram illustrates various IT security measures surrounding a central padlock icon, representing a comprehensive security perimeter. The measures include:

- Network Device Backup and Recovery
- Content Filtering Devices
- Email Security Gateways
- VPN Gateways
- Proxy Server
- Spam Filter
- Web Filter
- Firewall
- Antivirus
- Intrusion Detection System (IDS)
- Unified Threat Management
- Wireless Intrusion Prevention and Detection System (WIDPS)
- Network Access Control (NAC)
- Network Load Balancer (NLB)

On the left, a hand offers a bunch of carrots, symbolizing a bait. On the right, a hooded figure sits at a laptop labeled "Social Engineering Hacker", representing the attacker.



97

Automatisk lagring 2021.06.26.MacroDoc.doc - Kompatibilitetstilstand • Gemt i Denne pc ▾

Filer | Hjem | Indsæt | Design | Layout | Referencer | Forsendelser | Gennemse | Vis | Udvikler | Hjælp

SIKKERHEDSADVARSEL Noget aktivt indhold er deaktiveret. Klik for at få flere oplysninger.

BESKYTTET VISNING Pas på – filer fra internettet kan indeholde virus. Medmindre du har brug for at redigere, er det sikrere at forblive i beskyttet visning.

Hackerne benytte forskellige overbevisnings metoder for at få trykket på knapper eller links..

SPEED **GREED** **LOVE** **FEAR**

The cartoon illustrations represent the four motives:

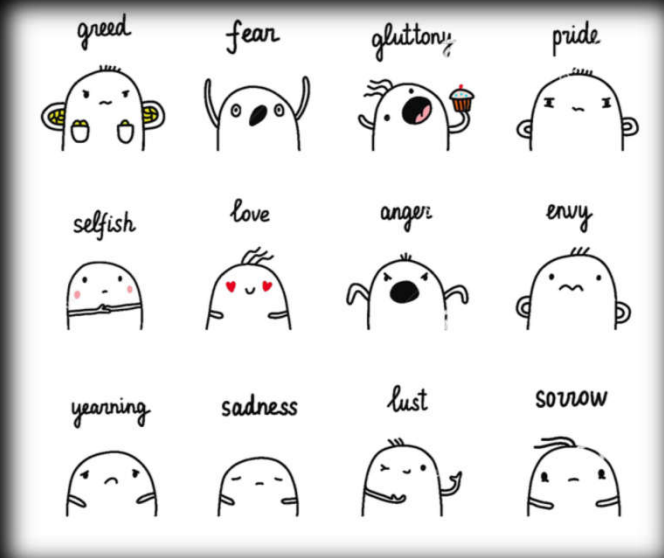
- SPEED**: An alarm clock with "TIME OUT" written on it.
- GREED**: A large wooden treasure chest with a keyhole.
- LOVE**: A man in a blue shirt and a woman in a purple dress, both looking at a smartphone.
- FEAR**: A man in a white shirt and tie looking startled, while a man in a black and white striped shirt and mask (the hacker) stands next to him.

98

Hvordan virker phishing?

- Frygt
- Grådighed
- Nysgerrighed

- Tillid
- Tidspres
- Hjælpsomhed

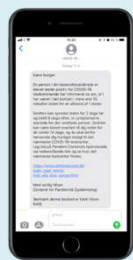


99

Det her, er som oftest, det hackerne bruger i dag til social engineering



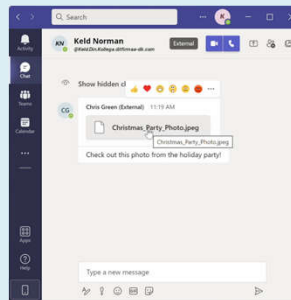
Phishing (e-mails)



SMiShing (SMS beskeder)



Quishing (QR-koder)



IMshing (Instant messaging)



Vishing (Video eller Voice)



