Kommune-CSIRT

Trusler i cyberdomenet mot kommunesektoren
- og hva kan kommunene gjøre med det?

Bjørn T. Tveiten, daglig leder

Kommune-CSIRT

Hjem > Aktuelt > Norconsult Digital utsatt for dataangrep

Norconsult Digital utsatt for dataangrep

Norconsult Digital ble i midten av juli utsatt for et omfattende dataangrep hvor uvedkommende forsøkte å få tilgang til informasjon på servere gjennom hackede brukerkontoer. Rask implementering av sikkerhetstiltak og god beredskapshåndtering har trolig avverget et mer alvorlig angrep. Systemene er nå i normal drift igjen.

Nyhet | Publisert 19.07.2023

Norconsult Digitals løsning «ISY Cloud» for drift av kundeapplikasjoner ble nylig rammet av et omfattende dataangrep hvor uvedkommende via brukerkontoer har forsøkt å få tilgang til servere. Selskapets kunder benytter disse til blant annet å hente ut informasjon til prosjekt- og forvaltningsløsninger, som f.eks. prosjektplanlegging, eiendomsregistre og kommunale tjenester.

12 departementer er utsatt for dataangrep

IKT-plattformen til 12 departementer er utsatt for dataangrep. Politiet etterforsker saken.

1 MIN | PUBLISERT: 24.07.23 — 08.24 | OPPDATERT: 21 DAGER SIDEN

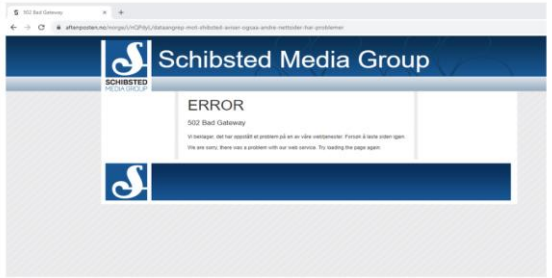
Tomra utsatt for «omfattende» dataangrep

Flere av gjenvinningsselskapets datasystemer er rammet, opplyser Tomra.

Tomra er utsatt for dataangrep. Arkivbilde fra hovedkontoret utenfor Asker. Foto: Thomas Bjørnflaten / NTB

Flere Schibsted-aviser rammet av dataangrep

Torsdag ettermiddag ble flere Schibsted-aviser og Finn.no utsatt for et dataangrep. Politiet vil ikke at utelukke at også de ble rammet av det samme.



NEDE: Slik ser aftenposten.no ut torsdag kveld.

Sverre Holm-Nilsen
Journalist
Berit Helle Jonsbråten
Journalist
Elise Pedersen
Journalist

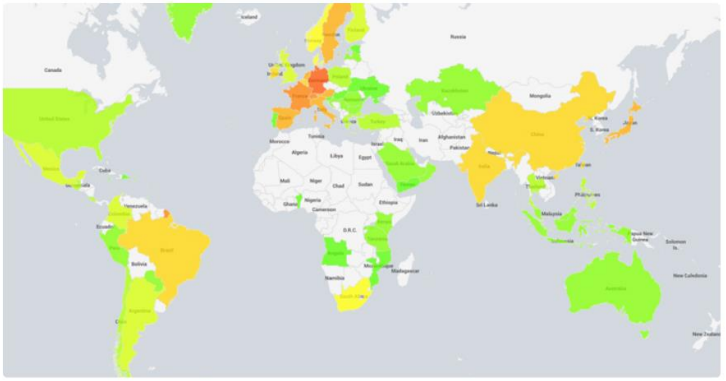
Publisert 27. juli kl. 18:26
Oppdatert 27. juli kl. 22:09

Angrepet mot Schibsted startet torsdag kveld, og rammet flere store aviser.

Bergens Tidende, Aftenposten og Stavanger Aftenblad var blant dem som hadde problemer.

Nearly 2,000 Citrix NetScaler Instances Hacked via Criti

Aug 16, 2023 THN Vulnerability / Enterprise Security



Nearly 2,000 Citrix NetScaler instances have been compromised with a backdoor by weaponizing a recently disclosed critical security vulnerability as part of a large-scale attack.

"An adversary appears to have exploited CVE-2023-3519 in an automated fashion, placing web shells on vulnerable NetScalers to gain persistent access," NCC Group said in an advisory released Tuesday.

