TRUSSELBILDET I NORGE

NORWAY THREAT INTELLIGENCE REPORT

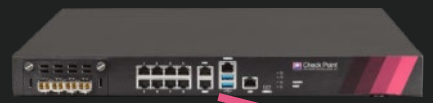
Pål H. Aaserudseter

Security Engineer

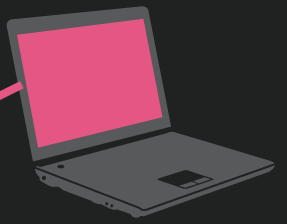
Trusselbilde eller “ulv, ulv”?

- Forskjellig oppfatning av virkeligheten
  - Forskjellige ståsted/områder
  - Tilgjengelige data
- Fokus på hva som kan gå galt
  - **MYE** går også veldig bra
  - Hvorfor går det bra eller galt?
- Dette er ingen fasit på trusselbildet
  - Men vi kan fortsatt lære av historien
  - Bildet endrer seg kontinuerlig

Omfattende innsyn i den reelle digitale verden



Over 100K sensorer
og honning krukker

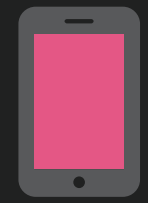


Millioner av endepunkt

THREATCLOUD

Milliarder av fil analyser

Millioner av mobile enheter



CHECK POINT RESEARCH

Check Point SandBlast ZERO-DAY PROTECTION

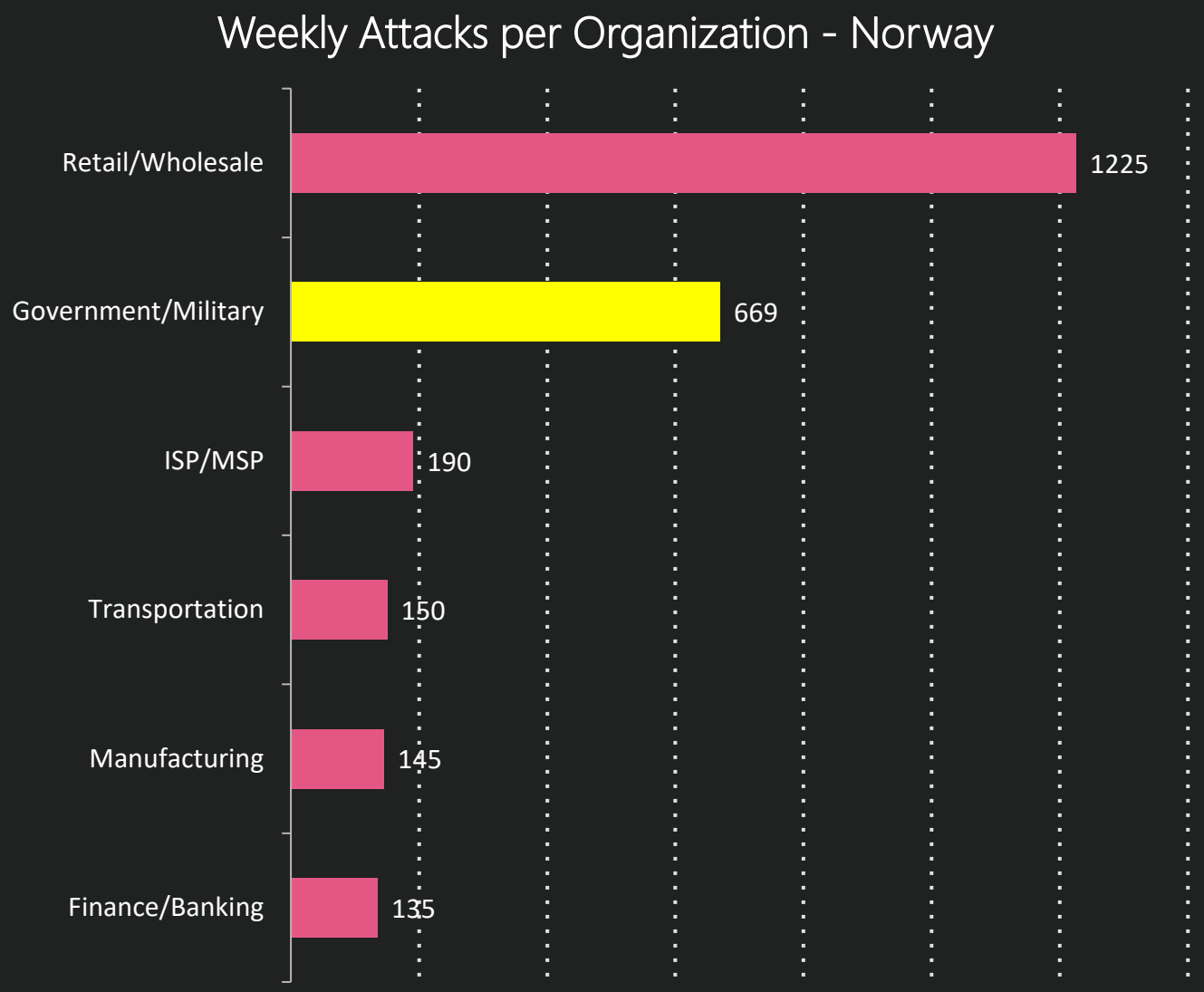
ThreatCloud inspiserer over 3 milliarder websider og 600 millioner filer daglig

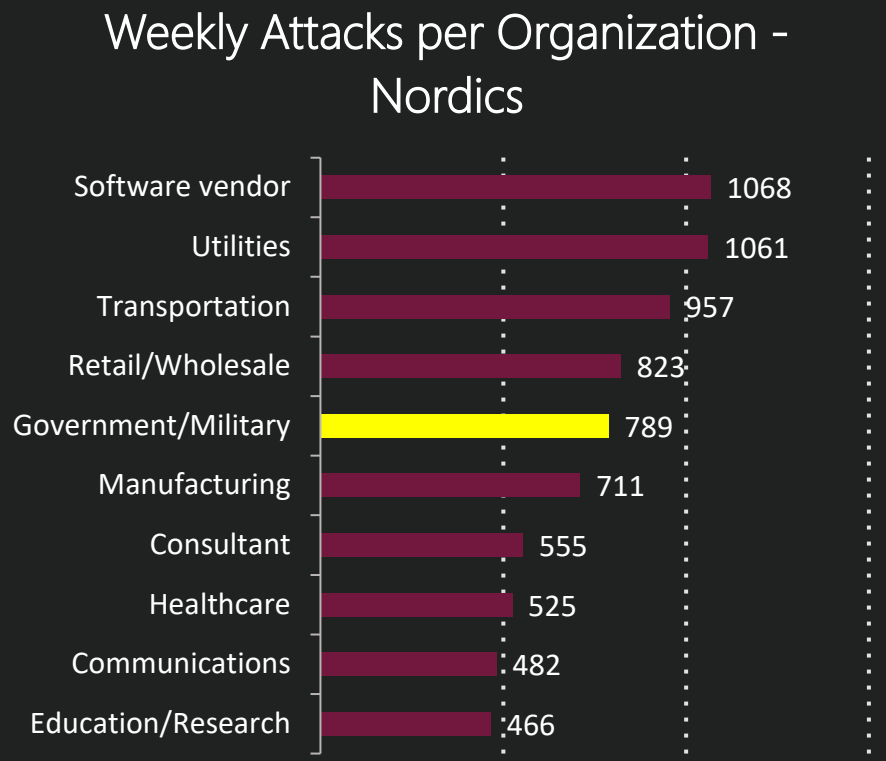
og finner over 250 million skadelige aktiviteter per dag