100



101



102



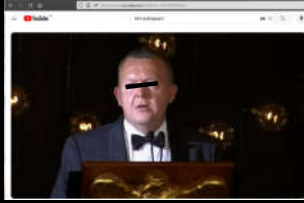
103



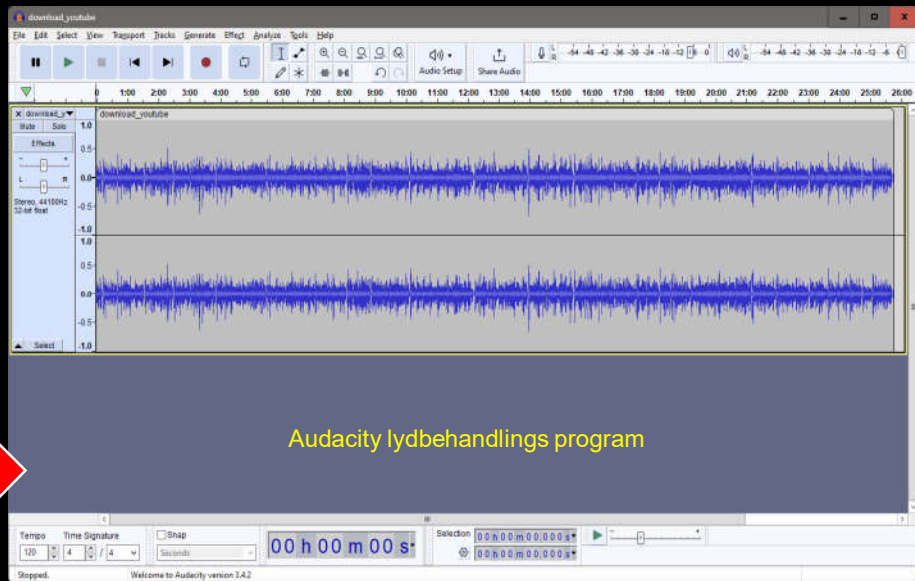
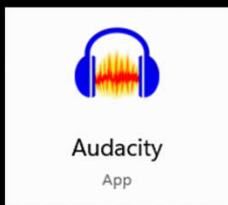
104

Ned til 15 sekunders lyd kan bruges til at lave en stemme profil med..

Download fra Youtube



Udtræk lyd fra klip

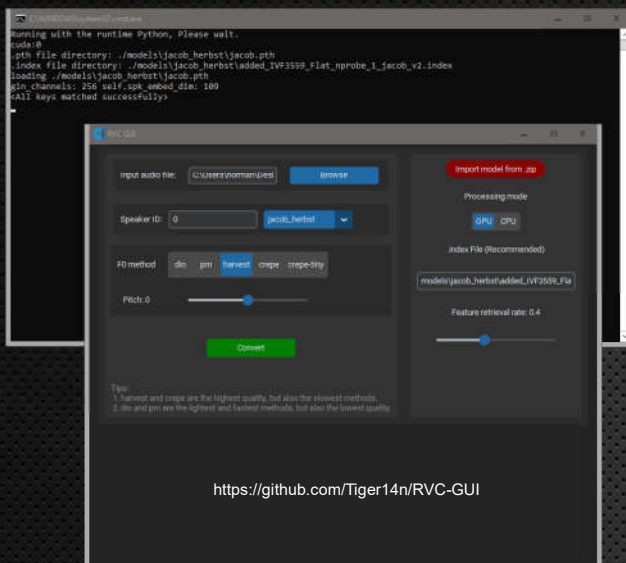


Audacity lydbehandlings program

Audacity er et freeware lyd behandlings software der kan udtrække lyden fra filmen

105

Brug stemme profilen og den optagede besked og lav stemmen om



<https://github.com/Tiger14n/RVC-GUI>



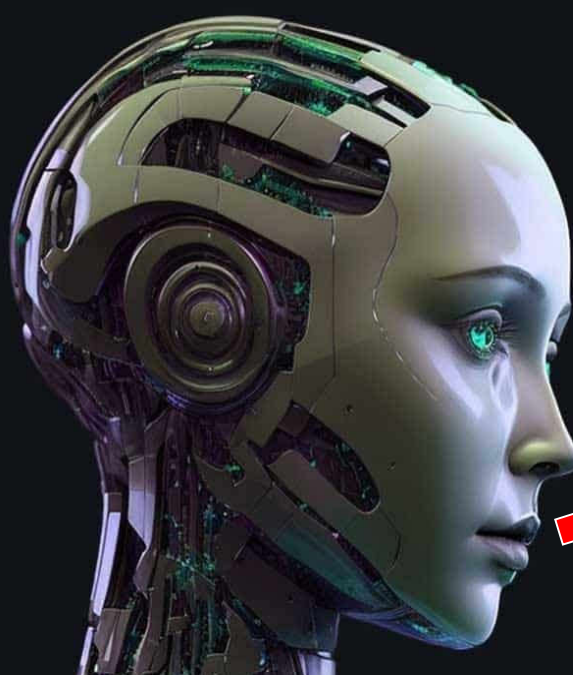
Hej jeg hedder Lars

Hej jeg hedder også Lars..



