

E-1337 SCRIPT KIDDIE

A script kiddie is a person who uses existing computer scripts or codes to hack into computers, lacking the expertise to write their own.

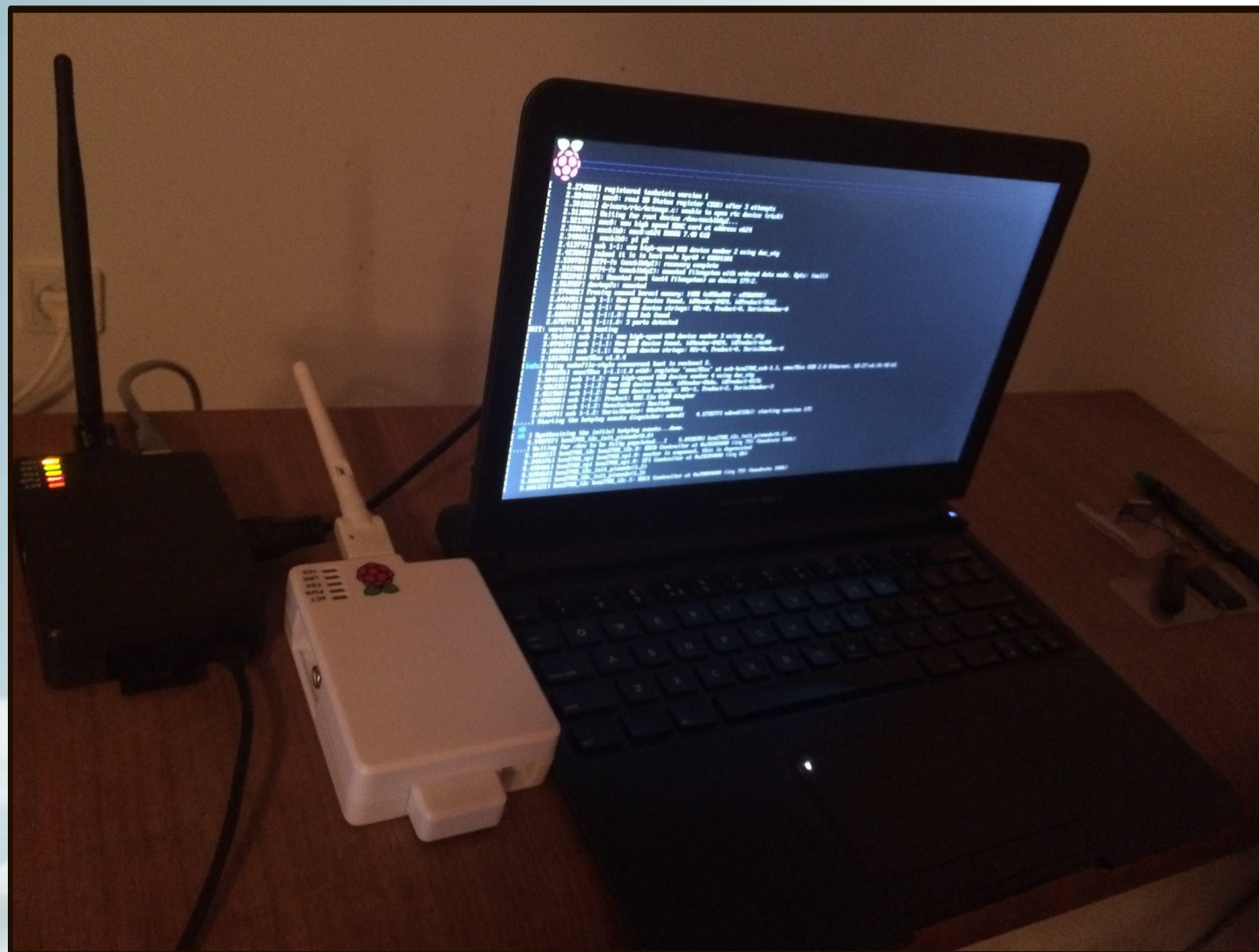


Keld Norman
Dubex A/S
Security Consultant
kno@dubex.dk

Hvem er jeg..



Keld Norman
kno@Dubex.dk



Dubex:

Dubex:

Dubex:



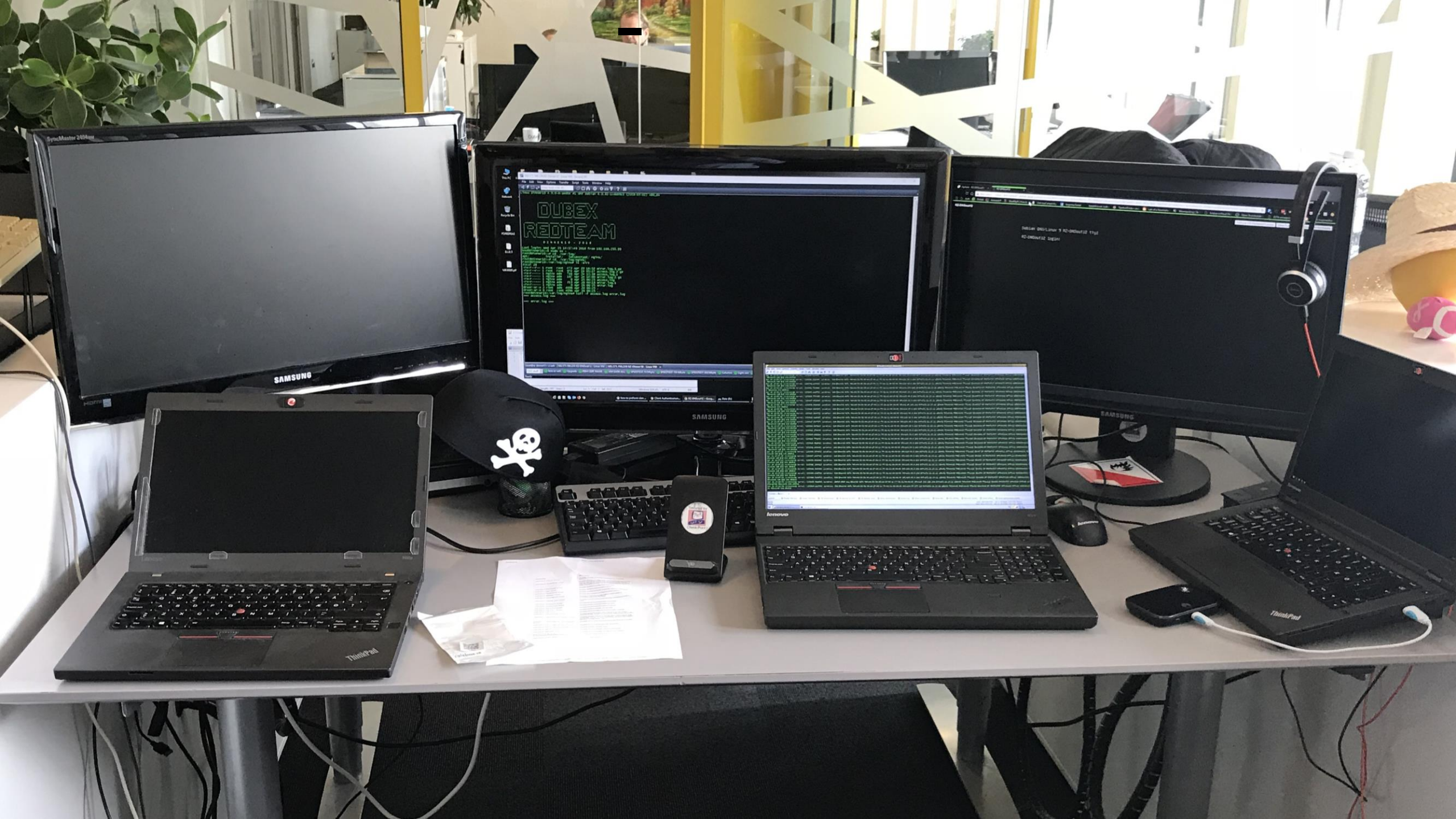
Dubex
Incident
Response
Team



Coding PIRATES

<https://codingpirates.dk/>





5 Live hacks...

Gallium & en hængelås..

- Konboot
- Rubberducky
- Mousejack
- Evil ninja usb kabel
- Apple bleee
- Tøm Dankortsautomaten

Hvordan har låsen det ?



USB NINJA & USB KILLER
DECEMBER 2018



<https://usb ninja.com/shopusb ninja> (koster i dag mellem 1100-2800 DKK)

MOUSEJACKING



Rubber Duck Attack



Apple Bleee Attack

er logget på Wifi
med en WPA2 kode

SCAN ME



PS: JEG KAN OGSÅ SE DIT TELEFON
NUMMER HVIS DU PRØVER AIRDROP



Hacker

GALLIU

AliExpress™

I'm shopping

Home > All Categories > Toys & Hobbies > Nov



Sign in | Join My AliExpress



10/20/50g 99.99% Pure Ga Gallium Metal Toy Educational Diy Toy Low Melting Point Metal Magic Magician Supplies

5.0 ★★★★★ (1 votes)

Store: smilewill 01 Store

US \$8.83 - 25.02

Gallium

atomic number

31

symbol

Ga

electron configuration

[Ar]3d¹⁰4s²4p¹

name

gallium

atomic weight

69.723

acid-base properties of higher-valence oxides

crystal structure

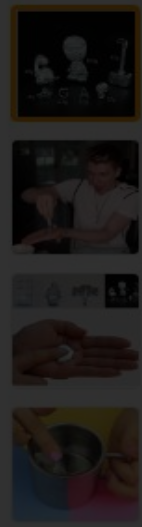
physical state at 20 °C (68 °F)