Oppsummering av trusselbildet (siste 6mnd)

- I gjennomsnitt angripes en organisasjon i Norge 498 ganger i uken
- Den mest utnyttede malware i Norge er Lokibot
- Topplista for malware i Norge består av: 1 Backdoor, 1 Banking Trojan (Trickbot), 1 Cryptominer (XMRig) og 1 Infostealer (Lokibot)
- 50% av skadevare i Norge kommer gjennom E-post
- Den vanligste sårbarheten i Norge er «Remote Code Execution», som påvirker 62% av organisasjonene

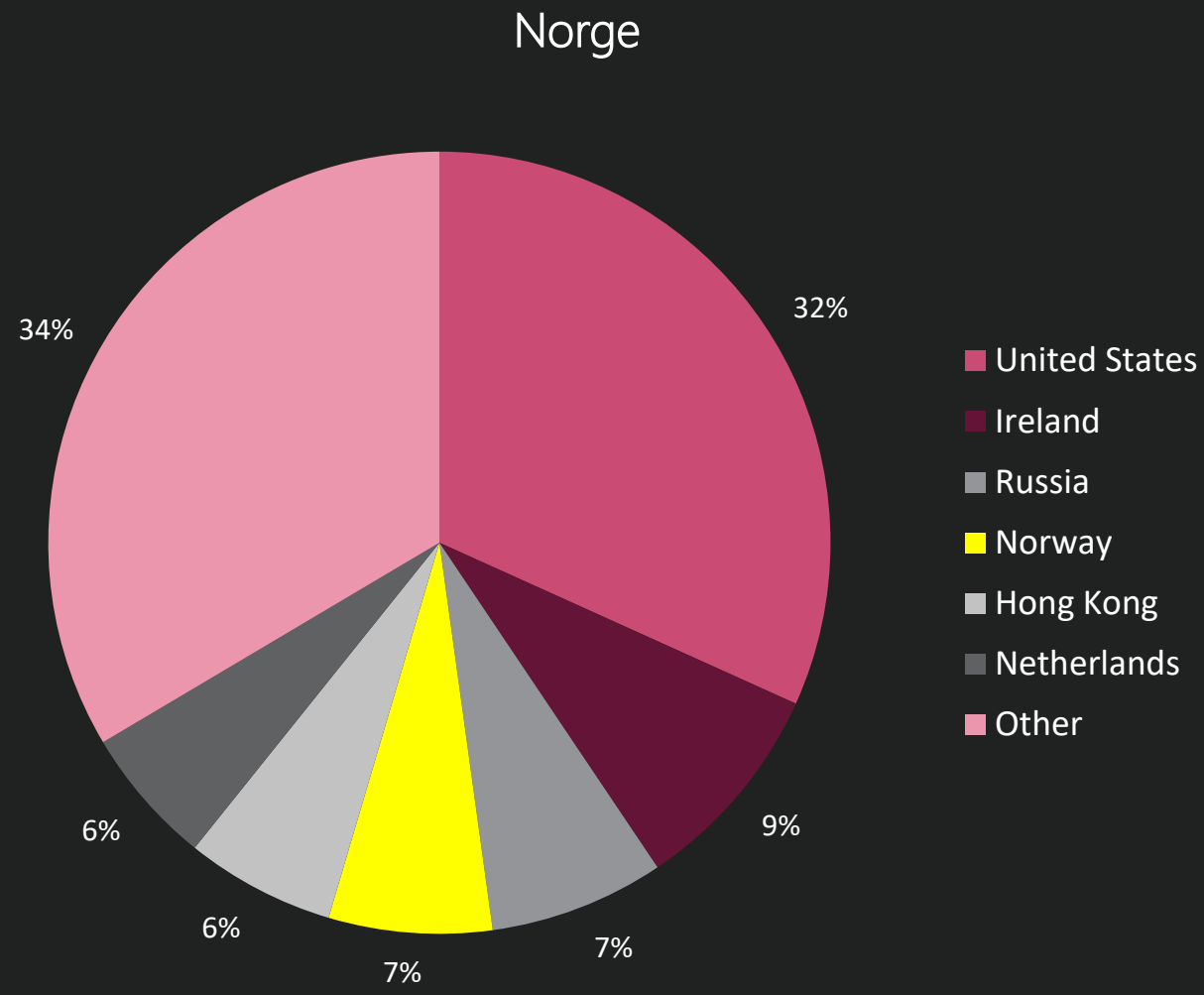
De mest berørte næringene, siste 6 måneder





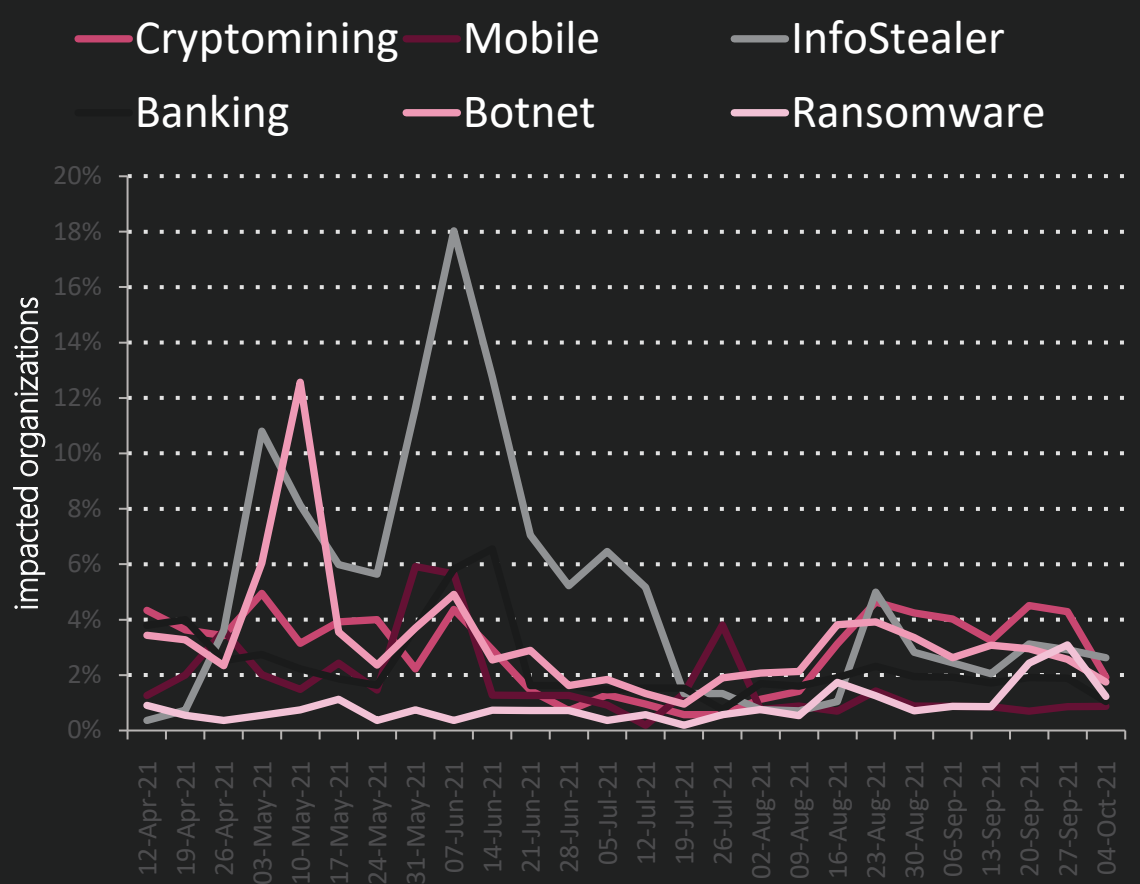
Skadelige aktivitet mot Norge – siste 6 mnd