MOVEit Cyber Attack - Affected organizations (as of September 14, 2023)

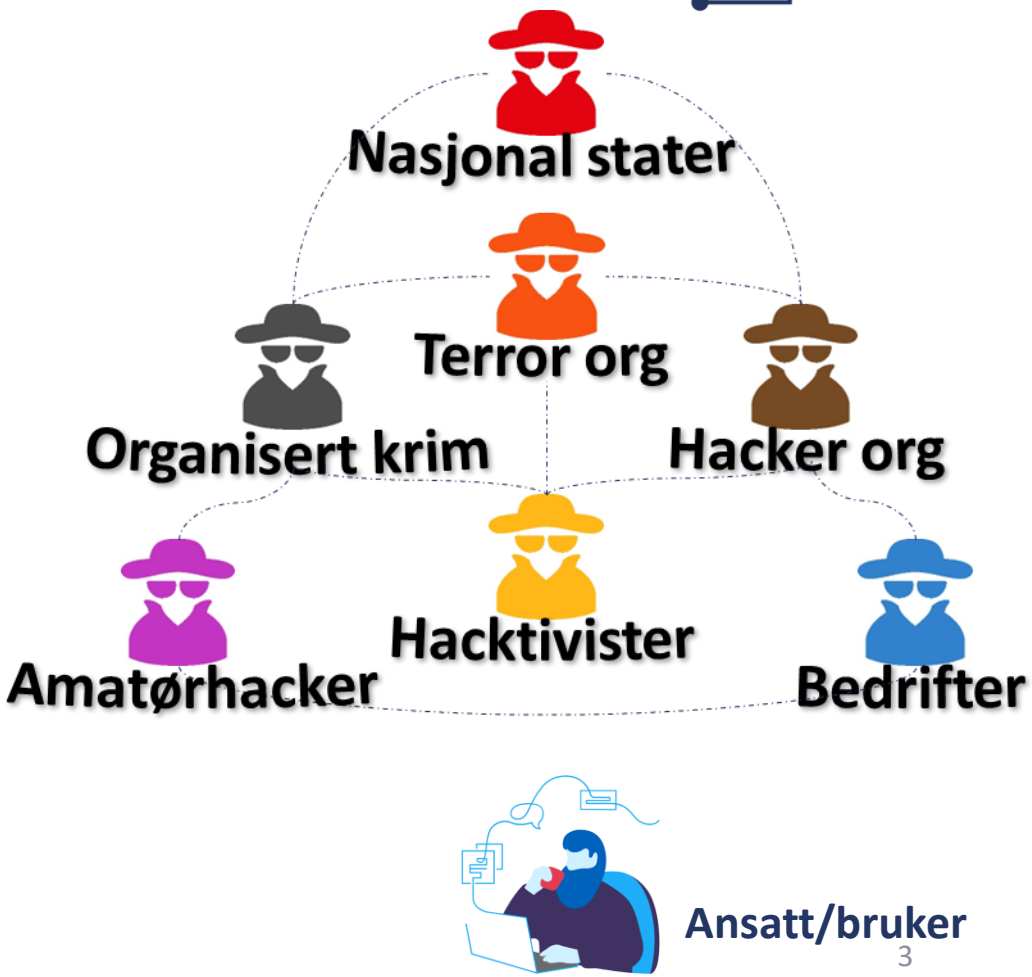
By country

6 ??	5 Australia	4 Austria	1 Belgium	2 Bermuda
1 Brazil	36 Canada	2 China	1 Denmark	1 Finland
5 France	37 Germany	1 Guatemala	3 India	6 Ireland
1 Israel	1 Italy	2 Japan	1 Luxembourg	3 Malaysia
10 Netherlands	1 Norway	1 Oman	2 Philippines	1 South Africa
1 Spain	2 Sweden	9 Switzerland	2 Turkey	1 UAE
24 UK	973 USA			