Other metals

Solid

Orthorhombic

Equal relative strength



45g

10g

2.5

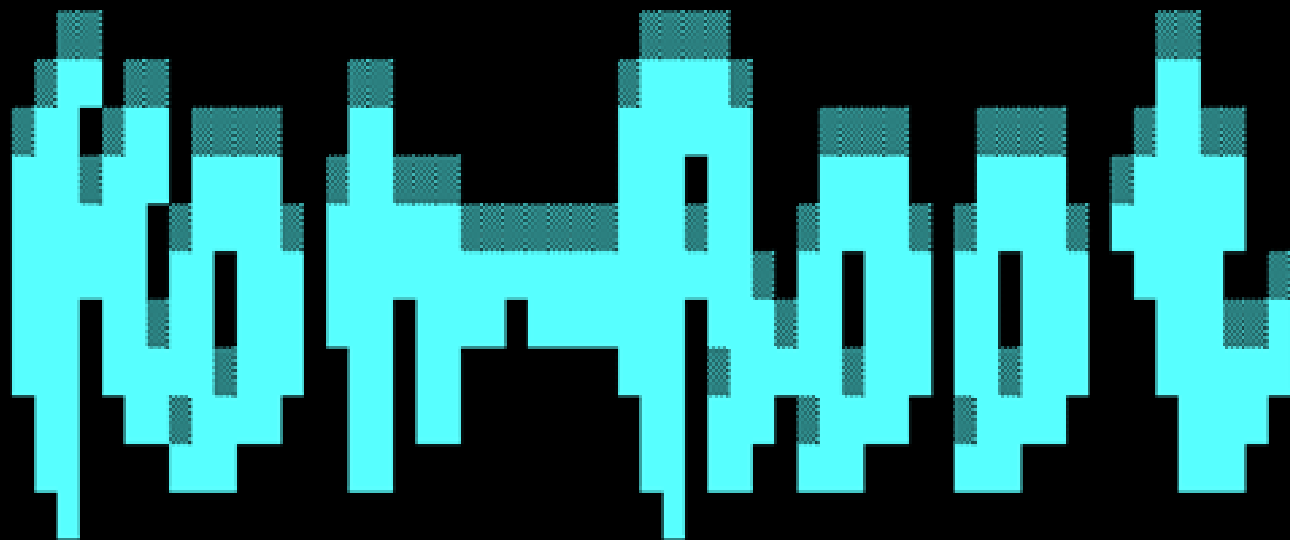


Toy Educational Diy Toy
plies

- 3 atomic weight
- acid-base properties of higher-valence oxides
- crystal structure
- physical state at 20 °C (68 °F)

- Solid
- Equal relative strength

FYSISK ADGANG: Kon-Boot



by Piotr Bania
www.kryptoslogic.com

BYPASS LOGIN WINDOWS & MAC

- » Kon-Boot ver. 1.0 - ready! h4x0Rin uH?
- » This software is freeware for not commercial usage!
- » Checking SMAP BIOS entries ...
- » BIOS seems to be OK.
- » Booting up! - EOT

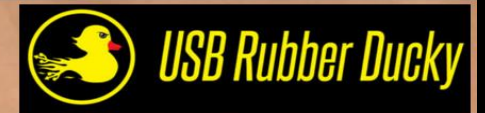
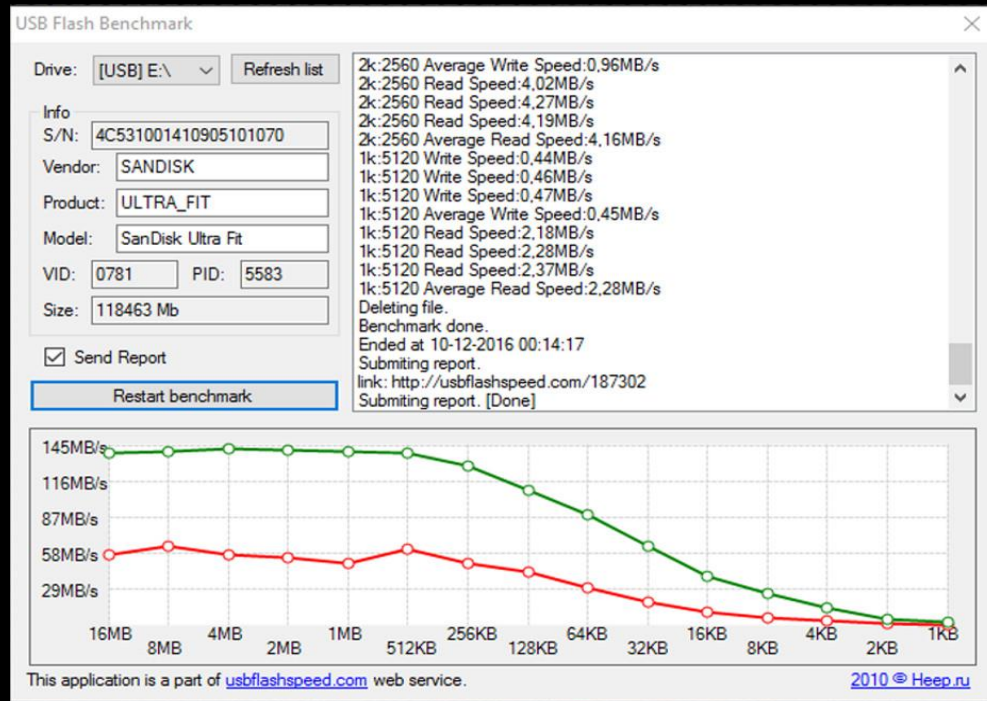


<http://www.kon-boot.com>





Rubber Ducky Attack



#HAK5 #RubberDucky

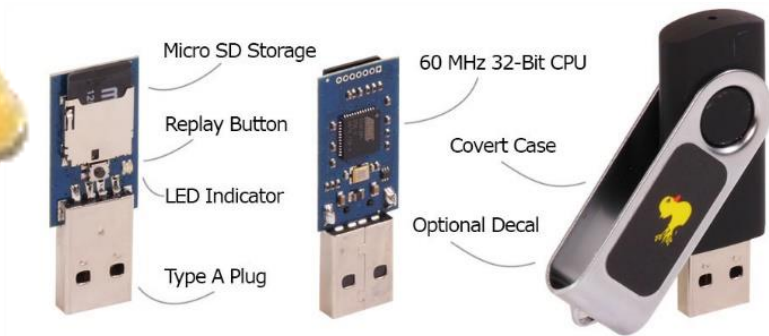
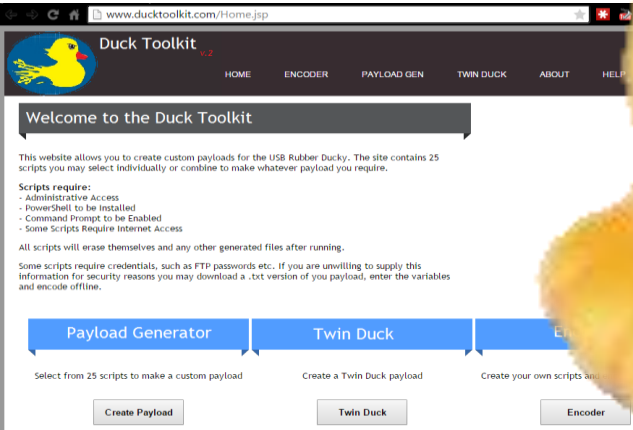


Fysisk adgang.



The "Rubber Ducky Attack"

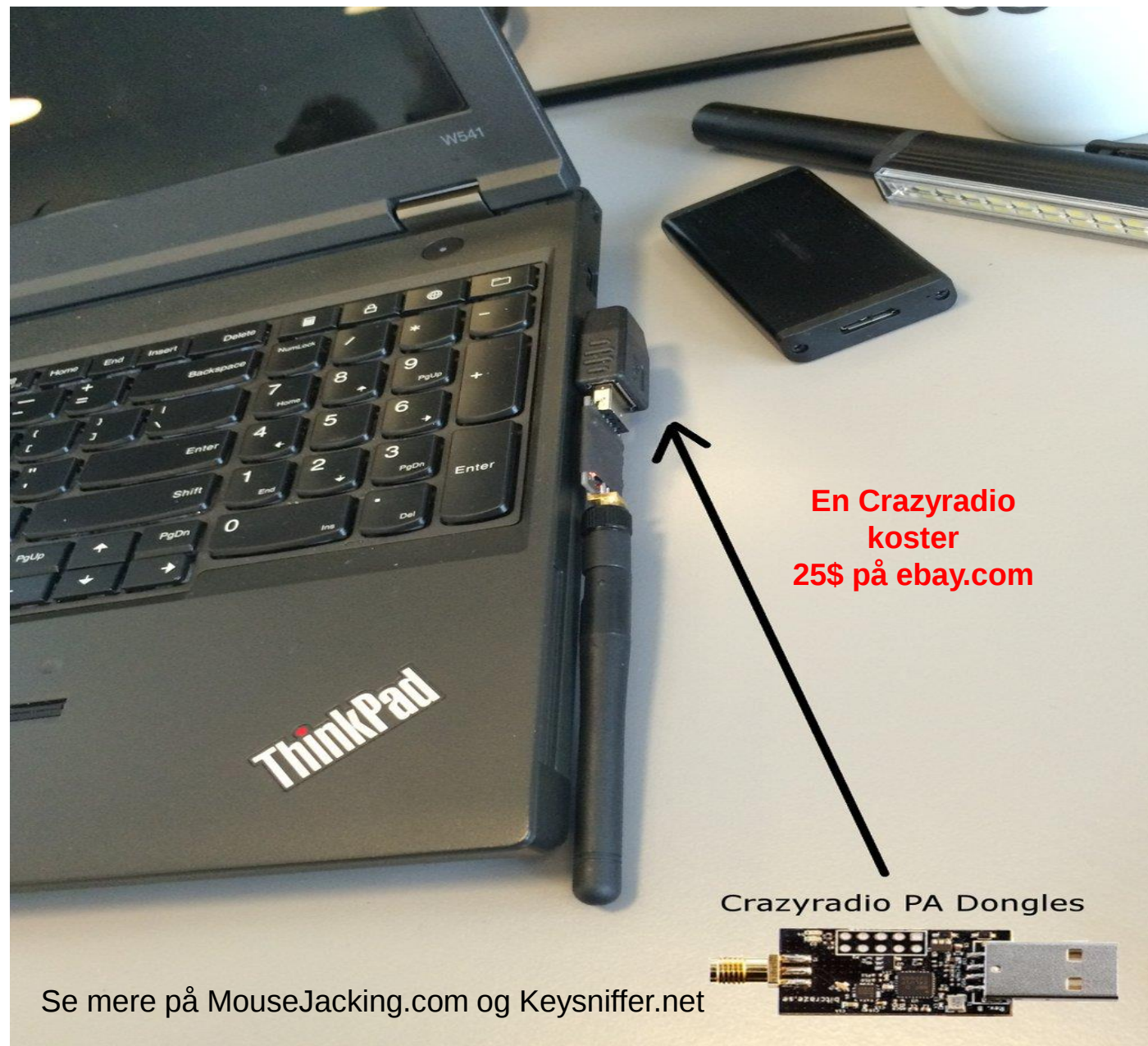
Reconnaissance:	Exploitation:	Reporting:
Computer Information	Find and Upload File (FTP)	Save Report
User Information	Disable Firewall	FTP Report
USB Information	Add User	Email Report
Shared Drive Information	Open Firewall Port	
Program Information	Start Wi-Fi Access Point	
Installed Updates	Share C:\ Drive	
User Document List	Enable RDP	
Basic Network Information	Create a Reverse Shell	
Network Scan	Local DNS Poisoning	
Port Scan	Delete a Windows Update	
Copy Wireless Profile		
Take Screen Captures		
Copy FireFox Profile		
Extract SAM File		