- Viser hvor den kompromitterte enheten som brukes som mellomledd er lokalisert
- Egentlig aktør er noe helt annet
  - Må avdekkes på andre måter
- Mye sky infrastruktur er dårlig sikret
  - Store datasentre i USA, Irland og Nederland
- Kina og Russland er nykommer
  - Trenger ikke være lokale aktører
  - Mer sårbar infrastruktur også der



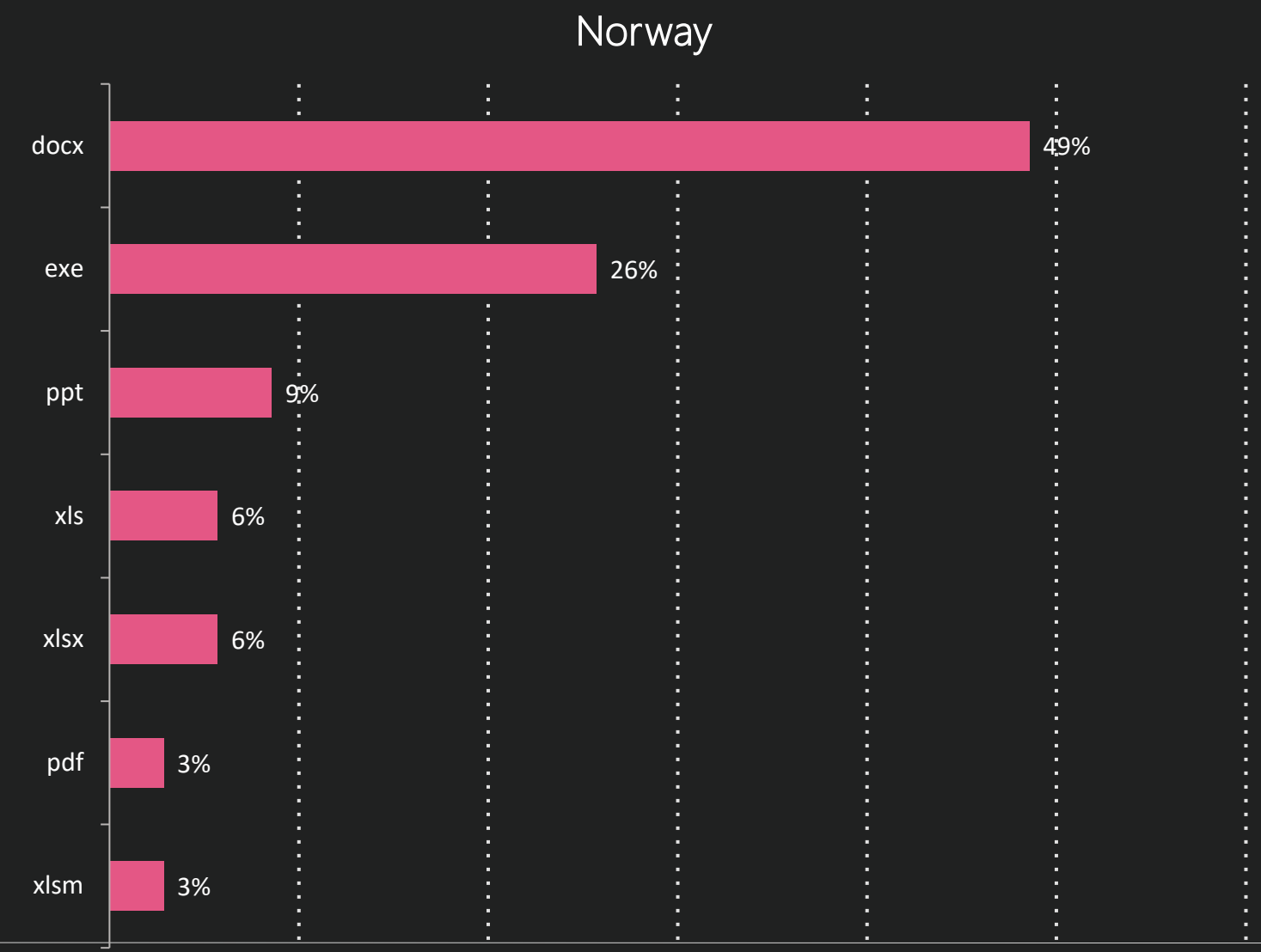
Hvilke skadelige aktiviteter ser vi i Norge?

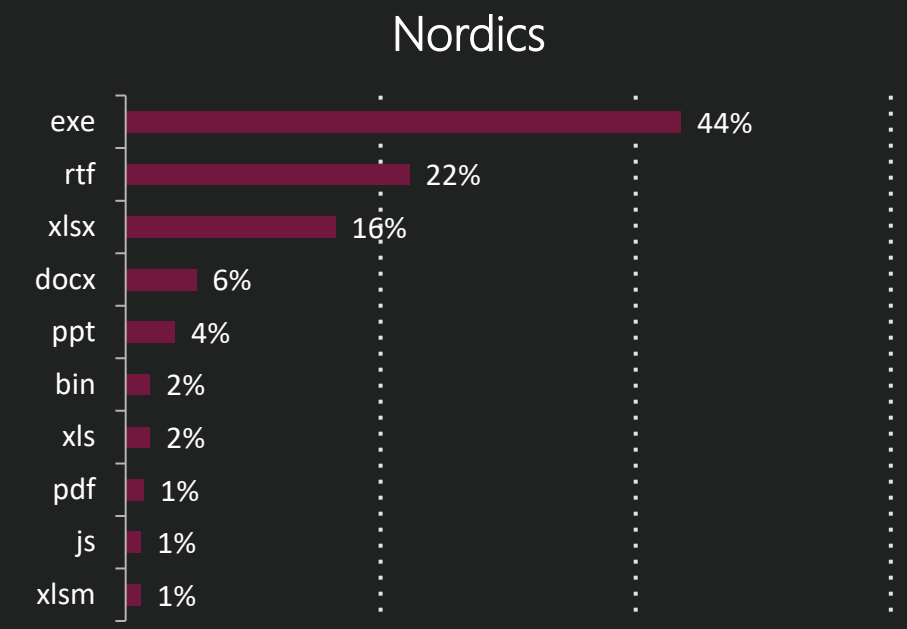
- Alt starter gjerne som «Bot»
- Neste steg er
  - Cryptomining
  - Bank trojaner
  - InfoStealer
- Siste steg er Ransomware
  - Alt annet er hentet ut
  - Skvise ut siste dråpe



