H4CKER

Hvordan og hvorfor blir tjenester hacket?
Hva kan vi gjøre?

H4CKERE

Hvem er de?

WHITE HAT

De gode

GREY HAT

De over-nysgjerrige

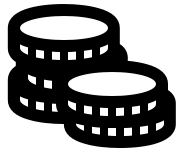
BLACK HAT

De onde

Som en ondsinnet hacker, hva motiverer meg?

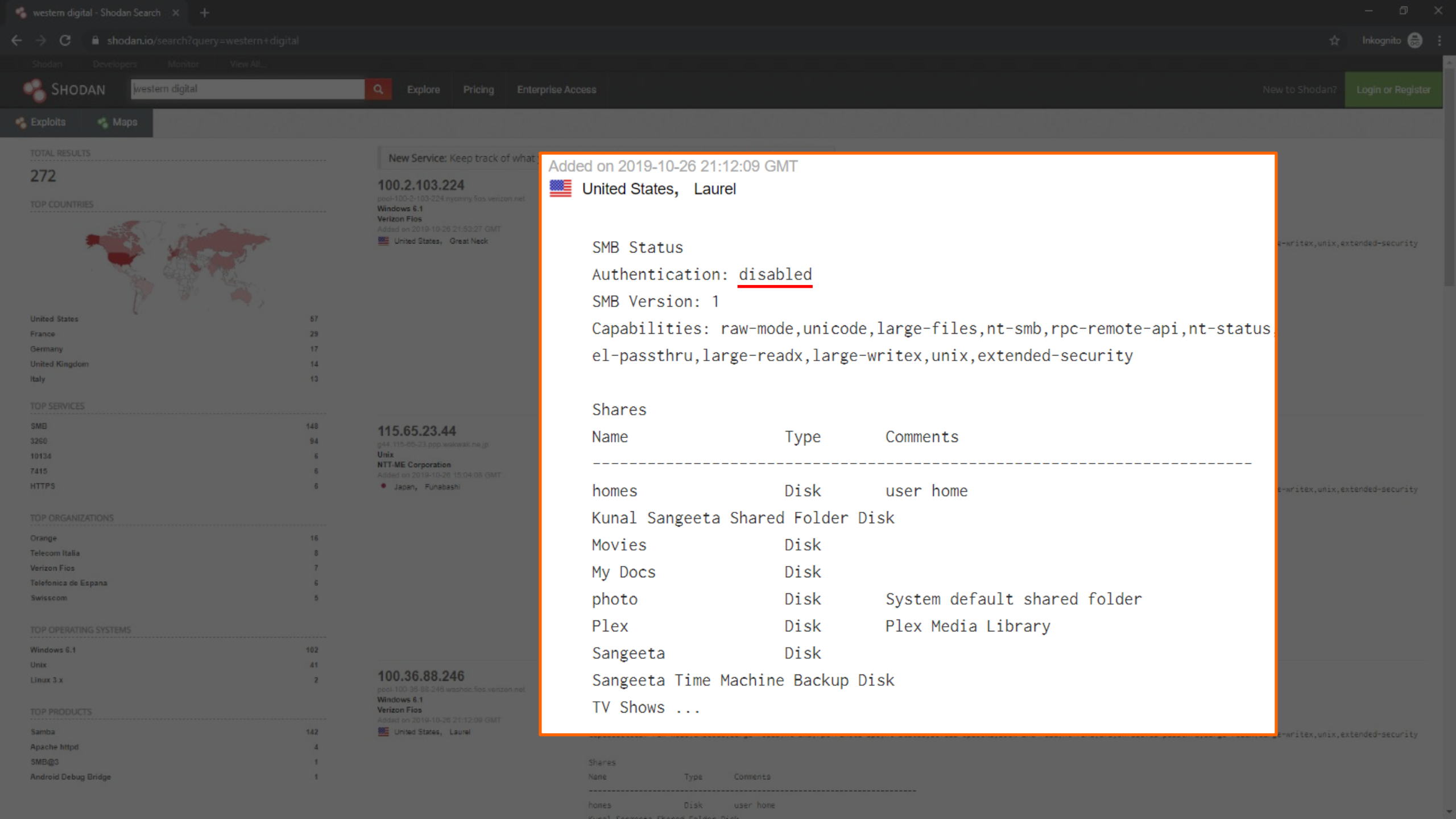
- Hærverk
- Sabotasje / Spionasje
- Identitetstyveri
- Økonomisk vinning