Har du har sådan en "dongle" i din computer ?



Mulig hacker afstand: 200 meter



En Crazyradio
koster
25\$ på ebay.com

Crazyradio PA Dongles

Se mere på MouseJacking.com og Keysniffer.net

MOUSEJACKING



USB NINJA & USB KILLER

DECEMBER 2018

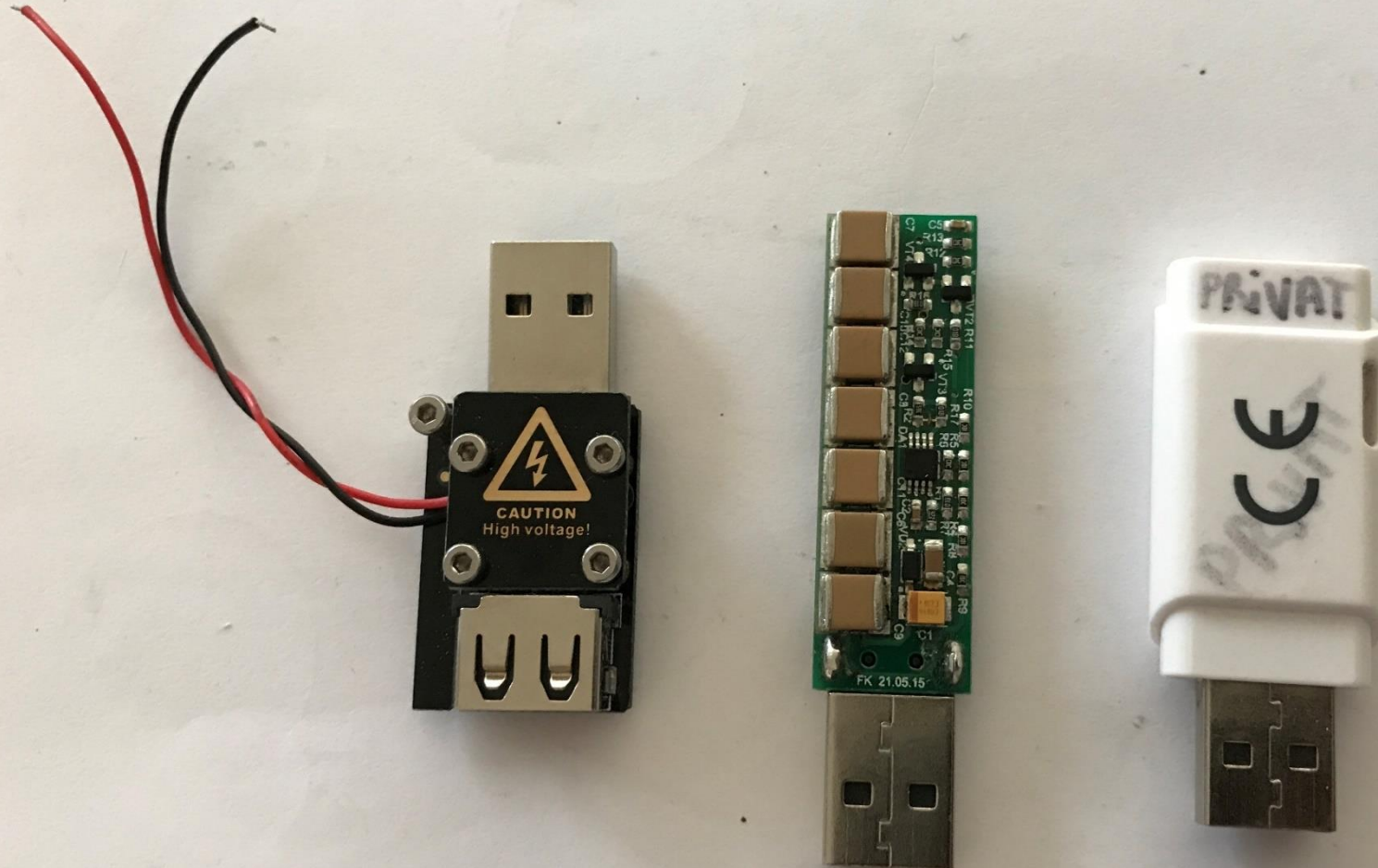


<https://usb ninja.com/shopusb ninja> (koster i dag mellem 1100-2800 DKK)

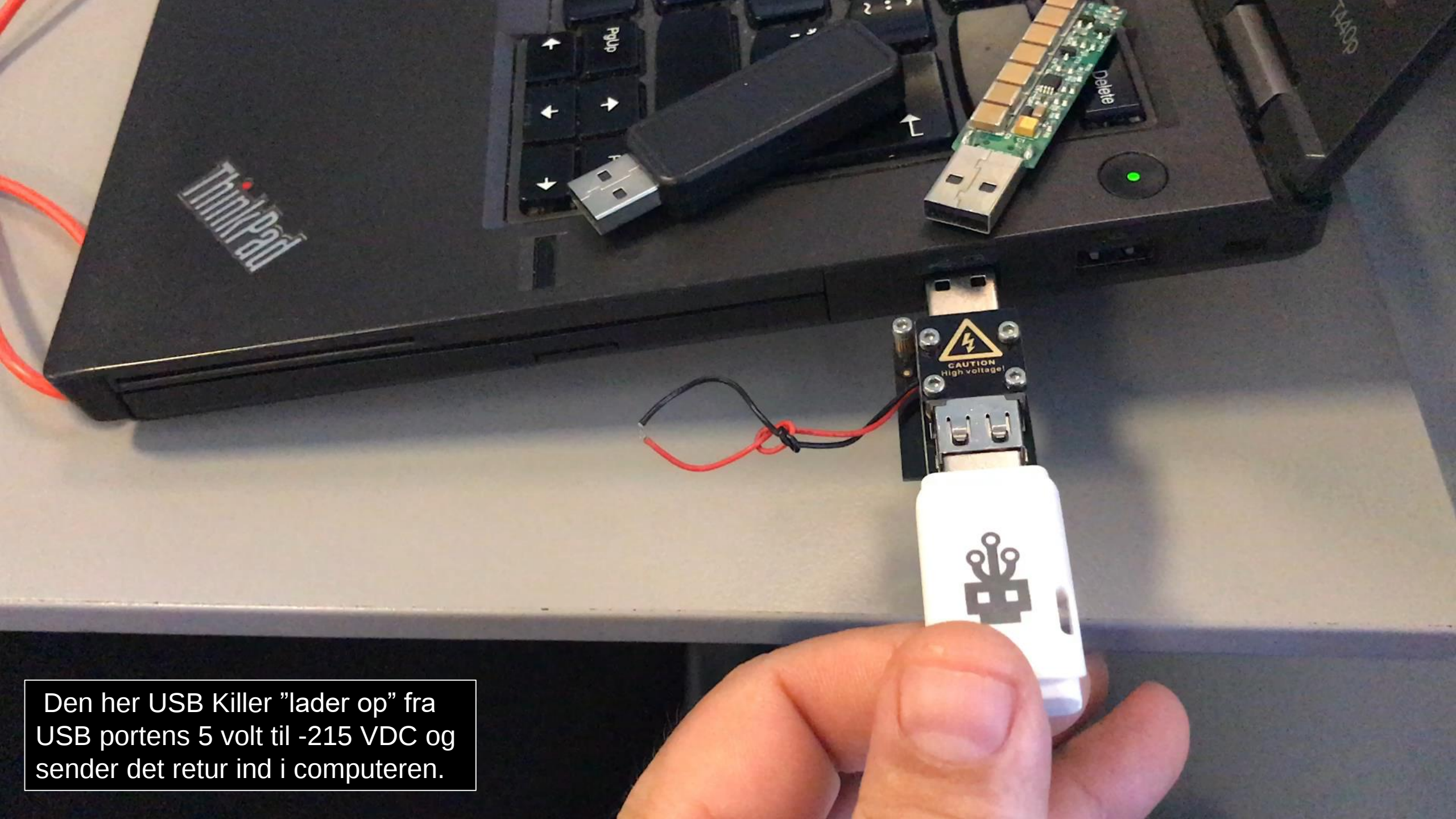
USB NINJA



USB KILLER



MARTS 2015



Den her USB Killer "lader op" fra USB portens 5 volt til -215 VDC og sender det retur ind i computeren.