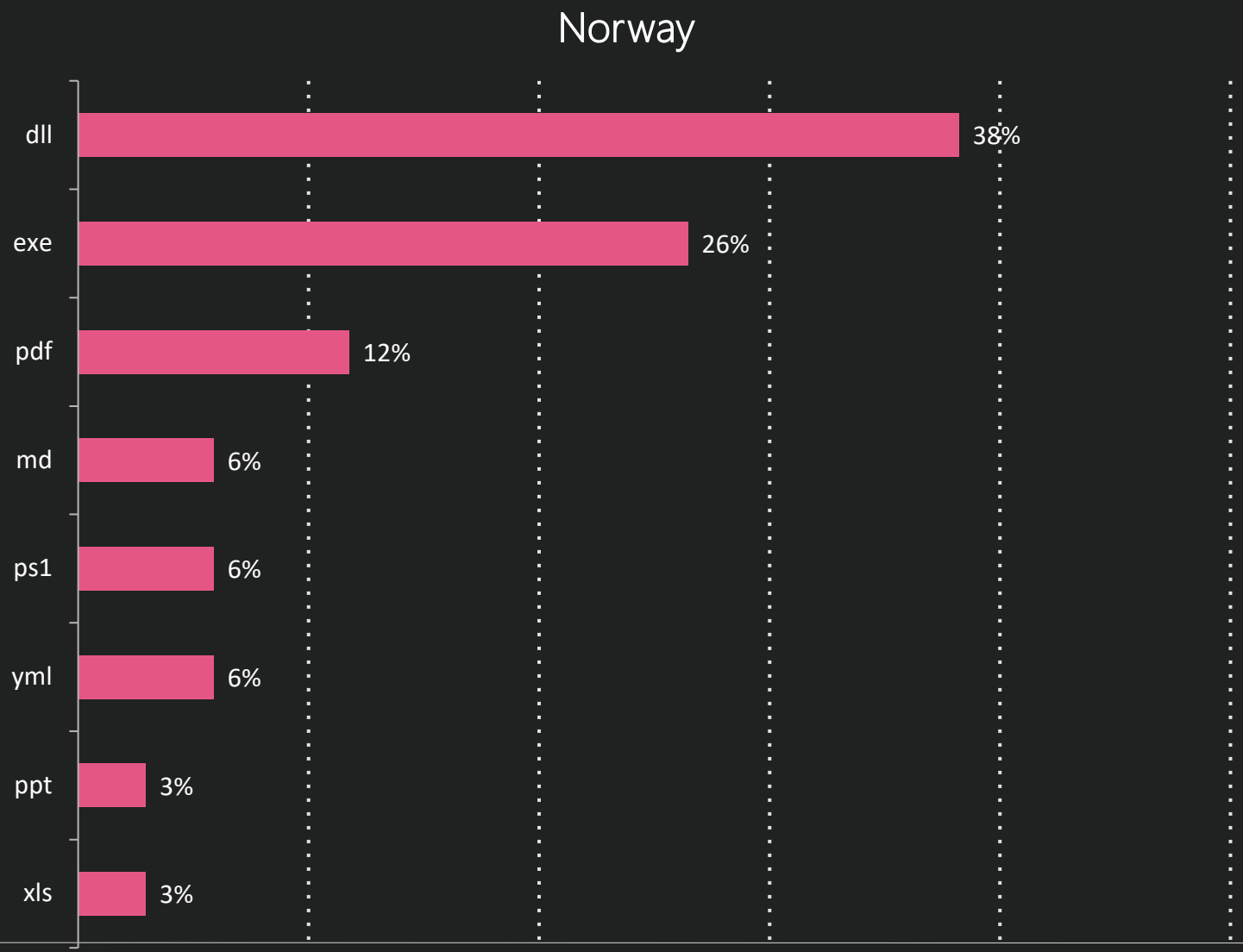
MOTIVASJON: PENGER

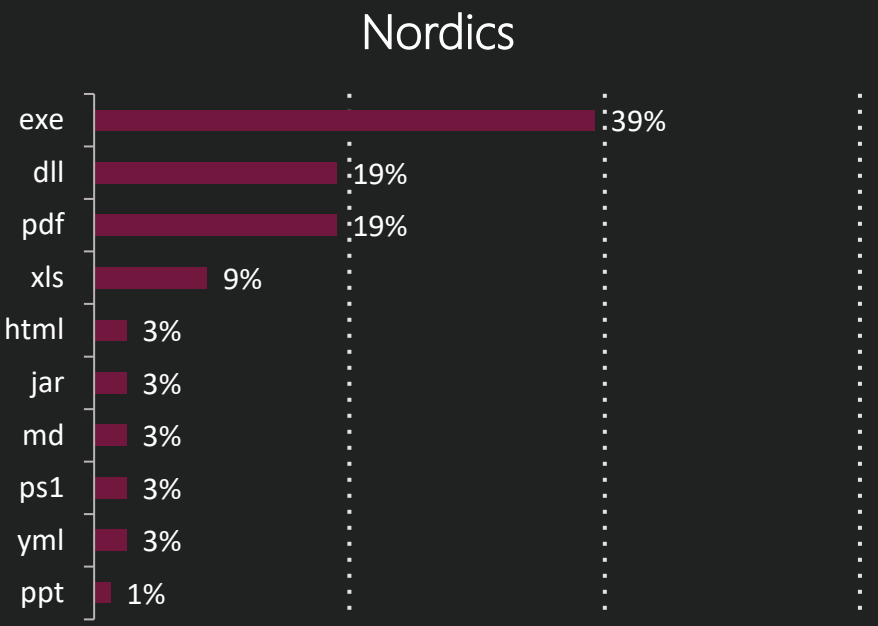
Toppliste over ondsinnede filer (E-post)





Toppliste over ondsinnede filer (Web)