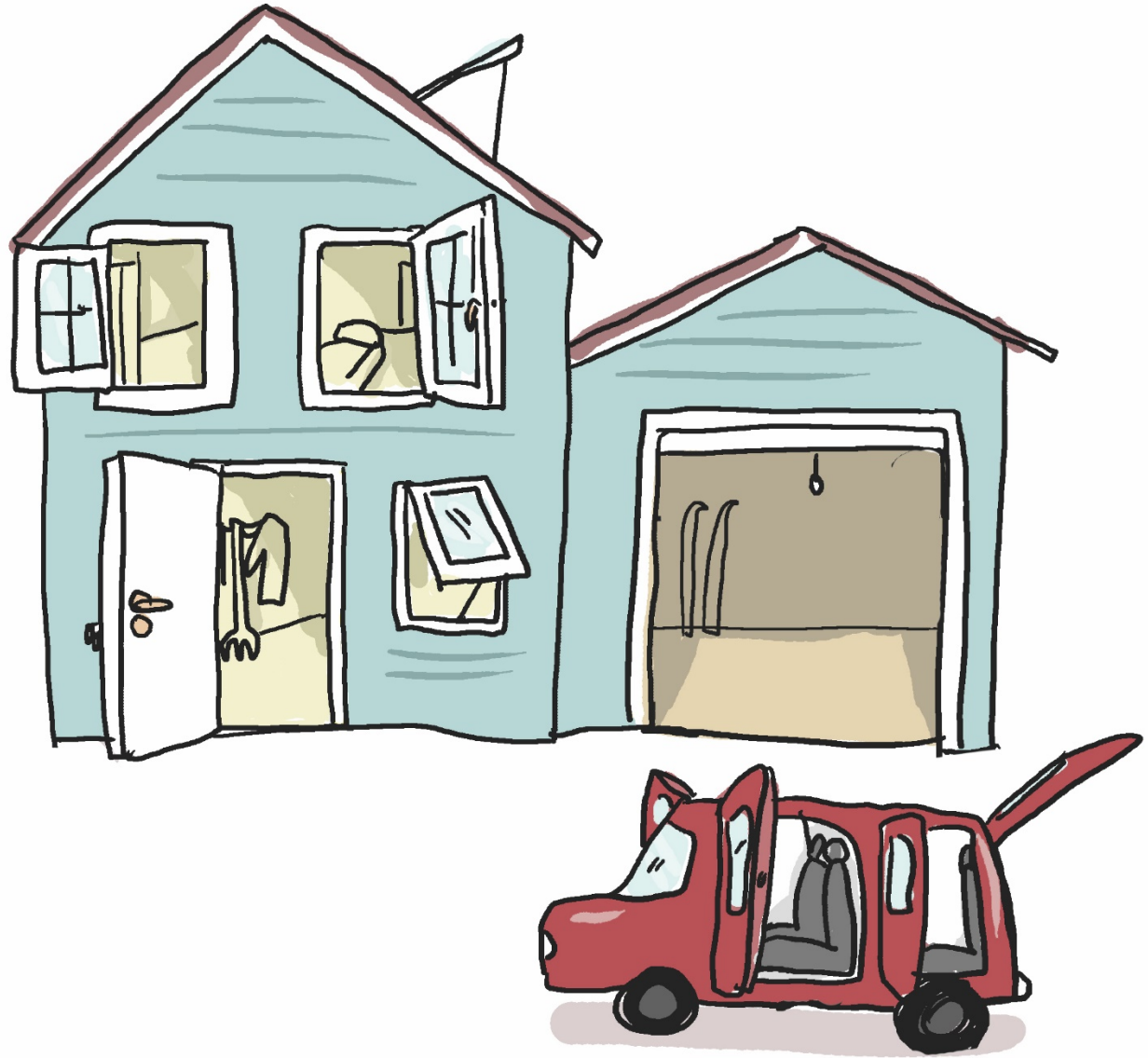
ØKONOMISK VINNING



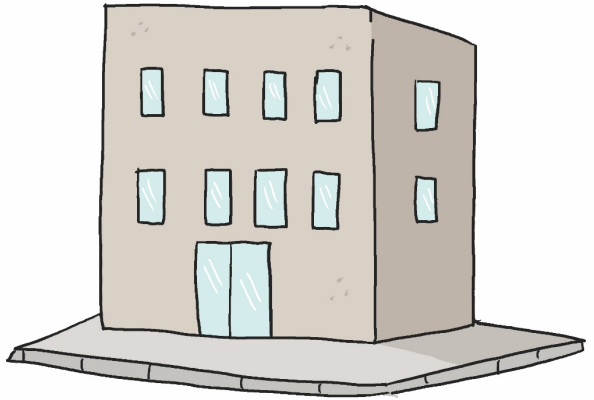
Hvem er **målet**?

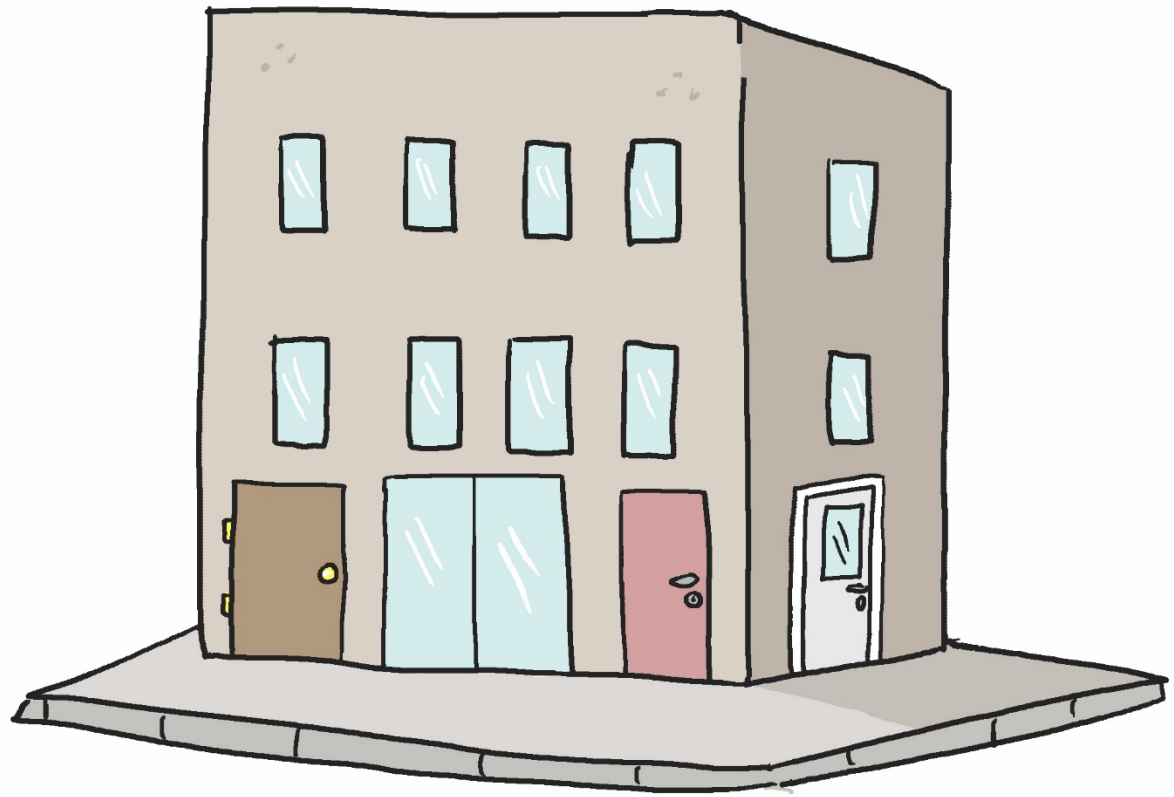
De som står "**laglig til for hogg**"