USB KILL

PRO KIT

ADAPTORS

TEST SHIELD

FAQ

LATEST TESTS

COMMUNITY

CONTACT

Account



USB KILL PRO KIT

SALE €77.35 ~~€85.95~~

VERSION

QUANTITY

Anonymous ▾

- 1 +

ADD TO CART**Each USB Kill Pro Kit includes:**

- ♥️ **10% Discount off individual prices:** already applied!
- ♥️ **Free Worldwide Shipping:** Via Worldwide Rapid Post
- ♥️ **Purchase Protection:** Money Back Guarantee
- ♥️ **Private Encrypted Checkout:** Secure & Discrete

Apple Blee Attack

Hvis du er logget på Wifi
med en WPA2 kode

SCAN ME



Wi-Fi-adgangskode



Vil du dele Wi-Fi-adgangskoden til
"DubexTestLab" med "Din Chef"?

Del adgangskode

A man in a blue shirt is shown from the side, interacting with an ATM. The ATM screen displays logos for JCB, Diners, Visa, and Mastercard. The machine is mounted on a brick wall. The text 'Sydbank' and 'Ind- og udbetaling' is visible at the top of the machine.

Hvordan tømmer man en pengeautomat ?

Et andet eksempel på hacking via fysisk adgang... ☺





4000 12 >

4000

GOOD
THRU 1.

B. PARKER

1510

A

GlobeCard
MasterCard

Credit



KELD BRIAN NORMAN



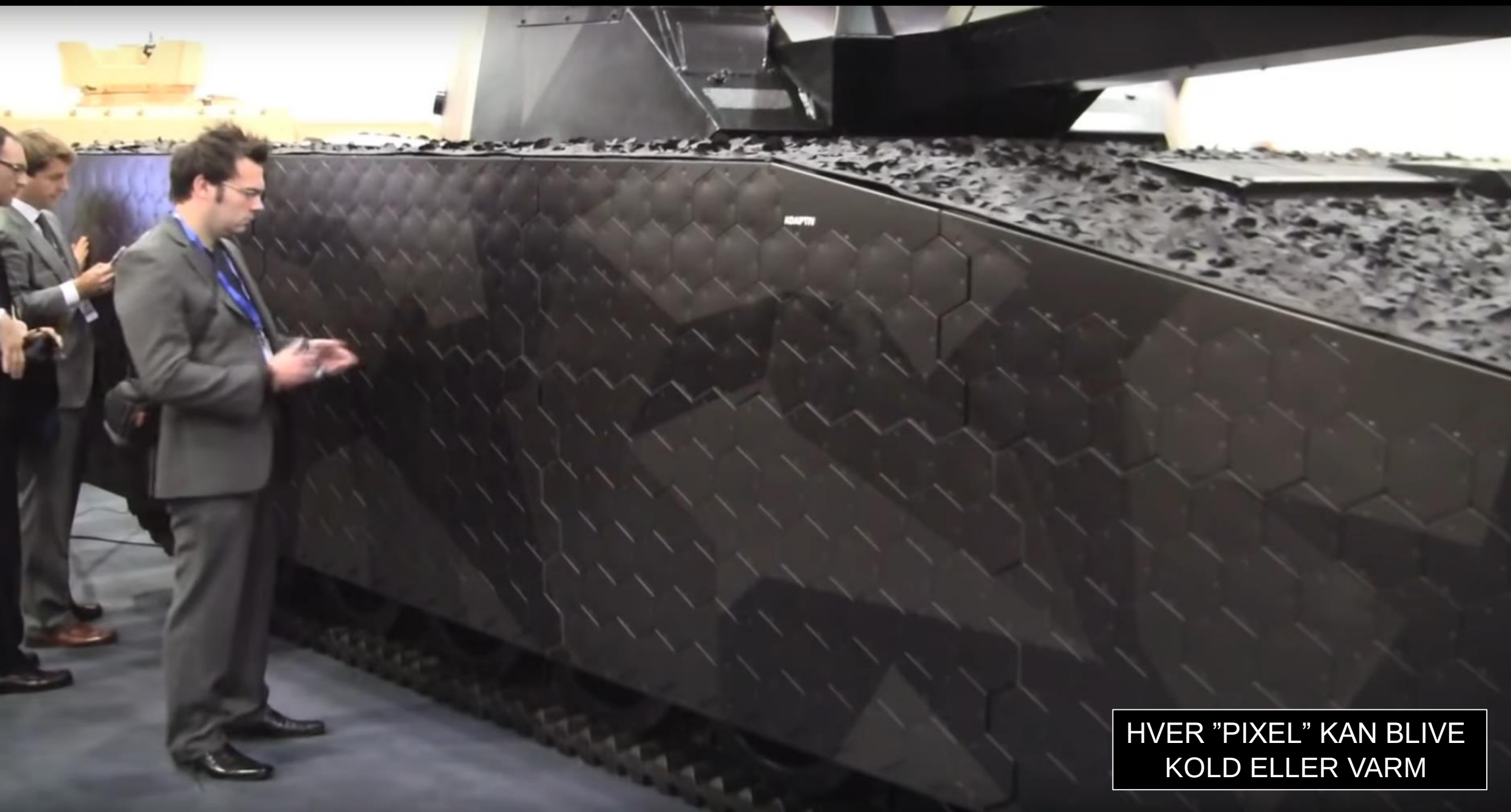
Der aflæses hele kortnummeret, udløbsdatoen og de 10 sidste transaktions størrelser (og valuta)

ATCounter	date	time	amount	currency	terminal country
41	14.08.2018	15:49:37	585.00	DKK	
40	13.08.2018	16:06:56	38.86	USD	
39	13.08.2018	13:01:05	25.20	USD	
37	08.08.2018	17:00:42	31.02	USD	
35	08.08.2018	09:18:24	16.60	GBP	
34	08.08.2018	06:54:00	56.00	DKK	
33	08.08.2018	06:40:11	52.00	DKK	
32	04.08.2018	15:10:28	5.00	SEK	
31	04.08.2018	13:41:30	152.00	SEK	
30	02.08.2018	14:41:52	243.00	SEK	