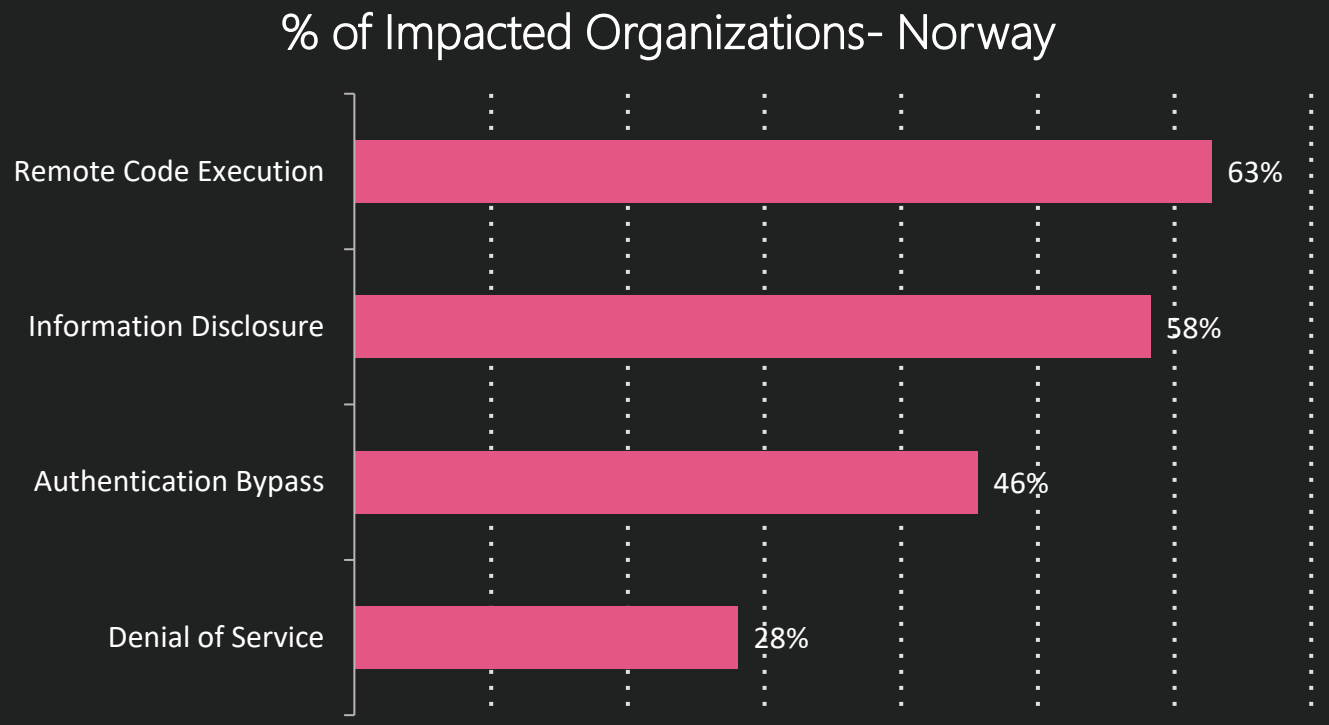


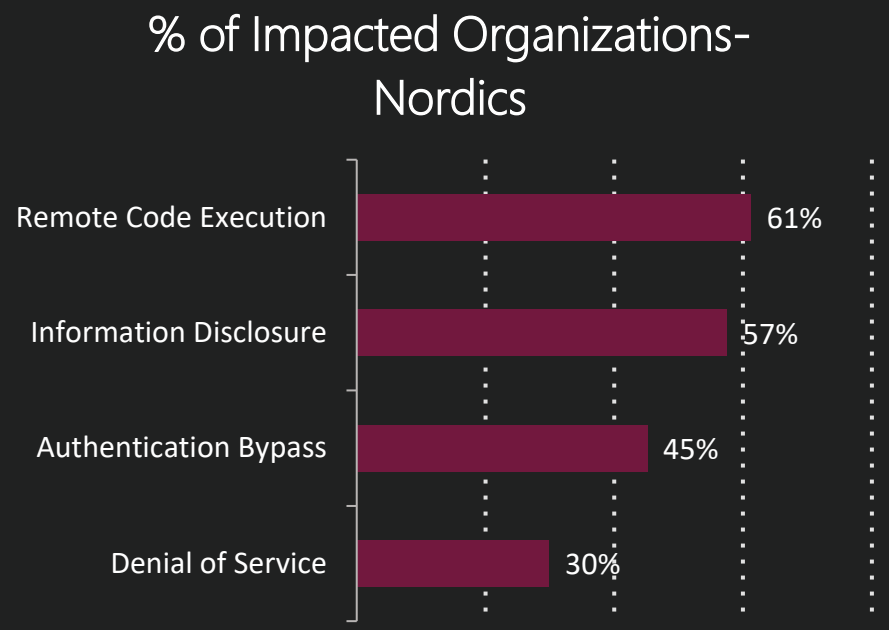


Topp MITRE teknikker, ondsinnede EXE filer

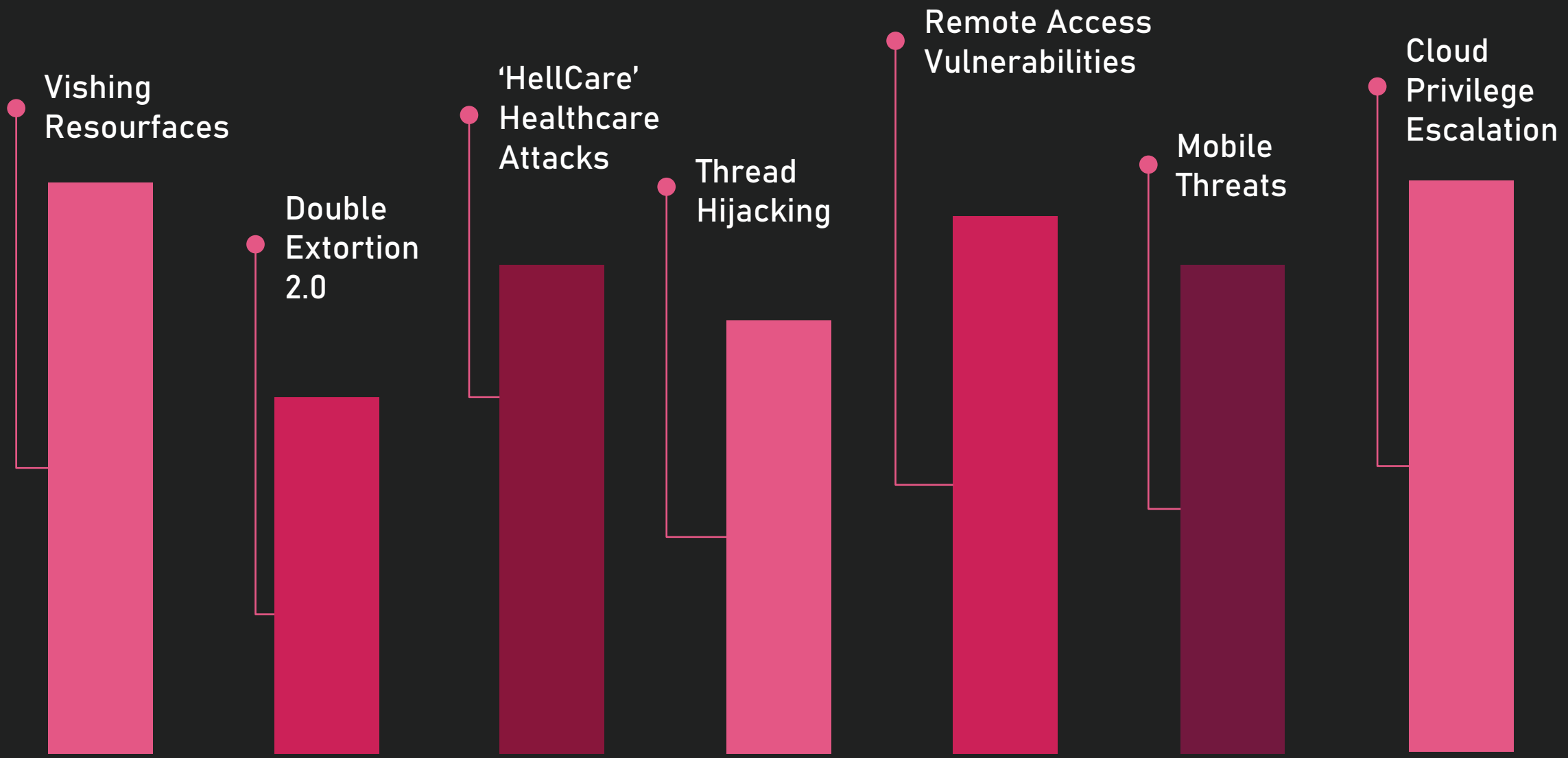
TECHNIQUE	RELATED TACTICS	NORWAY IMPACT	NORDICS IMPACT
Execution through API	Execution	61%	52%
System Information Discovery	Discovery	50%	46%
Virtualization / Sandbox Evasion	Defense Evasion, Discovery	46%	49%
Data Encrypted	Exfiltration	38%	40%
File Deletion	Defense Evasion	38%	40%