western digital - Shodan Search
shodan.io/search?query=western+digital
SHODAN
western digital
Explore
Pricing
Enterprise Access
Login or Register
Exploits
Maps
TOTAL RESULTS
272
TOP COUNTRIES
United States 57
France 29
Germany 17
United Kingdom 14
Italy 13
TOP SERVICES
SMB 148
3260 94
10134 6
7415 6
HTTPS 6
TOP ORGANIZATIONS
Orange 16
Telecom Italia 8
Verizon Fios 7
Telefonica de Espana 6
Swisscom 5
TOP OPERATING SYSTEMS
Windows 6.1 102
Unix 41
Linux 3.x 2
TOP PRODUCTS
Samba 142
Apache httpd 4
SMB@3 1
Android Debug Bridge 1
100.2.103.224
Windows 6.1
Verizon Fios
United States, Great Neck
115.65.23.44
Unix
NTT-ME Corporation
Japan, Funabashi
100.36.88.246
Windows 6.1
Verizon Fios
United States, Laurel
Added on 2019-10-26 21:12:09 GMT
United States, Laurel
SMB Status
Authentication: disabled
SMB Version: 1
Capabilities: raw-mode,unicode,large-files,nt-smb,rpc-remote-api,nt-status,
el-passthru,large-readx,large-writex,unix,extended-security
Shares
Name Type Comments
homes Disk user home
Kunal Sangeeta Shared Folder Disk
Movies Disk
My Docs Disk
photo Disk System default shared folder
Plex Disk Plex Media Library
Sangeeta Disk
Sangeeta Time Machine Backup Disk
TV Shows ...