BAE SYSTEMS "Adaptiv" cloaking system



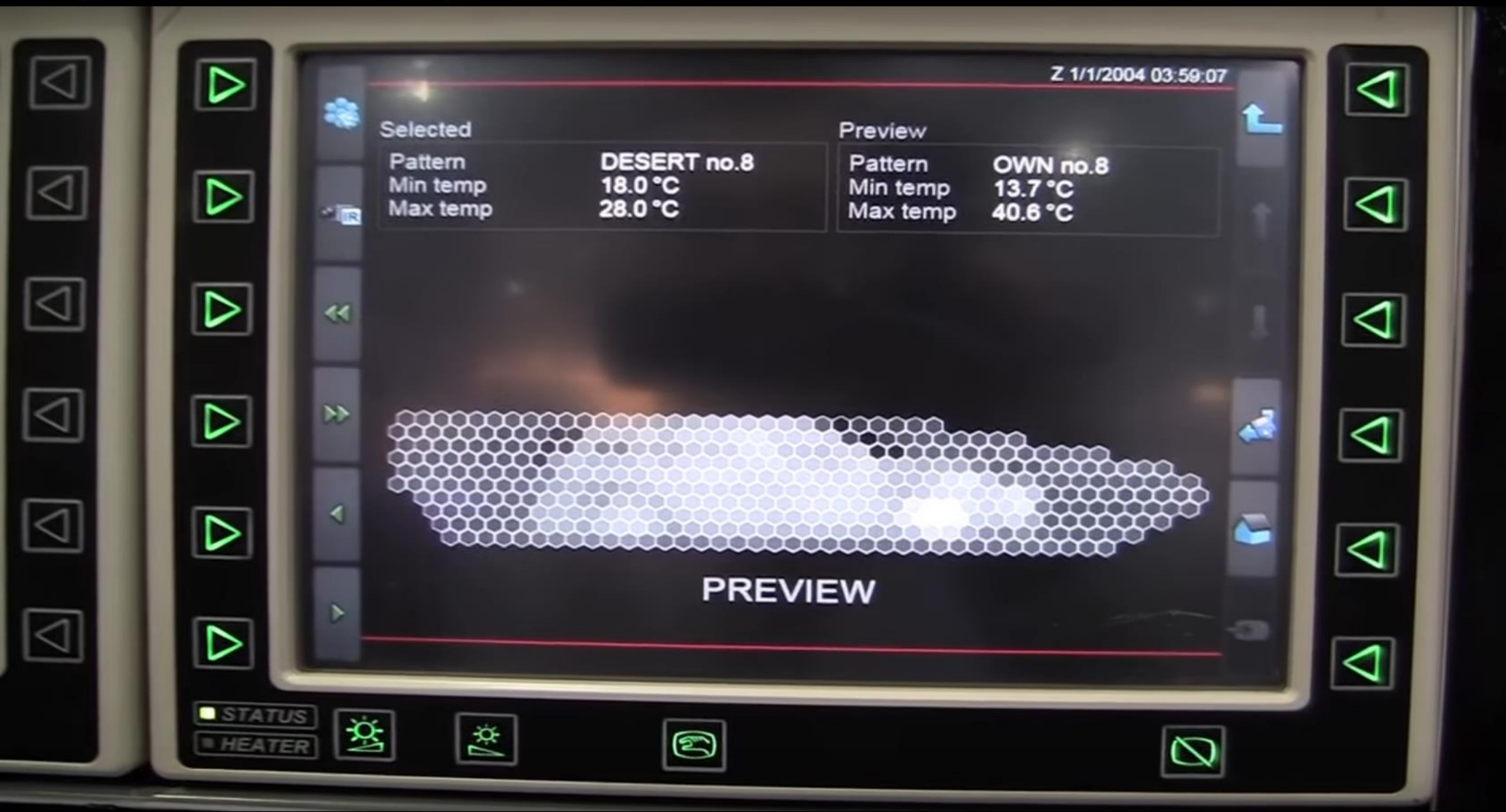


HVER "PIXEL" KAN BLIVE
KOLD ELLER VARM





BAE Systems' Adaptiv infra-red 'invisibility cloak' for military vehicles





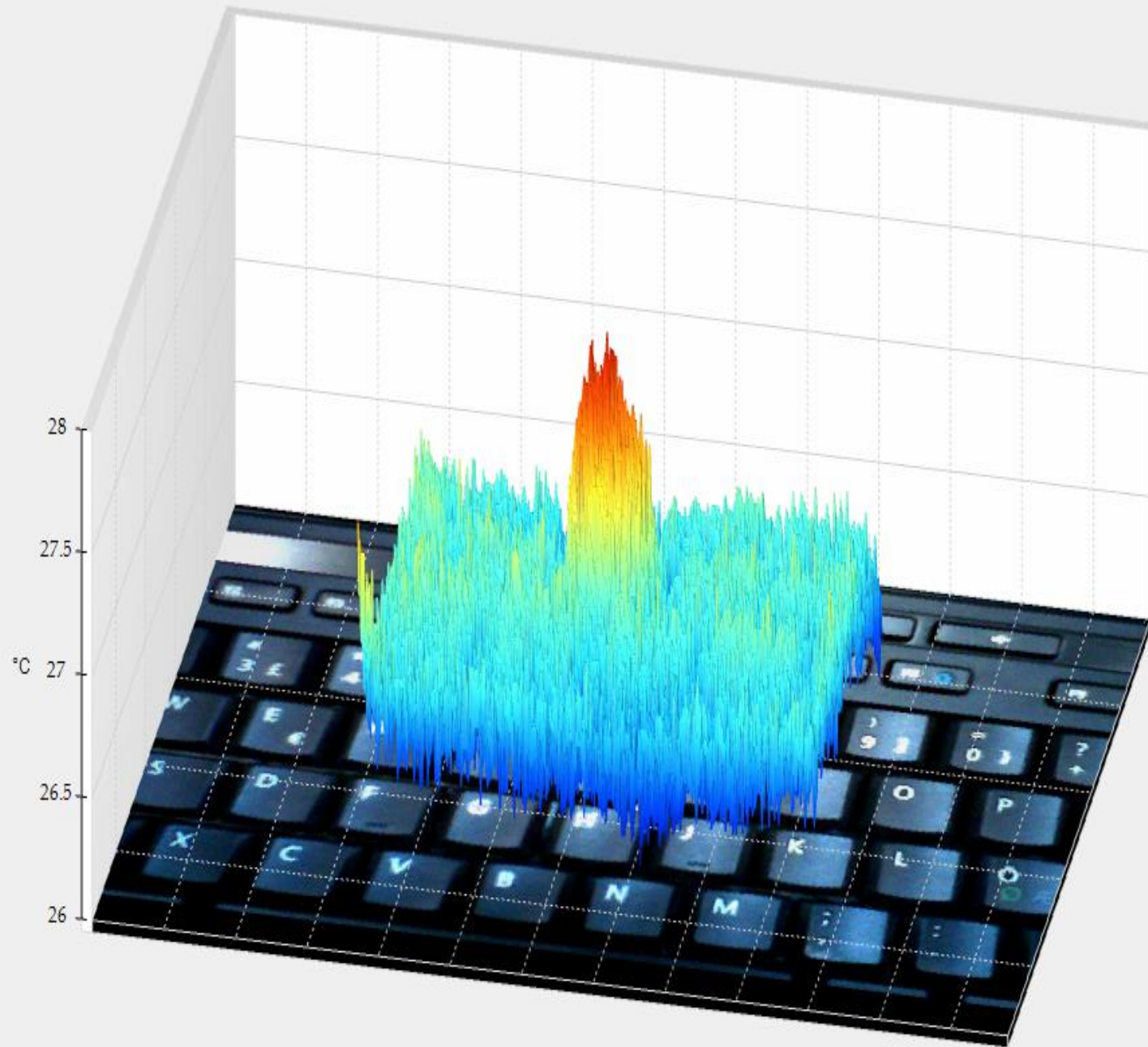
ET FLIR (FORWARE-
LOOKING
INFRARED)
KAMERE KAN
KØBES PÅ EBAY I
DAG FOR OMKRING
3000,- DKK

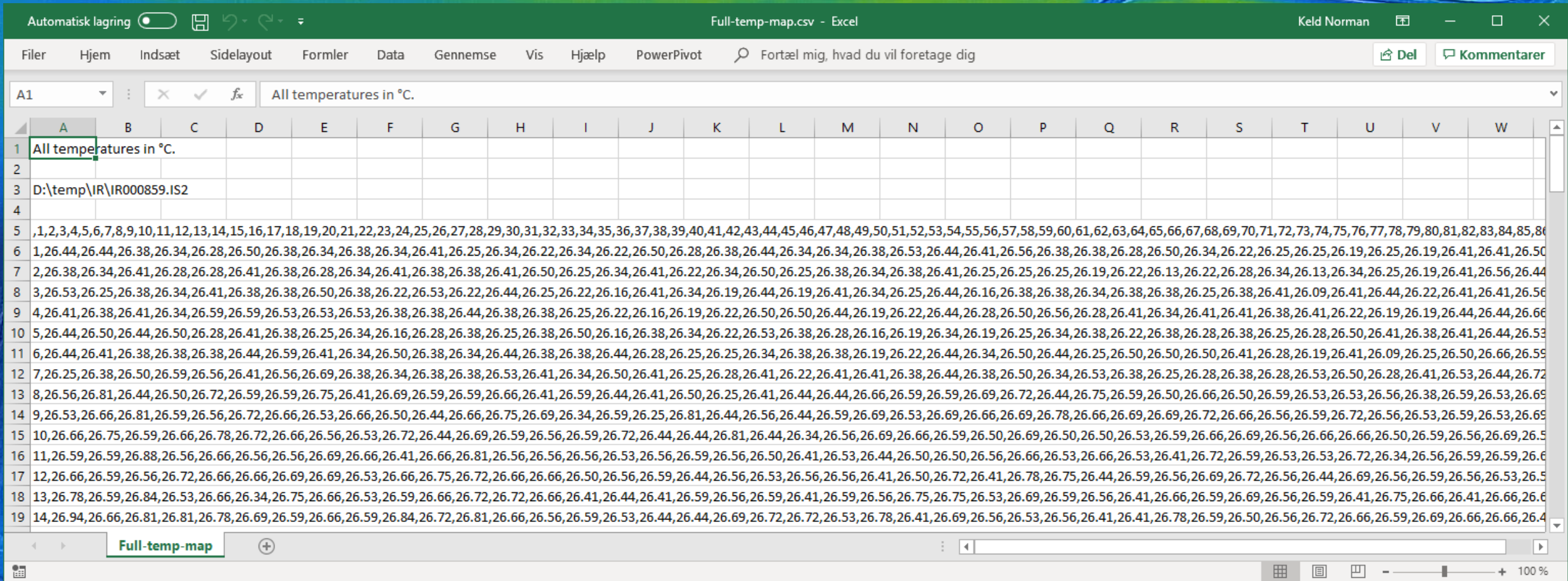




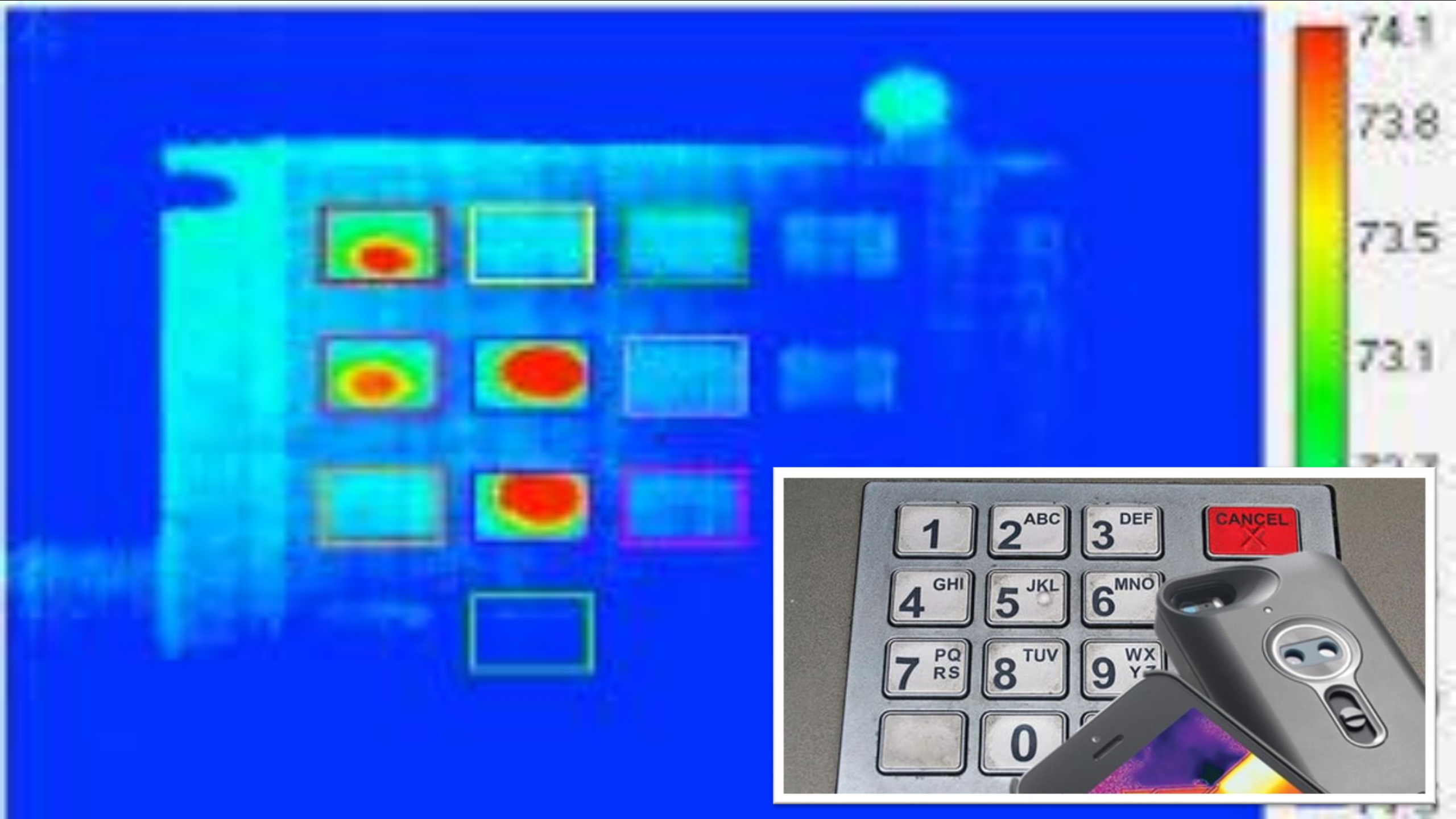
Vi testede det samme på en iPhone







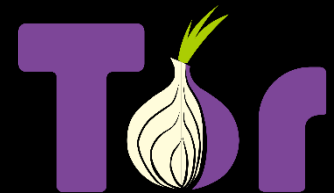




Hvad er TOR/Onion/Deep Web?