Toppliste for utnyttede sårbarheter



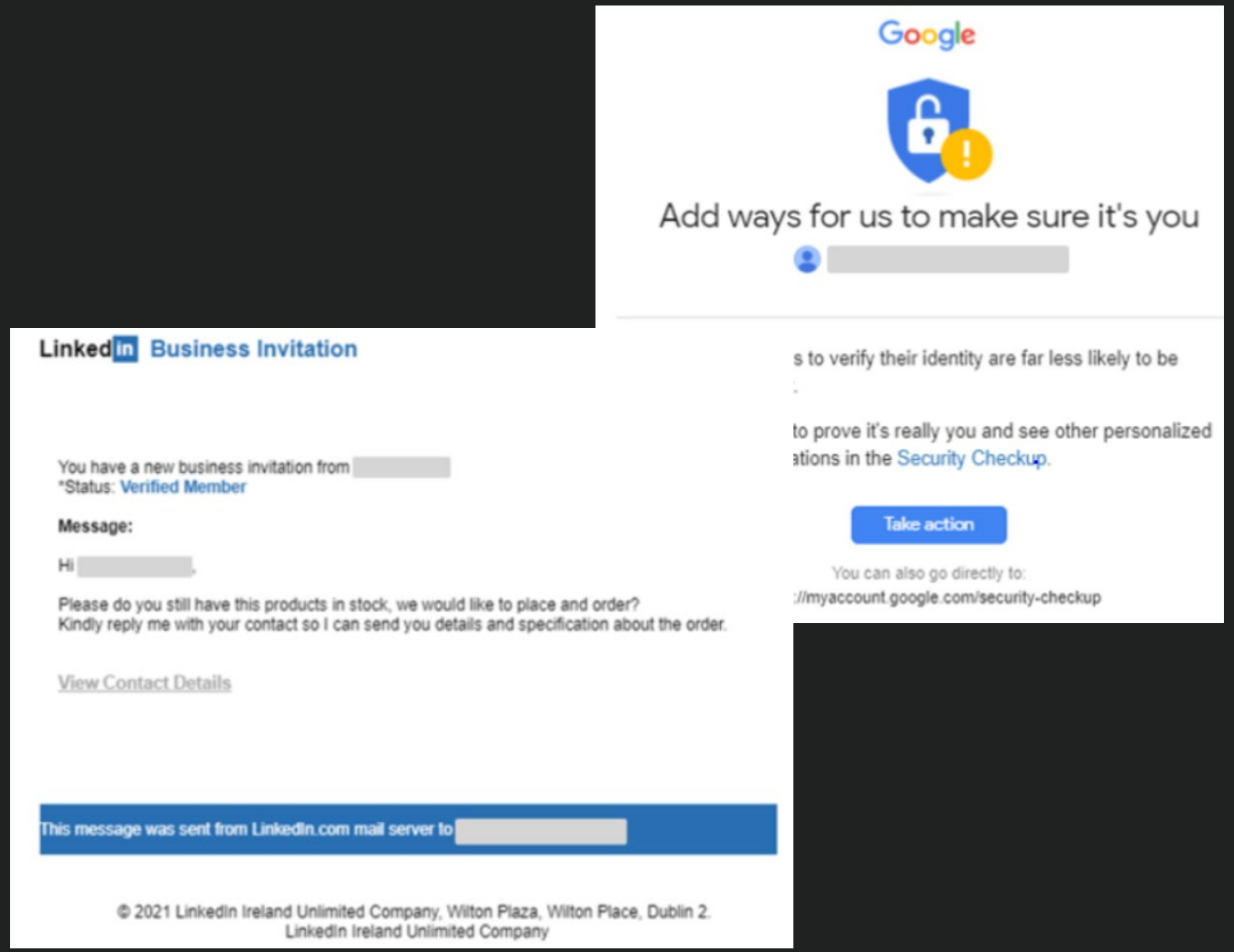


Trussel trender i 2021



Men (brand) Phishing er også økende

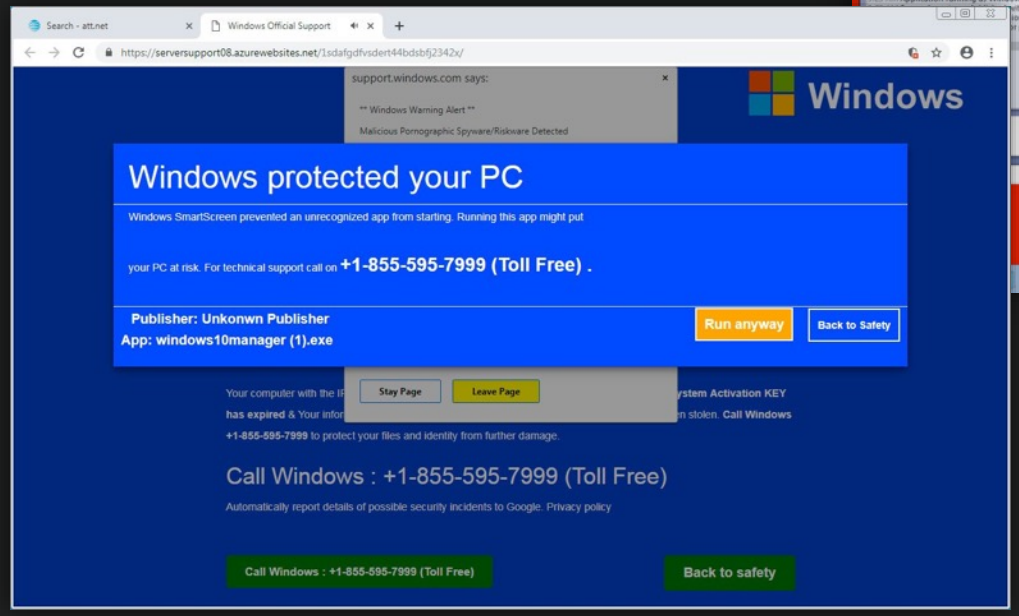
- Microsoft (29%)
- Amazon (13%)
- DHL (9%)
- Bestbuy (8%)
- Google (6%)
- WhatsApp (3%)
- Netflix (2.6%)
- LinkedIn (2.5%)
- Paypal (2.3%)
- Facebook (2.2%)

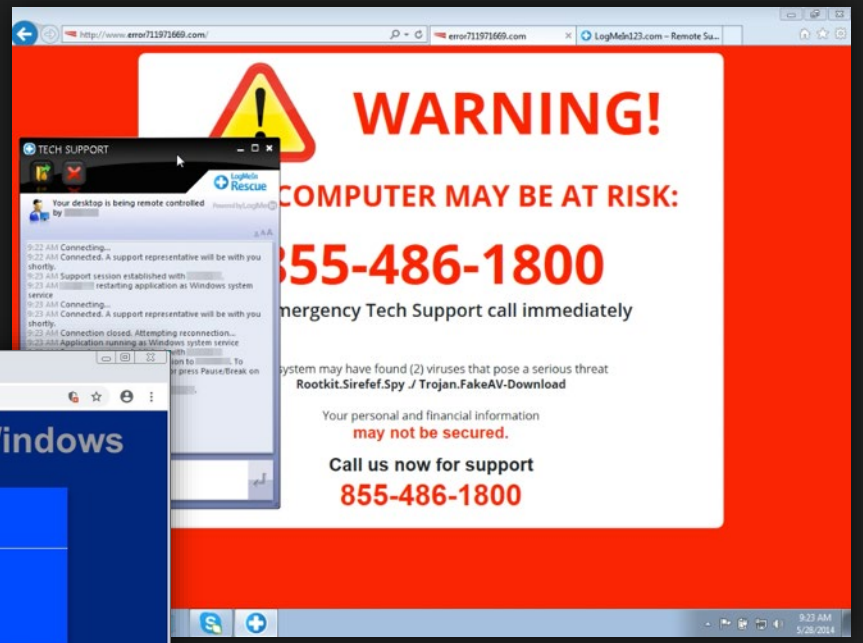


Vishing (fra gammelt av)

- Mest vanlig frem til nå;