Bedrift eller organisasjon med tilstedeværelse på internett

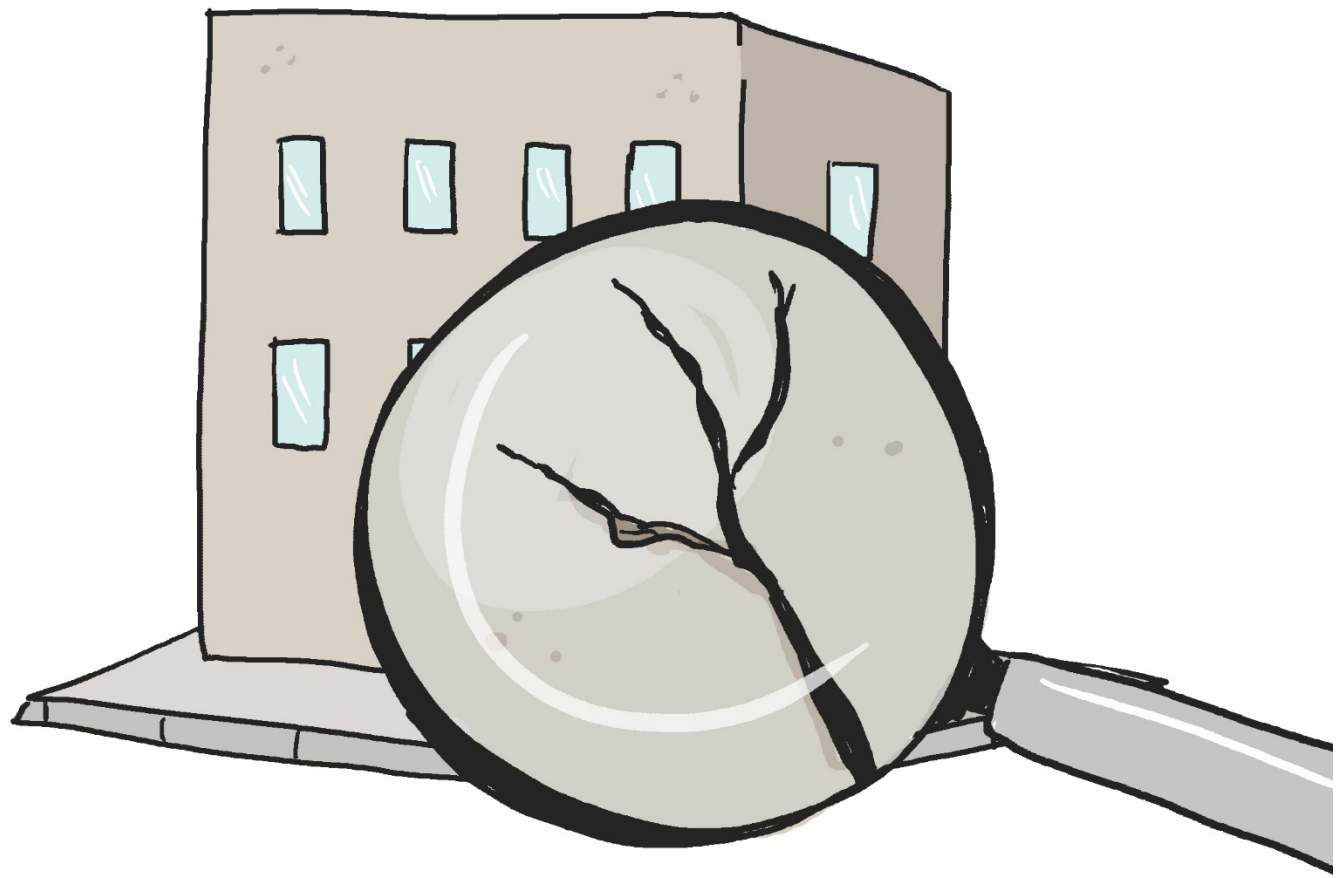




REKOGNOSERING

Brønnøysundregistrene

Virtuelt Privat Nettverk



Eksempel:

Oppdager at et nettsted er bygget med Wordpress 5.0

Desember 6, 2018
(utdatert)

CVE-2019-8942
Remote code execution
(autentisert)

KARTLEGGE BRUKERE

File Edit View Search Terminal Help

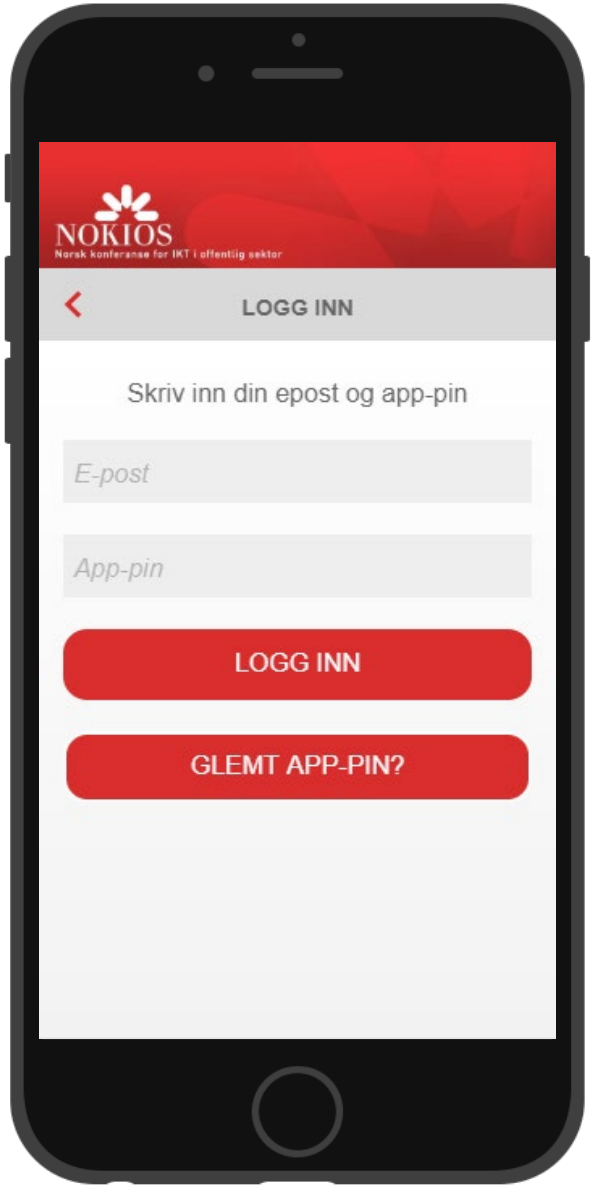
```
[i] User(s) Identified:

[+] admin
[+] naiveNils
 | Detected By: Rss Generator (Aggressive Detection)
 | Confirmed By:
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)


[+] Finished: Wed Oct            2019
[+] Requests Done: 3100
[+] Cached Requests: 10
[+] Data Sent: 776.536 KB
[+] Data Received: 1.409 MB
[+] Memory used: 221.477 MB
[+] Elapsed time: 00:01:58
root@kali:/#
```

Kan jeg gjette meg til passordet?

NOKIOS app

- E-postadressen du registrerte med
- Jeg "gjetter" 10.000 ganger
- Forsøker 111 ganger per sekund
- Gyldig PIN på 1min 30sek

- **Heldigvis ikke så veldig sensitive data**



Er passordet brukt andre steder?

(Les: gjenbruk)

Erna solberg sier det er greit.

[redacted]

LÅ UTE: Denne artikkelen lå ute på Dagbladets nettavis torsdag ettermiddag. Henvisningen på Dagbladets front var en artikkel om BMW-innbrudd på Østlandet Foto: Skjermdump/Dagbladet.no

Gutt siktet for Dagbladet-hacking

Politiet har siktet en ungdom etter at Dagbladet torsdag måtte stenge nettavisen som følge av at en artikkel med grove utsagn dukket opp.