Det frie
browser
valg 😊



<https://www.torproject.org/>

Her er alle
.onion siderne



TOR
Browser

CC Autoshop

Welcome to the CC autoshop! This section allows you to search for credit cards or fulls in the most convenient way possible. Be careful when using checkers, as they can have side effects on the cards.

Buy Cards

My Purchased Cards

BIN: City: State: Zip: Country:

DOB: SSN: Birth Year: to Price: to

Seller: Bank: Type:

Credit: Level:

	BIN	Exp.	Seller	Name	Zip	City	State	Country	DOB	SSN	Price
☐	405268	11 / 20	exotic2015 (80%)	Serry ...	2300	Copenhagen	Copenhagen	Denmark	N/A	N/A	\$25.00
☐	457198	1 / 20	vespacc (85%)	Henrik...	8660	SKANDERBORG	SKANDERBORG	Denmark	N/A	N/A	\$25.00
☐	457134	7 / 17	leaguemode (-9%)	Marian...	9280	Storvorde	dk	Denmark	N/A	N/A	\$12.00
☐	457135	8 / 17	leaguemode (-9%)	Lars ...	2000	Verdby Tjørrev...	lagelse	Denmark	N/A	N/A	\$12.00
☐	457136	7 / 17	leaguemode (-9%)	Mysse ...	1000	Arhus C	Other	Denmark	N/A	N/A	\$12.00
☐	402620	10 / 17	leaguemode (-9%)	Mikkel...	2100	København	Other	Denmark	N/A	N/A	\$10.00
☐	457179	7 / 17	leaguemode (-9%)	Jens B...	8520	Lystrup	Other	Denmark	N/A	N/A	\$12.00
☐	457176	8 / 17	leaguemode (-9%)	Rikke ...	4200	7400 Herning	Other	Denmark	N/A	N/A	\$12.00
☐	457107	5 / 20	leaguemode (-9%)	Kasper ...	0000	7620 Skjern	Other	Denmark	N/A	N/A	\$12.00
☐	457131	9 / 18	leaguemode (-9%)	Xavier ...	2660	Alle ... b ... k ...	Other	Denmark	N/A	N/A	\$12.00
☐	457132	9 / 17	leaguemode (-9%)	J. Jørgen...	4300	Holbæk	Other	Denmark	N/A	N/A	\$12.00
☐	457135	1 / 19	leaguemode (-9%)	Ole An...	5492	Vissenbjerg	Other	Denmark	N/A	N/A	\$12.00
☐	457133	4 / 19	leaguemode (-9%)	Frank ...	2800	Kgs. Lyngby	Other	Denmark	N/A	N/A	\$12.00
☐	457132	4 / 18	leaguemode (-9%)	Mikkel...	5700	Svendborg	Other	Denmark	N/A	N/A	\$12.00
☐	457153	6 / 18	leaguemode (-9%)	Michae...	2000	Frederiksberg	Other	Denmark	N/A	N/A	\$12.00
☐	457181	11 / 17	leaguemode (-9%)	L. Man...	2500	Valby	Other	Denmark	N/A	N/A	\$12.00
☐	457171	5 / 19	leaguemode (-9%)	Thomas...	4140	Borup	Other	Denmark	N/A	N/A	\$12.00
☐	457181	2 / 18	leaguemode (-9%)	Nicola...	2100	København	Other	Denmark	N/A	N/A	\$12.00
☐	457191	4 / 19	leaguemode (-9%)	Louis ...	0000	Frederne	Sorvag	Denmark	N/A	N/A	\$12.00

PIN: [Forgot PIN](#)

Dankort til salg
på TOR nettet..

ONIONSEARCH

[INDEX](#) [FAQ](#) [JSON](#) [SRC](#) [LANGUAGES](#) [STATS](#) -- 4131 fresh onions, 57 in the last 24 hours.

☐ show ignored hosts ☐ show never seen ☐ on-line only (☐ any ☐ genuine ☐ fake)

☐ search titles only ☐ show subdomains ☒ match phrase

search: search for title, email, bitcoin addr or onion domain.

[G] Genuine, [F] Fake clone site | Domain status is **alive**, **problems** or **down** | Showing 500 of **15522** results. [JSON](#)

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 ><((°>

Onion	Title	Added	Visited At	Last Up
(i) tordir	.onion The rougher the seas, the smoother we sail.	2 hr	2 hr	2 hr
(i) pumpdu	.onion Crypto Pump & Dump Bot	3 hr	an hr	an hr
(i) 4wphms	ondsruco... Encode / Decode	3 hr	21 min	21 min
(i) hacker	.onion The rougher the seas, the smoother we sail.	6 hr	21 min	21 min
(i) yin7qx	.onion	6 hr	15 min	15 min
(i) pcfly3	.onion 401 Authorization Required	7 hr	18 min	18 min
(i) retoxm	.onion RETOXSTORE	7 hr	21 min	21 min
(i) amusew	vy2q3gqb...	8 hr	an hr	8 hr
(i) amuses	q6xf6f4ua... AmuseCosy	8 hr	an hr	8 hr
(i) jna6su	ix6pqbh... HonestCocaine? -The most trusted online bulk cocaine seller in the world	8 hr	7 min	7 min
(i) gladia	.onion GladiatOR - Índice	8 hr	21 min	21 min
(i) 2222li	.onion ONIONLIST - SAFE .ONION LINKS LISTING	8 hr	21 min	21 min
(i) hidwkl	.onion The Original Hidden Wiki	8 hr	7 min	7 min
(i) glardz	ifnxd5yte... CHAT BRASIL PROIBIDO	8 hr	22 min	22 min
(i) 4dcsjn	de3avbgw...	8 hr	51 min	51 min
(i) geuvpa	lnzn2lm7i... Site Hosted by Freedom Hosting Reloaded	8 hr	2 hr	3 hr

We produce and modify all products we sell in our Workshops in US and Europe.
We ship all items with DHL, UPS, TNT, FedEx and USPS with traceable tracking number.