KonBriefing Research

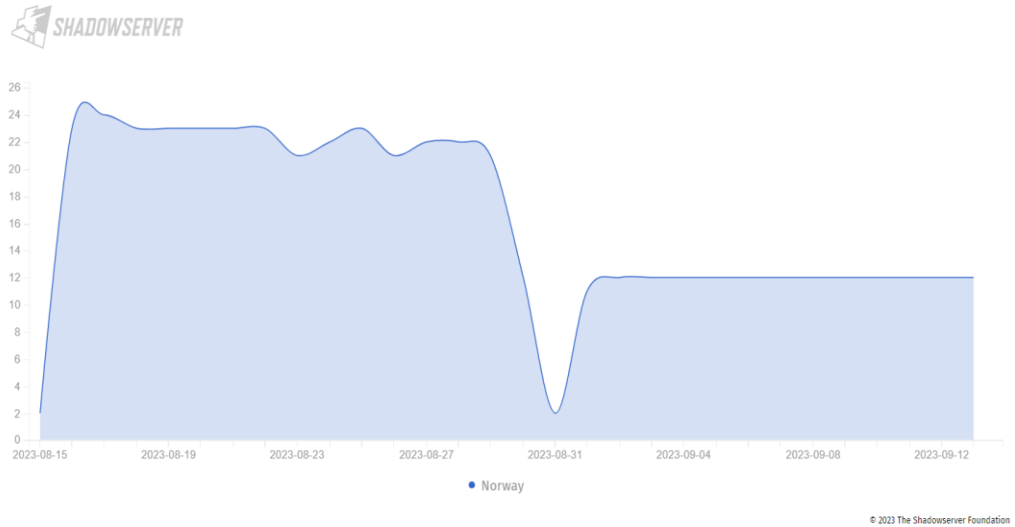
Digitale trusler

- Digital utpressing/ransomware
- Datatyveri/utnyttede informasjonslekkasjer
- Tjenestenektangrep
- Økonomisvindel
  - Direktørsvindel
  - Fakturasvindel
- Spionasje
- Sabotasje mot kritiske systemer og infrastruktur
- Misbruk av kommunens ressurser
- Sikkerhetsbrudd / brudd på personvern



Alvorlige sårbarheter utnyttet mai-september 2023

- MOVEIt – utnyttet spesielt av Cl0p
- Citrix ADC / Netscaler
- MobileIron Core/Ivanti Epmm (12 DEP-hacket)



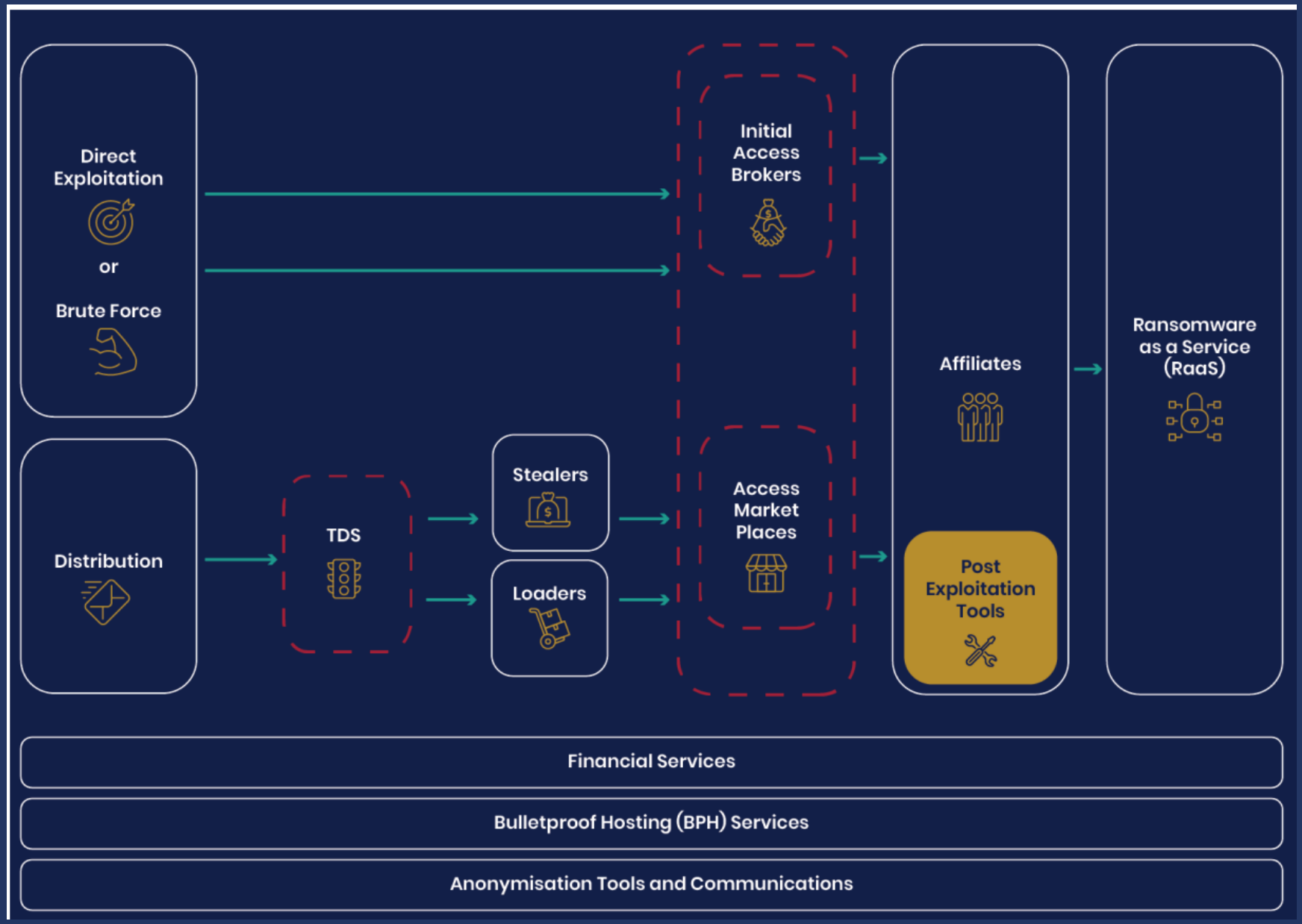
Inngangsvektorer

- Passord på avveie
- Default passord
- Brute force / svake passord
- Phishing
- Annen form for skadevare-lasting (USB-minne, delingstjenester)
- Sårbare eksponerte tjenester / utdatert teknologi
- Nulldagssårbarheter
- Eskalering av privilegier