Av ANNIKEN ARONSEN og OLA HARAM
Oppdatert 19. oktober

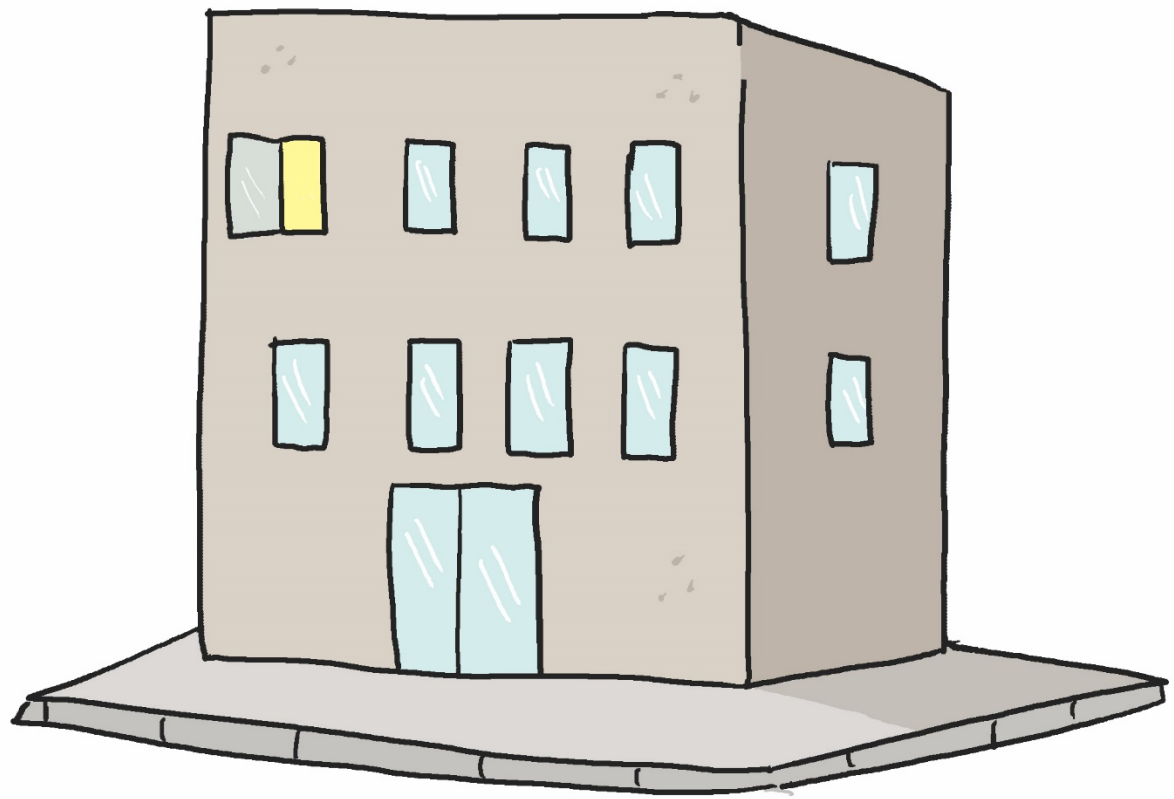
Kilde: VG.no


WordPress
Username
naiveNils
Password
Remember Me
Log In
Lost your password?
← Back to WordPress Test Site
…
Sommer2016
Sommer2017
Sommer17
S0mmer17
S0mm3r17
…

“Vi bruker lange og komplekse passord”

“Ja, og vi har alltid oppdatert programvare”

Hvordan er det med funksjonalitet på nettsiden / appen?

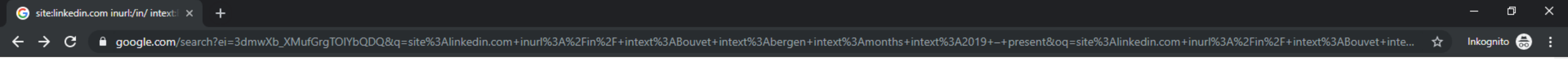


“Vi har kun én nettside med enkel og godt testet funksjonalitet, så det gjelder ikke oss”

Det stemmer… det er **DERE**

?

site:linkedin.com inurl:/in/ intext:Bouvet intext:bergen intext:2019 – present


site:linkedin.com inurl:/in/ intext:

google.com/search?ei=3dmwXb_XMufGrgTOIYbQDQ&q=site%3Alinkedin.com+inurl%3A%2Fin%2F+intext%3ABouvet+intext%3Abergen+intext%3Amonths+intext%3A2019+–+present&oq=site%3Alinkedin.com+inurl%3A%2Fin%2F+intext%3ABouvet+inte...

Inkognito

Google

site:linkedin.com inurl:/in/ intext:Bouvet intext:bergen intext:months intext:2

Sign in

All | Images | News | Shopping | Videos | More | Settings | Tools

About 653 results (0.32 seconds)

[redacted] - Avdelingsleder - Bouvet ASA | LinkedIn
https://no.linkedin.com › in › [redacted]
Avdelingsleder i **Bouvet** ... May **2019** – **Present** 6 **months** ... Integration developer for a project for Høgskolen i **Bergen**, using BizTalk, C#, SQL Server to build a ...