Bestsellers



860-960 MHz Long-Range RFID Reader

\$650.00

ADD TO CART



Diebold 3550 - Skimmer Kit

\$1,500.00

ADD TO CART



Gas Pump Skimmer

\$850.00

ADD TO CART



GSM Data Receiver

\$1,400.00

ADD TO CART



Ingenico iWL250 Wireless Skimmer

\$900.00

ADD TO CART



MSR-X6 Bluetooth Magnetic Stripe Card Reader / Writer

\$300.00

ADD TO CART



NCR SelfServ 22 - Skimmer Kit

\$1,500.00

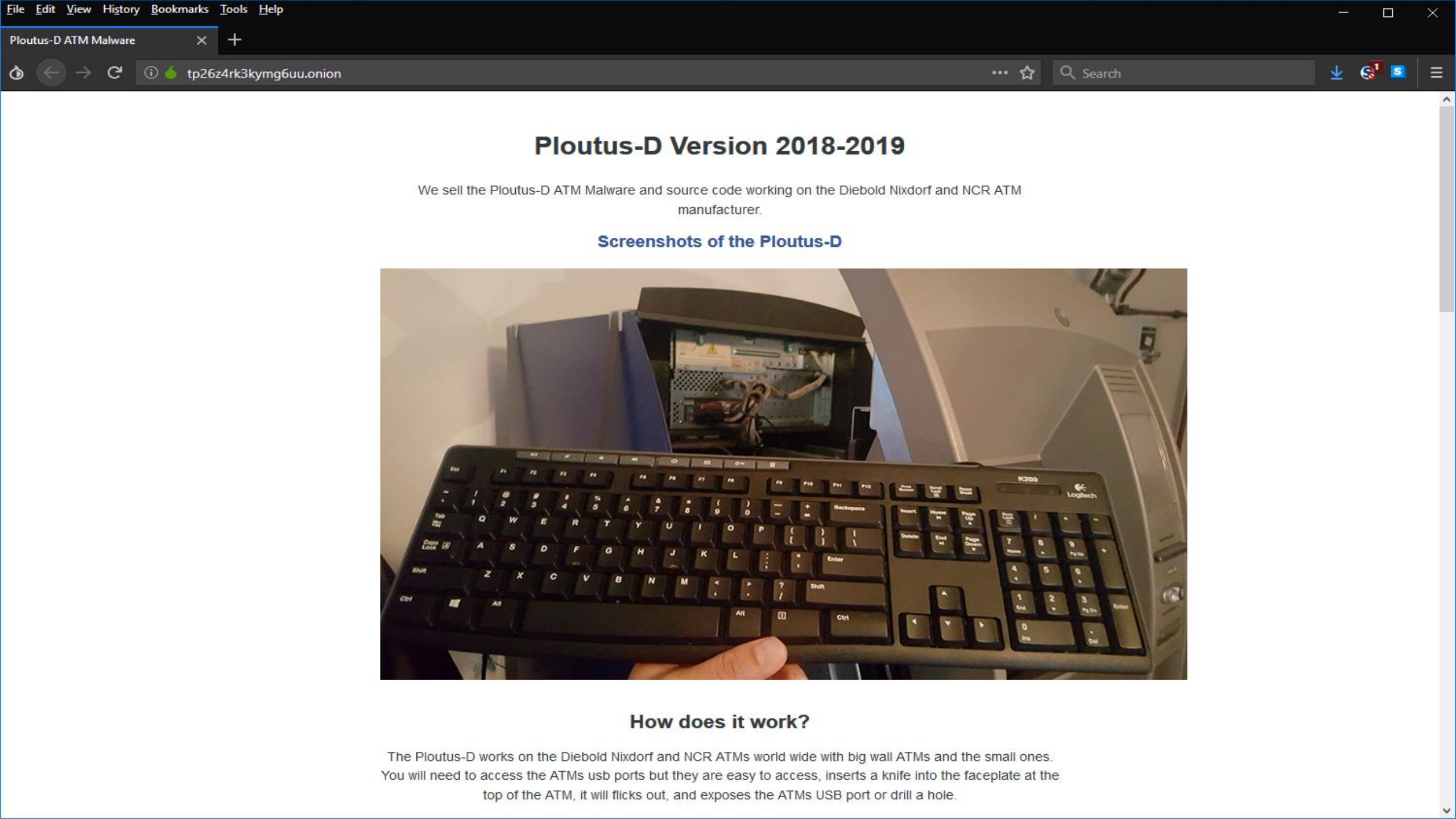
ADD TO CART



Ploutus-D ATM Jackpot

\$6,500.00

ADD TO CART



Ploutus-D Version 2018-2019

We sell the Ploutus-D ATM Malware and source code working on the Diebold Nixdorf and NCR ATM manufacturer.

Screenshots of the Ploutus-D



How does it work?

The Ploutus-D works on the Diebold Nixdorf and NCR ATMs world wide with big wall ATMs and the small ones. You will need to access the ATMs usb ports but they are easy to access, inserts a knife into the faceplate at the top of the ATM, it will flicks out, and exposes the ATMs USB port or drill a hole.

Tøm en pengeautomat for kun 42.867,- DKK

Guide og
malware
køber man
bare på TOR
nettet

File Edit View History Bookmarks Tools Help

Ploutus-D ATM Malware x +

tp26z4rk3kymg6uu.onion

Price list

Package #1	Manuals/Video's/Instructions	Price
Ploutus-D ATM Malware [latest]	Yes included	6.5k
Package #2	Manuals/Video's/Instructions	Price
Ploutus-D ATM Malware [latest] + Full source code	Yes included	15k

My email: darkexpress@torbox3uiot6wchz.onion

FAQ

How do I send you an email?

My email is darkexpress@torbox3uiot6wchz.onion Create an email account at: <http://torbox3uiot6wchz.onion/>

What is in the manuals?

The tools you need, Extra Instructions, Tricks and AV bypass (just in case)

How long does the ATM attack take?

Depending on small or wall ATM but usually around **Minimum of 3 minutes max 10.**

Does it work world-wide with all ATM manufacturers?

It works world-wide but it does only work with the Wincor Nixdorf and NCR ATMs.

Does it bypass the AV?

Yes it does, most of the ATMs doesn't have AVs but there will be a manual include to bypass just in case.

.. det tager under 10 minutter at tømme automaten for penge



Den "pakken" man køber indeholder instruktioner i hvordan man skifter mange forskellige typer ATM/Dankorts automater ad.



Dette eksempel viser hvor man skal bore i en automat af samme type som dem vi bruger i Danmark



Netherlands
(Holland)



Når hullet er boret er der direkte adgang til USB indgangen



KORT



KONTANTER



d. Ideal for low-cost

Shipping | See details

ges. ?



A woman with short dark hair, wearing a purple and yellow patterned top, is seated in a courtroom. Her face is partially obscured by a black rectangular redaction box. In the background, several other people are visible, including a man in a suit and another man in a striped sweater. The courtroom has wood-paneled walls and a wooden bench.

HUSK: Forbrydelser betaler sig ikke

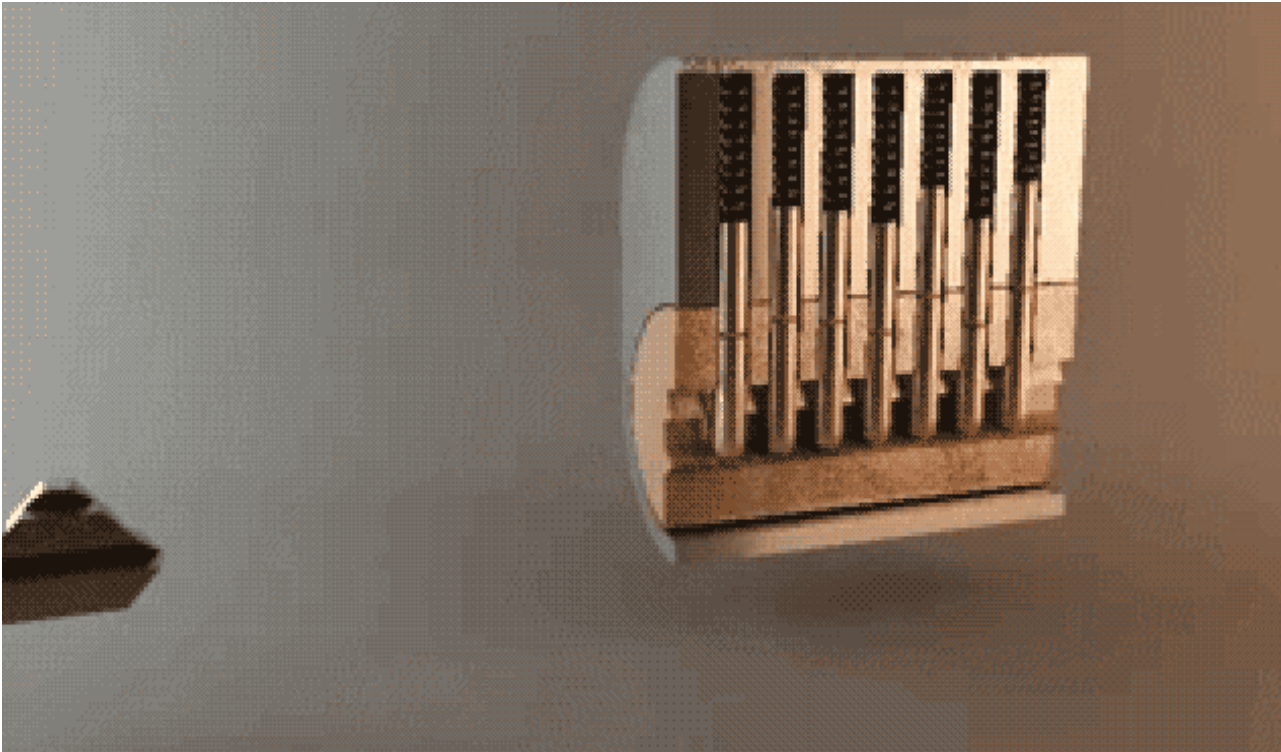
(hvis de bliver opdaget)



!!! VIGTIG NOTE TIL KELD !!!
HUSK AT SKJULE DEN HER SLIDE INDEN PRÆSENTATIONEN VISES

AND NOW BACK TO
OUR REGULARLY
SCHEDULED
PROGRAMMING

Knock / bump keys



Nøgle filet ned

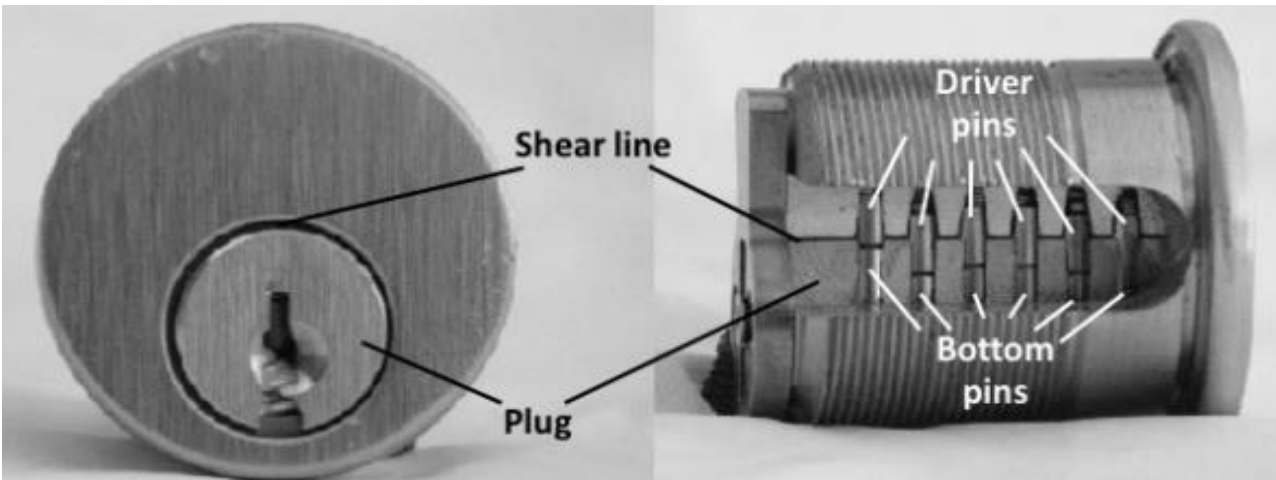


"Hammer"