NB: Det du hører her er KUN Keld der har indtalt noget
(og så lavet stemmen om til .. en andens)

106



The 'o' in chat GPT-4o stands for omni

Omni comes from Latin and means "all" or "everything"
 ..Related to the word 'omniscient,' which translates to "all-knowing"

OpenAI

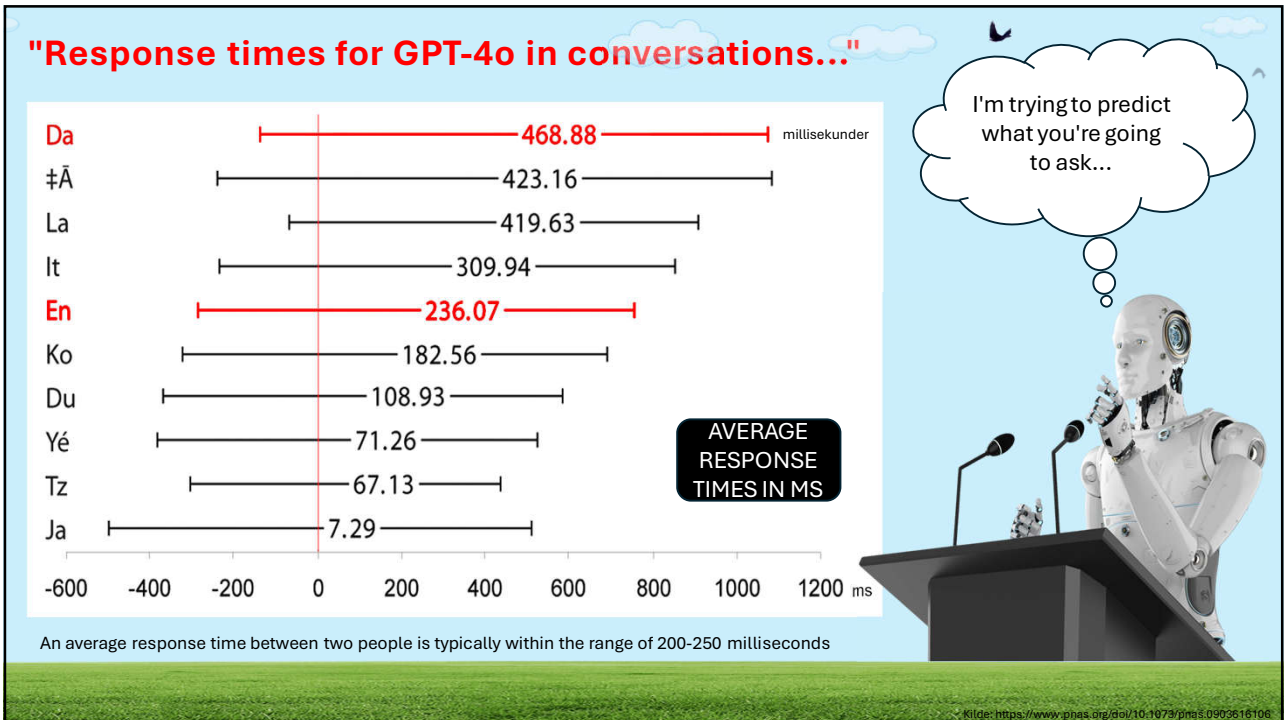
GPT-4

4

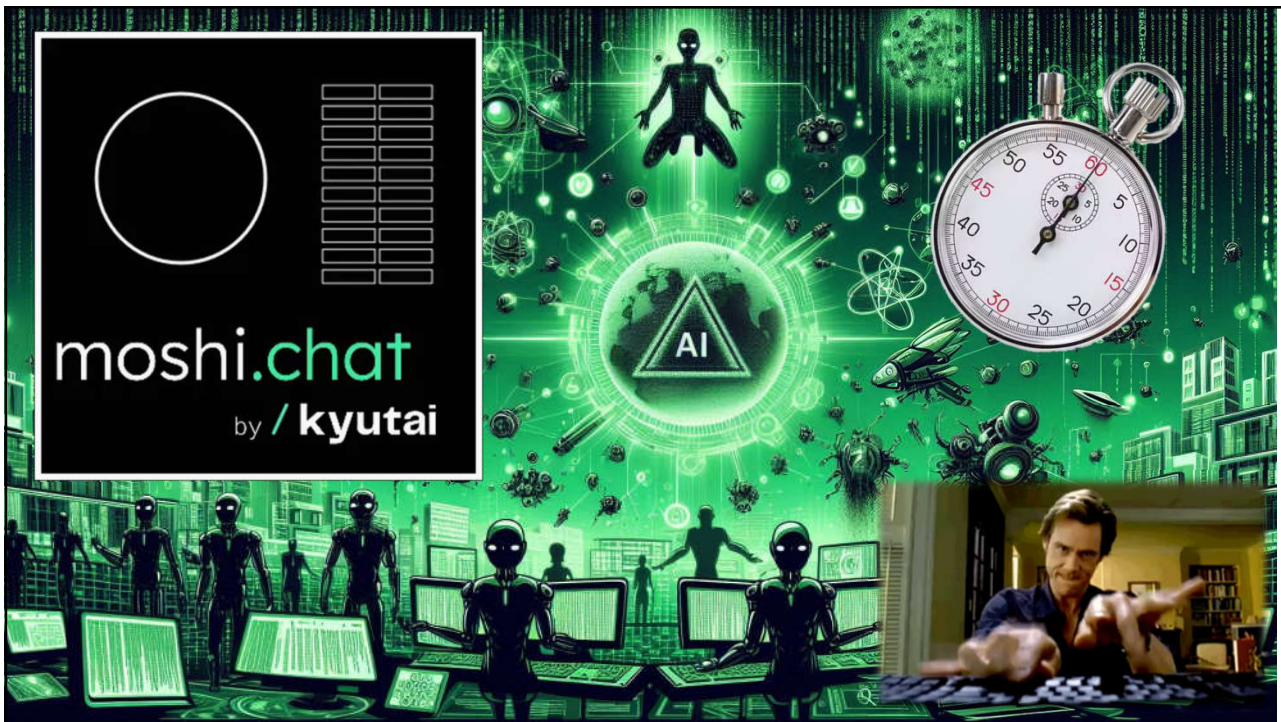
INPUT
 Text
Sound
 Pictures
 Video

OUTPUT
 Text
Sound
 Pictures

107



108



109

prosa
bladet

A ChatGPT question can cost up to **40 phone charges**.

40 opladninger af din mobiltelefon...

...det koster det potentielt, hver gang du laver en enkelt prompt til ChatGPT, og den sender dig et svar retur. Det viser en undersøgelse, som Raghavendra Selvan, der er forsker på Københavns Universitet, har lavet. Ifølge undersøgelsen "koster" en prompt i gennemsnit op til 0,19 kWh.

Forskeren har netop også lavet en "opskriftsbog", som indeholder AI-modeller, der kan klare det samme som andre modeller, men som bruger langt mindre energi.