  Tech Support Svindel





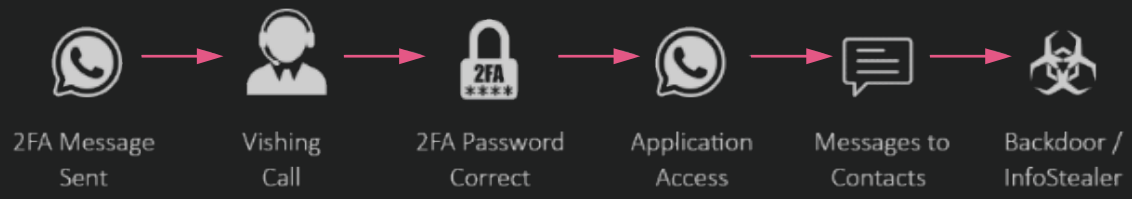
- Siden før 2000
- Brukeren oppfordres til å kontakte tekniker
- Det kreves avgift for 'tjenesten'
- Kredittkort data stjeles

Vishing v2 (en moderne variant)

- Nyere varianter;

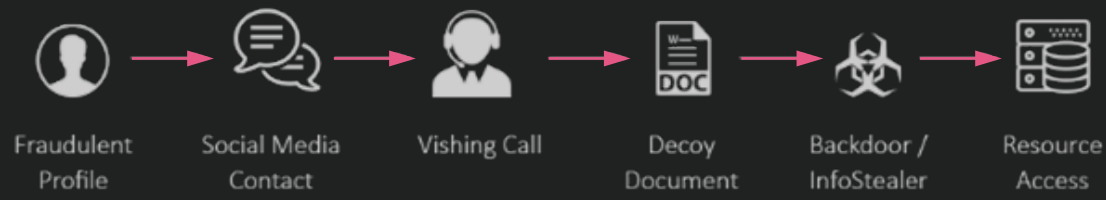
Skreddersydde angrep mot organisasjoner

1



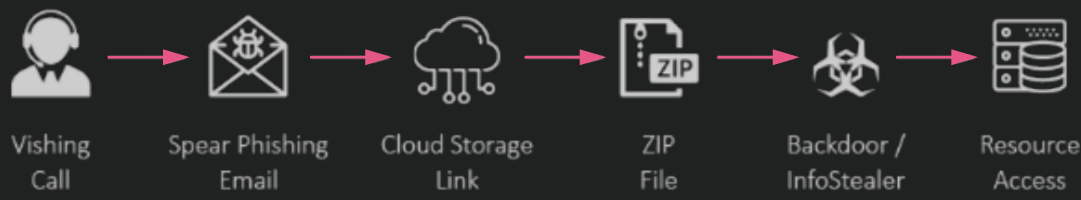
Vishing som den første fasen av et storskala angrep mot sluttbrukere

3



Vishing som midtfase av et målrettet angrep mot en organisasjon

2



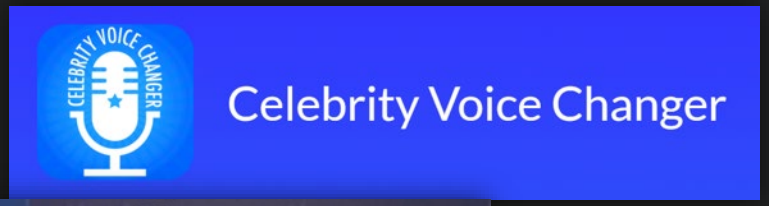
Vishing som den første fasen av et målrettet angrep mot en organisasjon

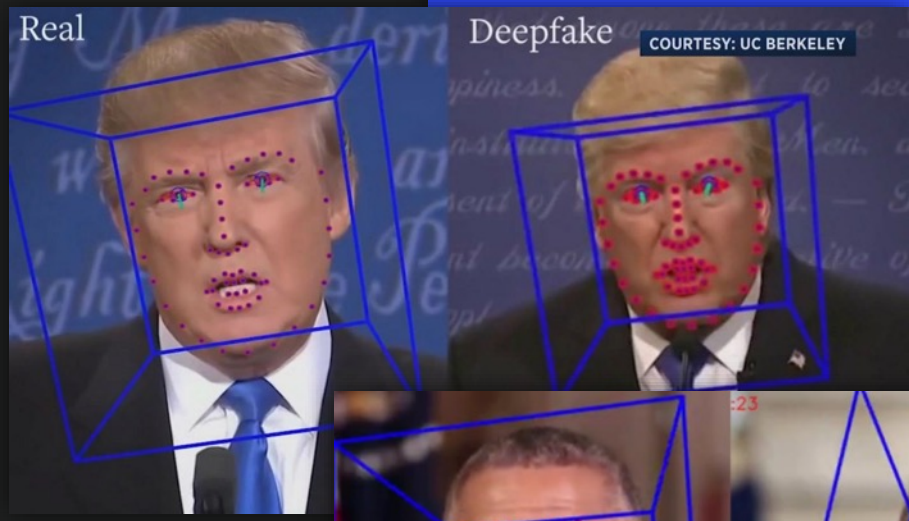
Vishing v3 (deepfakes blir bedre og bedre)

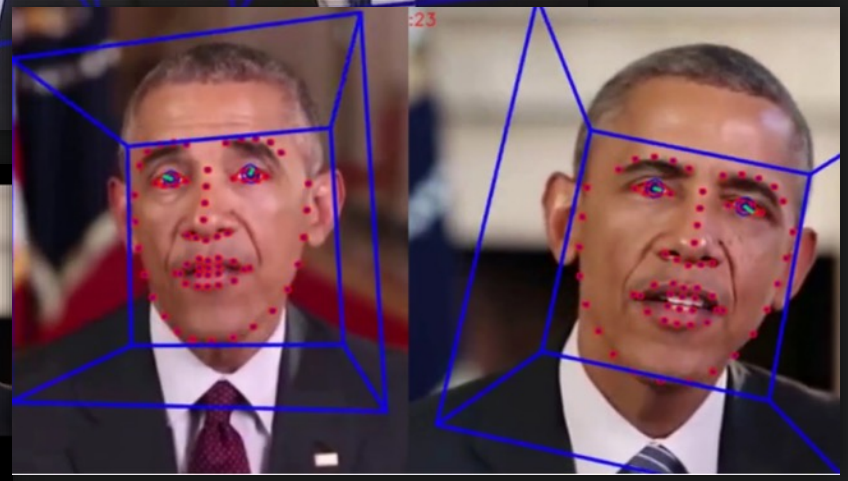
- Under planlegging;

  Deep-fake AI-basert samtale Phishing

  - Imitere sjefens stemme
  - Deepfake videoer
  - Applikasjoner for stemme-simulering







Dobbel til trippel utpressing

PSYKOTERAPIAKESKUS Vastaamo.fi
PARANNAMME PSYKOTERAPIAN SAATAVUUTTA

cp<r>
CHECK POINT RESEARCH

Milepæl; Finske psykologi kjeden Vastaamo ble angrepet

Data stjålet i mars 2019 ⟶ utpressing startet september 2020 ⟶ offentlig kjent i oktober 2020

- Over 40,000 pasienter berørt

1. Data stjålet fra kompromitterte systemer

Sadly, it appears as though security levels were raised at Vastaamo only after the 2019 h
the data had already gone. Vastaamo was informed of the extortion in late September, 2
three Vastaamo employees received an extortion message.

2. Firma blir presset – 40 BTC i løsepenger

Vastaamo has been summoned to pay roughly half a million US dollars in Bitcoin. But that's not the worst bit. Recently, the attackers started to send extortion messages to the patients, asking them to pay around $240 to prevent their data from being published. And that is a first, as far as we know—not just demanding a ransom from the breached organization, but also from all those that were unlucky enough to have their data on record there.