En svag nøgle



En sikker nøgle



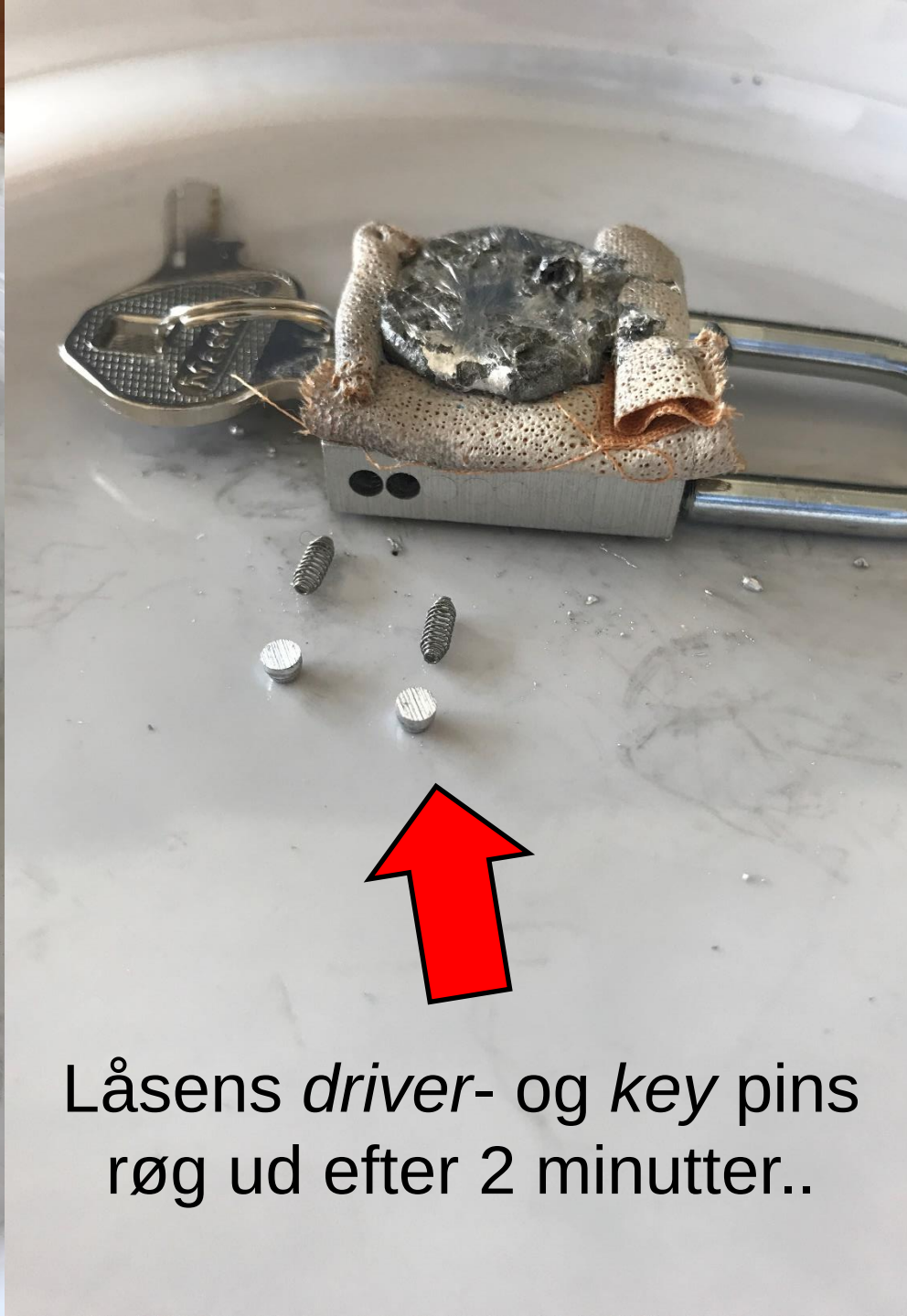




**Varm Gallium
(over 29,7646 °C)**

**Plaster som
barrierer så
Galliummet ikke
falder ned**

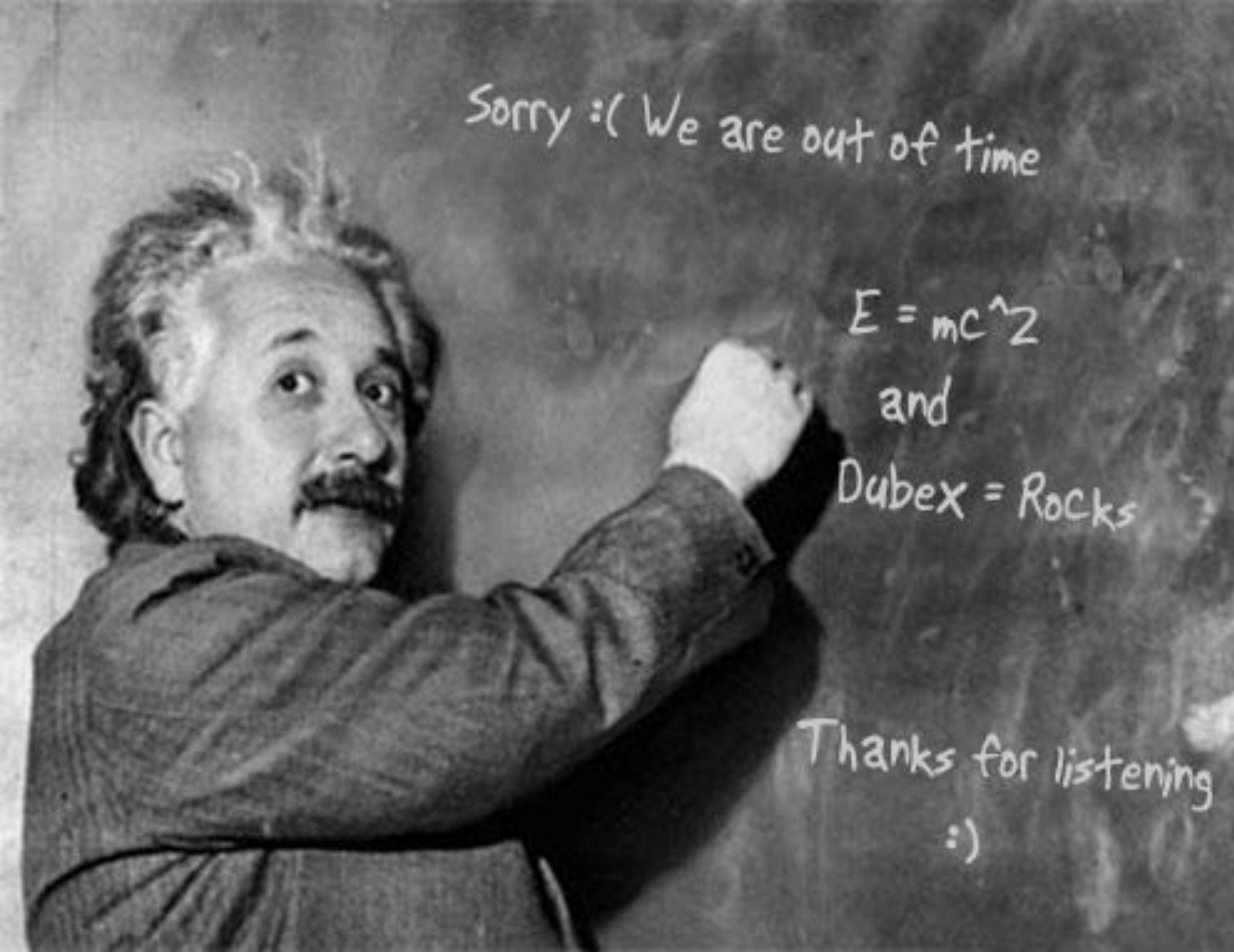




Låsens *driver*- og *key* pins
røg ud efter 2 minutter..







Dubex:

MANAGING RISK. ENABLING GROWTH.®

Keld Norman / kno@Dubex.dk



Husk
Kaffe
😊



Husk
Kaffe
😊



THE END

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 Elderw (Beijing Group, Sneaky **Panda**) Equation Group
Energetic Bear (Berserk Bear, Crouching Yeti, **Dragonfly**, Dr 3.0, Group 24, **Koala** Team) FIN4 Five Eyes FruityArmor
Gaza Hacker Team (**Molerats**) General Directorate for Ex Security Government Communications Security Bureau
Group5 Hellsing Goblin **Panda** (Cycldek) HIDDEN C s Hurricane **Panda** Bluenoroff Moafee
Moonlight Maze National Security Agency National Electronic Security Authority Neodymium No. 91 Office (NK)
Pacifier APT Patchwork - Dropping**Elephant** (Monsoon, T, Operation Hangover) Promethium Roaming **Tiger**
Rocket **Kitten** **Sandworm** Team (BE2 APT, Quedagh) S rC t Silent Chollima Spring **Dragon** (Lotus Blossom)
Stealth **Falcon** Strider - ProjectSauron **TigerMilk** Actor berworm (Cobalt Gypsy) Titan Rain Tonto Team
Turla Group (Group 88, KRYPTON, **Snake**, Venomous **Bear**, Waterbug) Unit180 Unit 8200 Zirconium Group

Lizard Squad



Stealth Falcon



Patchwork
DroppingElephant
(Monsoon APT, Operation Hangover)



APT15 Vixen Panda
(GREF, Ke3Chang, Mirage, Playful Dragon)



Turla Group
(Group 88, KRYPTON,
Snake, Waterbug)



Gaza Hacker Team (Molerats)



APT17 Deputy Dog (Hidden Lynx, Tailgater Team)



Sandworm Team
(BE2 APT, Quedagh)

QUILTED TIGER



MYTHIC LEOPARD



FLYING KITTEN



EXTREME JACKAL



HACKTIVIST

INDRIK SPIDER



DEEP PANDA



STARDUST CHOLLIMA
(enhjørning)



FANCY BEAR



THE WEBSITE HAVE BEEN DEFACED BY
~ THE MUTE SWAN ~





Dubex:

MANAGING RISK. ENABLING GROWTH.®

Keld Norman / kno@Dubex.dk