[redacted] - Konsulent - Bouvet ASA | LinkedIn
https://no.linkedin.com › in › [redacted]
Konsulent at **Bouvet** ASA. Stavanger Area, Norway. Oil & Energy. **Bouvet** ASA. Roxar. University of **Bergen** (UiB) ... January **2019** – **Present** 10 **months**.

[redacted] - Software Consultant - Bouvet ...
https://no.linkedin.com › in › [redacted]
Software Consultant at **Bouvet** ASA ... University of **Bergen** (UiB). Experience. **Bouvet** ASA. Software Consultant. **Bouvet** ASA. Jun **2019** – **Present**5 **months**.

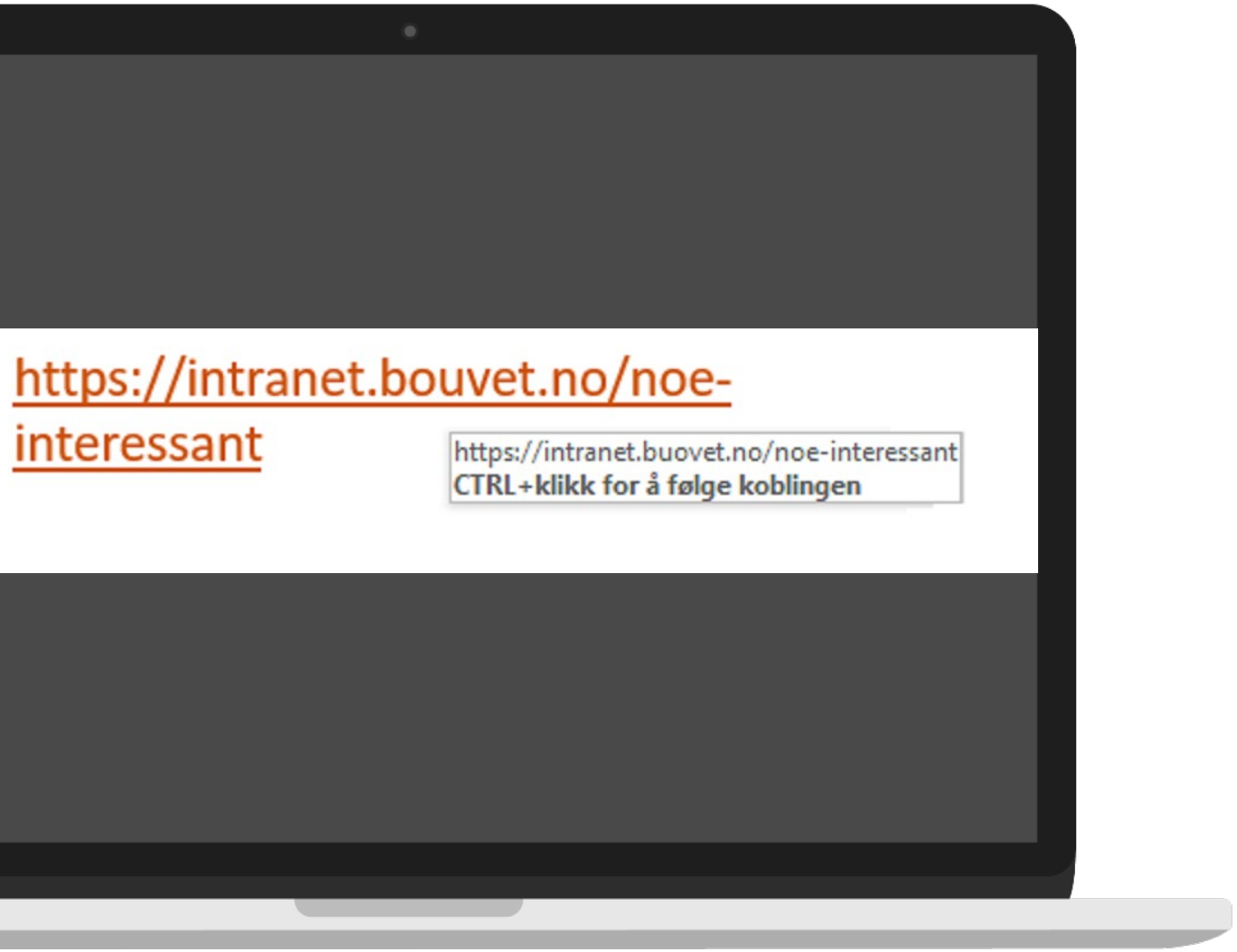
[redacted] - Consultant - Bouvet ASA | LinkedIn
https://no.linkedin.com › in [redacted]
Consultant at **Bouvet** ASA. **Bergen**, Hordaland, Norway. Information ... August 2016 – **Present** 3 years 3 **months** ... January 2011 – August 2016 5 years 8 **months**.

[redacted] - Consultant - Bouvet ASA | LinkedIn
https://no.linkedin.com › in › [redacted]
Consultant at **Bouvet** ASA. Oslo, Oslo, Norway. Management Consulting. **Bouvet** ASA. Crayon ... Show Camel Uten Filter, Ep 16 - Gordana Elvestuen - 6 Jul **2019**. Image for .... January 2018 – **Present** 1 year 10 **months** ... University of **Bergen**.

[redacted] - Consultant - Bouvet ASA | LinkedIn
https://no.linkedin.com › in [redacted]
Consultant at **Bouvet** ASA ... Høgskolen i **Bergen** / **Bergen** University College (HiB) ... October **2019** – **Present** 1 month ... January 2008 – July 2008 7 **months**.