"Udviklerne har i dag et snævert fokus på at bygge AI-modeller, der er effektive i form af, hvor præcist et resultat de kan opnå. Det svarer til at sige, at en bil er effektiv, fordi den får dig hurtigt frem, men ignorerer den mængde brændstof, den bruger," siger Raghavendra Selvan.

Klimaomkostningerne kan ifølge Selvan sagtens reduceres tidligt i designfasen og træningen af modellerne. I den nye opskriftsbog har han og kollegerne samlet modeller, der kan spare 70-80 pct. af energien i trænings- og implementeringsfasen og samtidig kun gå 1 pct. ned i ydeevne.

110

There are over 20 different Open Source alternatives to ChatGPT

- o lucidrains/PaLM-rlhf-pytorch
- o togethercomputer/OpenChatKit
- o oobabooga/text-generation-webui
- o KoboldAI/KoboldAI-Client
- o LAION-AI/Open-Assistant
- o tatsu-lab/stanford_alpaca
 - Other LLaMA-derived projects
- o BlinkDL/ChatRWKV
- o THUDM/ChatGLM-6B
- o bigscience-workshop/xmft
- o carperai/trix
- o databricks/dolly
- o LianjiaTech/BELLE
- o ethanyanjiali/minChatGPT
- o cerebras/Cerebras-GPT
- o TavernAI/TavernAI
- o Cohee1207/SillyTavern
- o h2oai/h2ogpt
- o mlc-ai/web-llm
- o Stability-AI/StableLM
- o clue-ai/ChatYuan
- o OpenLM/Lab/MOSS