3. Data fra 300 pasienter blir offentliggjort

the company resisted, "RANSOM_MAN" published the personal data of 300 people, including various public figures and police officers. They communicated with people on Torilauta (meaning "market board"), a Finnish discussion forum on the dark web,

4. Pasienter pres

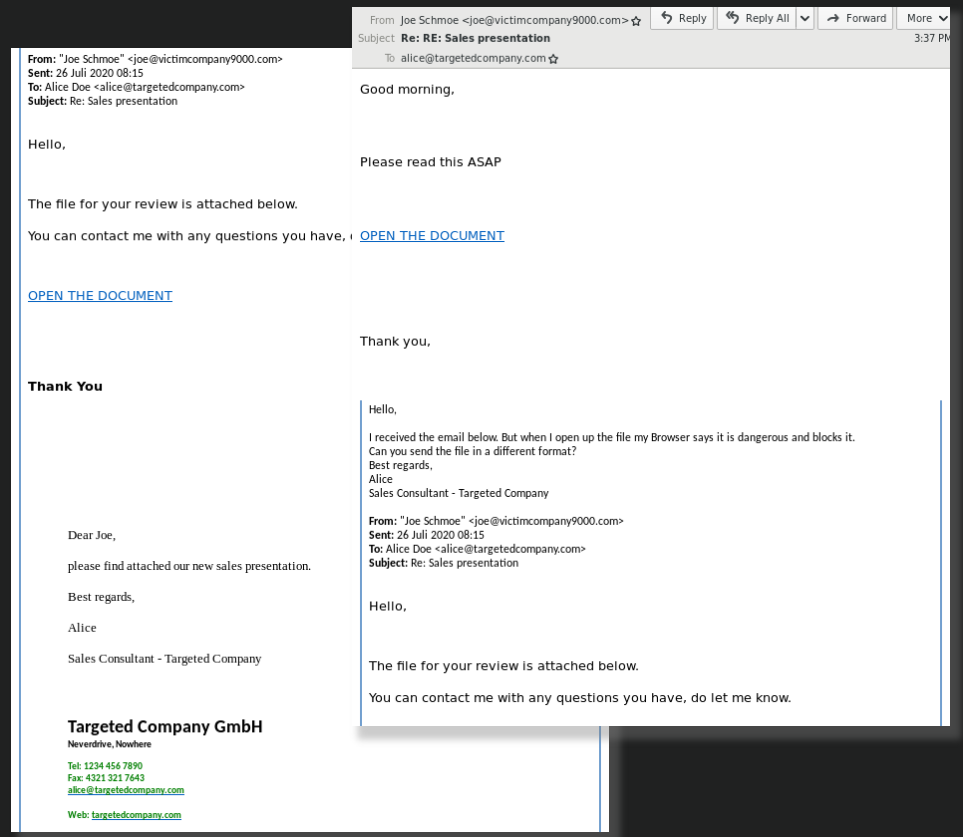
After attempting to extor
Vastaamo, the unidentifie
from the individual victims, including children. Puro received an email on October 24 demanding €200 in bitcoin; if he didn't pay within 24 hours, the ransom would rise to €500, otherwise the content of his conversations with his therapist would be made public.

5. Myndighetene griper inn

On Monday, authorities launched a website for victims of the cyber-attack, offering advice and telling them not to pay the ransom demand. "Do not communicate with the extortionist - the data has most likely already been leaked elsewhere," the Data Leak Help website said.

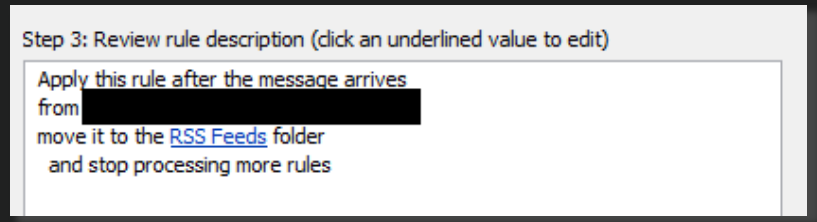
Thread Hijacking (Kapring av Epost tråder)

- Før: Ikke stol på vedlegg eller linker i eposter fra ukjente sendere
- Nå: Ikke stol på eposter i pågående eposttråder med kollegaer og venner



Epost tråd kapring

1. *Offerets epostdatabase blir kompromittert.*
2. *Angriper henger seg på gamle eller pågående tråder.*
3. *Deltagere i tråden mottar vedlegg/linker fra "kjente" kilder.*
4. *Nye offer blir kompromittert.*
5. *Angriper legger inn regler for å skjule kommunikasjonen.*



Cloud Privilege Escalation

- Sky feilkonfigurering angriper kontoer istedenfor ressurser
- Identity and Access Management (IAM) svakhet pga leverandørfeil eller feil tillit mellom systemer

Attackers can abuse a misconfigured IAM role across 16 Amazon services

CLOUD

AWS IAM Assume Role Vulnerabilities Found in Many Top Vendors

amazon web services

Abusing Privilege Escalation in Salesforce Using APEX

salesforce

Cloud misconfiguration continues to pose a huge threat

"We found thousands upon thousands of other accounts that were susceptible to the same type of identity misconfigurations. So, we know this isn't just an isolated problem. This is a widespread problem in the cloud," he explained.

The Blended AWS Attack: Extracting IAM Role Credentials

Azure

Noen gode ting..

- Heldigvis samarbeider myndigheter og sikkerhetsmiljøet

Arrestasjoner

A 17-year-old in Tampa, Florida, has been arrested in connection with the massive Twitter hack that hijacked dozens of high-profile accounts

Bringing VandaTheGod down to Earth: Exposing the person behind a 7-year hacktivism campaign

Synliggjør aktører

Feds Arrest Member of Fin7, Group Tied to a Billion Dollars Worth of Hacks

US Indicts Sandworm, Russia's Most Destructive Cyberwar Unit

The Department of Justice has named and charged six men for allegedly carrying out many of the most costly cyberattacks in history.

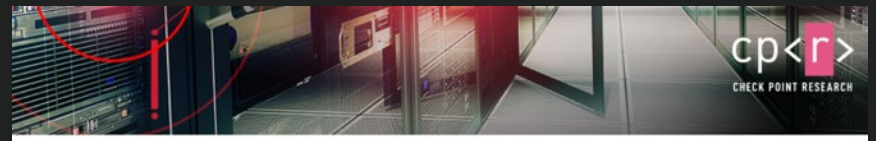
Samarbeid og utlevering av kriminelle

Greece Extradites Alleged Launderer of $4B in BTC Alexander Vinnik to France

Spore Tor

179 arrested in massive dark web bust

Publisering av forskning



Remote Cloud Execution – Critical Vulnerabilities in Azure Cloud Infrastructure (Part II)

Nedstenging av Botnet

Microsoft's Trickbot Takedown Offers Lessons for Cybersecurity Pros

Anbefalinger til slutt

Epost

- GULL for enhver angriper
  - Profilering av brukere
  - Kapre tråder
  - Misbruke relasjoner
- Hjemmekontor en utfordring
  - Færre sikkerhetsnett
  - Ingen kollegaer å spørre
  - Epost mer brukt mellom kollegaer

Identitets løsning (AzureAD, Okta, etc)

- Flere går over til SaaS
- Komplekst/vanskelig å forstå
  - Få kan se under panseret
- Få 3. parts verktøy
  - Skal man kun ha 1. lag?
  - Kan produsenten avdekke alt?
- **Viktig grunnstein i ZeroTrust**
  - Kan omgå multifaktor autentisering

Check Point
SOFTWARE TECHNOLOGIES LTD

TAKK FOR MEG

Pål H. Aaserudseter

Security Engineer