[redacted] - Consultant / Team Lead - Bouvet ASA ...
https://no.linkedin.com › in › [redacted]


Google
GULE SIDER



Fellen

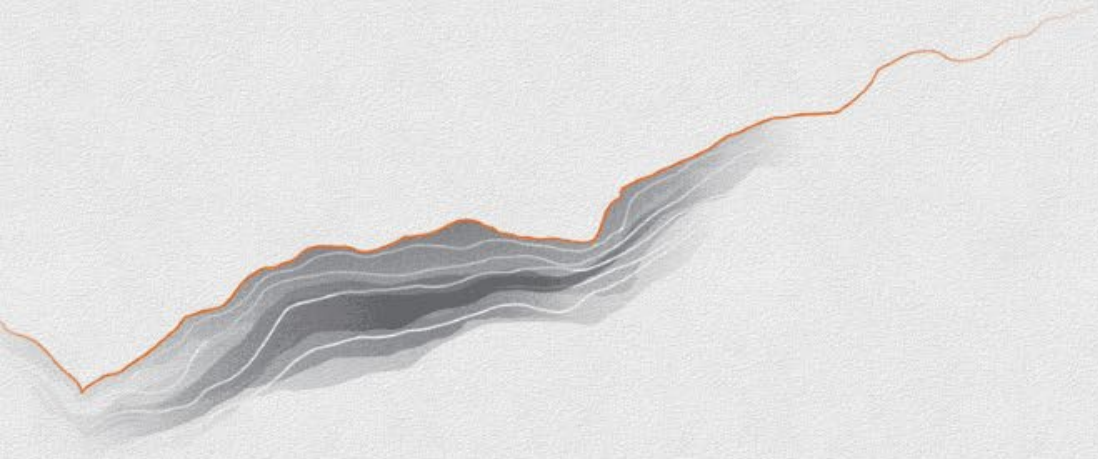
- Anskaffe buovet.no
- Falsk portal, kopi av ekte portal
- Sikre den med HTTPS
- Send interessant e-post til alle ny-ansatte
- https://intranet.bouvet.no/noe-interessant

>

Logg på

intranet.buovet.no/noe-interessant

Inkognito



bouvet

Logg på med din organisasjonskonto

hoen@example.com

Passord

Logg på

© 2013 Microsoft

naivenils@bouvet.no
logget inn med
S0mmer18

kulekristine@bouvet.no
logget inn med
Jeg3lsker!1nternett

barebeate@bouvet.no
logget inn med
123456

“Vi har to-faktor pålogging, så lykke til…”

Revidert felle

- Word dokument eller Excel regneark med bakdør
- Misbruke dine menneskelige egenskaper - du åpner bakdøren

Hei Frank,
Til orientering: Se **vedlegg** for utkast av **nedbemanningsplan**.
Høyst konfidensielt! Passordet til dokumentet er "**firmaNavn2019**"...

Bonus: Priming

“Hæ? Sende SMS fra en annen sin telefon – det er jo ikke mulig…”