The collage displays several open-source AI projects and their interfaces. Key elements include:

- TavernAI**: A chat interface with a dark theme and a 'backends' dropdown.
- minChatGPT**: A project page with a 'Crosslingual Generalization through Multitask Finetuning' header.
- Stanford Alpaca**: A project page for 'An Instruction-following' model.
- PaLM + RLHF - Pytorch**: A project page for 'Implementation of RLHF (Reinforcement Learning with Human Feedback) on top of the PaLM architecture'.
- OpenChatKit**: A project page with a 'MOSS' logo and a list of supported models like GPT-NeoXT-Chat-B.
- MOSS**: A project page with a large blue parrot logo and a 'Contents' section.
- StableLM**: A project page with a colorful parrot logo and the text 'Stability AI Language Models'.

 A red 'Deepfake' label is positioned in the top right corner of the collage. At the bottom, there is a caption in Norwegian: 'NB: Disse projekter er ikke bare en alternativ frontend til OpenAI eller benytter OpenAI's APIs'.

111

Det tager under 10 minutter at lave en deep fake video som den her..

Deepfake



112



113



114



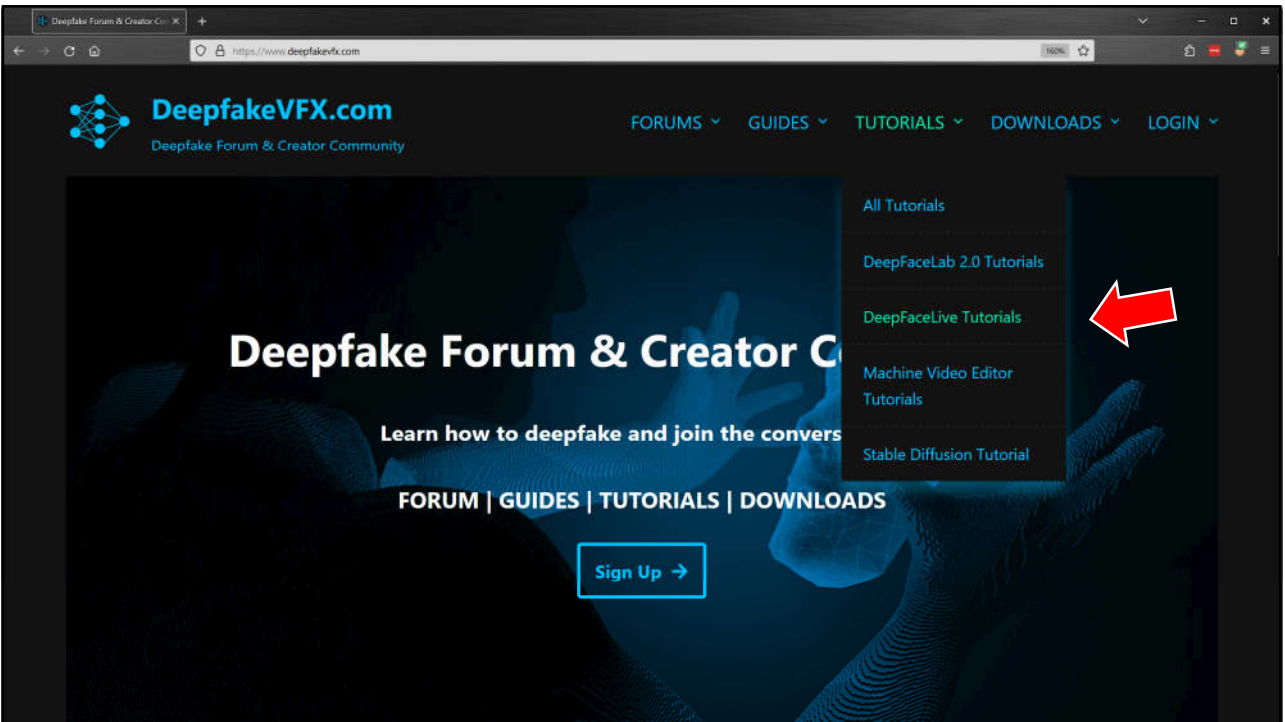
115



116




117



118

Højeste opløsning og detaljerings grad med "pre-trained" ansigts profiler..



Hvis man vil lave realistiske realtime deepfakes af en person i dag skal man kun bruge et videoklip hvor personen optræder i og en A.I. der finder personens ansigt i forskellige vinkler og lave en ansigts profil.

119



120



121



122