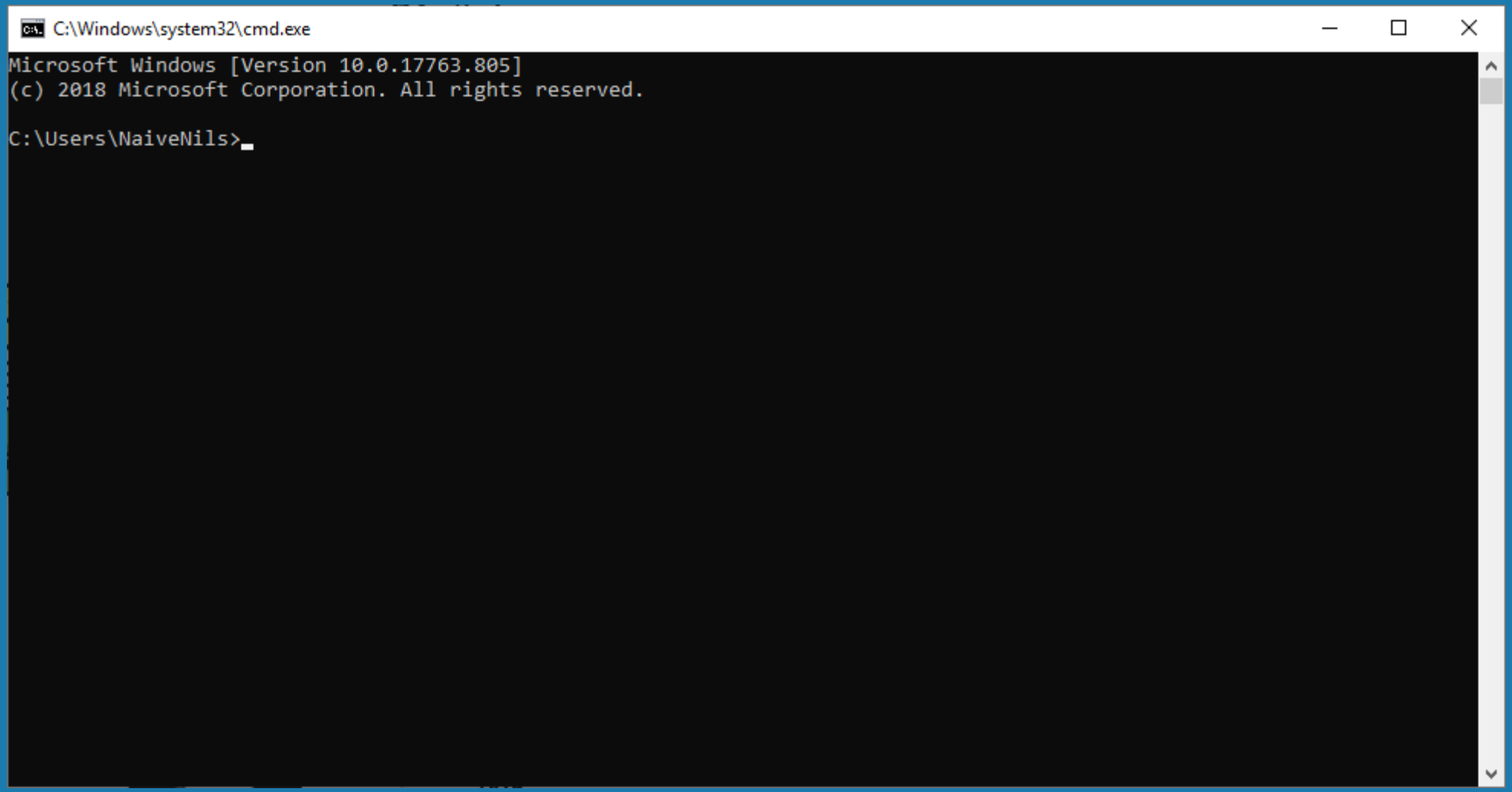
Lånt tillit

Etablere tillit til en ekstern e-postadresse

Hei,
se mailen BareBeate sendte feil i går, ganske drøyt...
Passordet til vedlegget er "**firmaNavn2019**"

Avsender: arne.privat93@gmail.com


PASS
Tegnehanne
2019


C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.805]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\NaiveNils>

“Vi har oppdatert antivirus, så vedlegget blir stoppet”


No engines detected this file
SHA-256 a06e513444be0b3d5cb35da7eb864aa281ccc0314e12a5ba9f4d1acbbc751333
File name Loddtrekning.xlsm
31.77 KB
Last analysis 2018-07-03 14:36:52 UTC
XLSX
0 / 60
Detection
Ad-Aware
AhnLab-V3 Clean
ALYac Clean
Arcabit Clean
Avast Mobile Security Clean
Avira Clean
Babable Clean
BitDefender Clean
CAT-QuickHeal Clean
AegisLab
Alibaba
Antiy-AVL Clean
Avast Clean
AVG Clean
AVware Clean
Baidu Clean
Bkav Clean
ClamAV Clean
60 forskjellige antivirus programmer synes at min hjemmelagde trojanske hest var helt OK


PASS
Tegnehanne
2019

“Men jeg har kastet maskinen min ned i en aktiv vulkan”

Jeg er på innsiden av nettverket

- Forstå landskapet og verdiene jeg har tilgang på
- Oppnå «administrator» på maskinen ~~din~~ min
- Overvåke nettverket og samle inn passordhasher++
- Angripe andre datamaskiner / printere / enheter i nettverket
- Forholde meg stille til jeg har kontroll over kritiske ressurser

3-6 måneder senere…


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

“Vi har daglig backup kjørende”

Nei, dere **hadde** det…

Jeg er på innsiden av nettverket

- Forstå landskapet og verdiene jeg har tilgang på
- Oppnå «administrator» på maskinen ~~din~~ min
- Overvåke nettverket og samle inn passordhasher++
- Angripe andre datamaskiner / printere / enheter i nettverket
- Forholde meg stille til jeg har kontroll over kritiske ressurser

Hydro ble hacket i løpet av desember 2018

19. mars 2019 kom selve angrepet

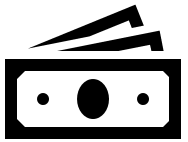
Hvorfor blir tjenester hacket?

- Kryptovaluta -> ransomware (løspengevirus)
- Stadig flere ting skal på internettet
- Mangel på forståelse av produktene vi bruker
- Ny teknologi, ukjent
- Mangelfull patching og oppdatering når sårbarheter blir kjent

Sterkt svekket eller fraværende operasjonell evne?

Persondata på avveie?

Norge er et rikt land



Hva kan dere gjøre….?

IKKE TA E-POSTER
OG SMS
FOR GOD "PHISK"

(Tren de ansatte!!!)

Husk 5 “likes”

- 👍 Sterke passord
- 👍 Oppdatert programvare
- 👍 Ingen huller i funksjonalitet
- 👍 Multifaktor pålogging
- 👍 Antivirus

Noen ekstra grep

- Baser forsvaret på at angriperen allerede er i nettverket deres
- Ansett de nysgjerrige hackerne, ikke politianmeld dem!
- Krypterte disker
- VPN off-site
- **Tren de ansatte!!!**
- **Penetrasjonstesting**

Triks: bruke de gode og de nysgjerrige hackerne til å beskytte oss mot de onde

Krister Kvaavik

- Sikkerhetskonsulent hos Bouvet
- Utvikler
- Penetrasjonstester
- Selvutnevnt phishing-ekspert

- CE|H – Certified Ethical Hacker
- OSCP – Offensive Security Certified Professional

Krister Kvaavik

- Sikkerhetskonsulent hos Bouvet
- Utvikler
- Penetrasjonstester
- Selvutnevnt phishing-ekspert

Spørsmål?

Send meg gjerne en e-post (ja takk, phishing e-poster også):
krister.kvaavik@bouvet.no