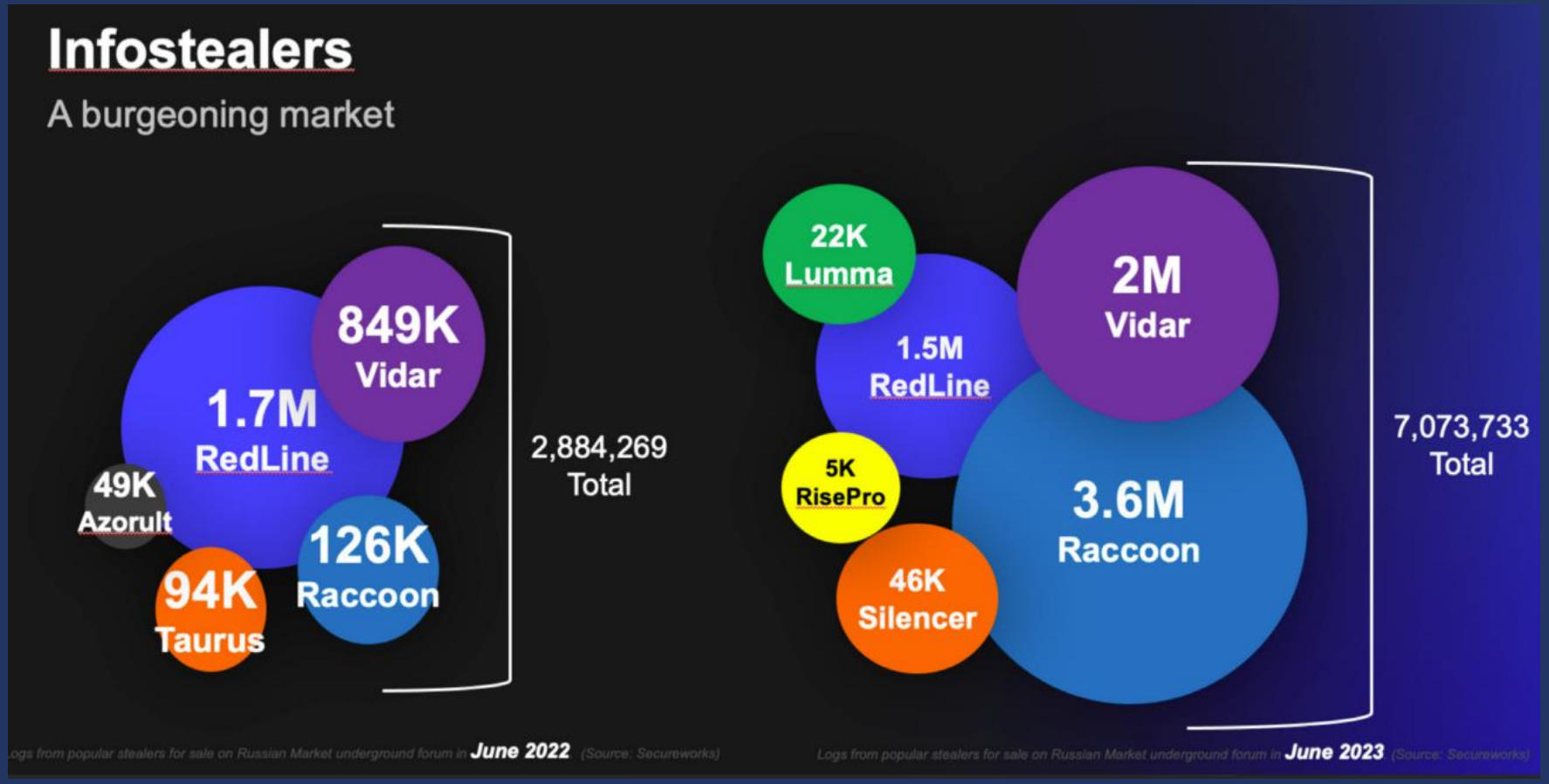
Ansatt/bruker/leverandør

Samarbeid mellom kriminelle grupper - digital utpressing.

Verdikjeder og støttetjenester.



Infostealer-markedet



Trusselaktørenes angrepskjede og -teknikker

(Kilde: Analyst1)

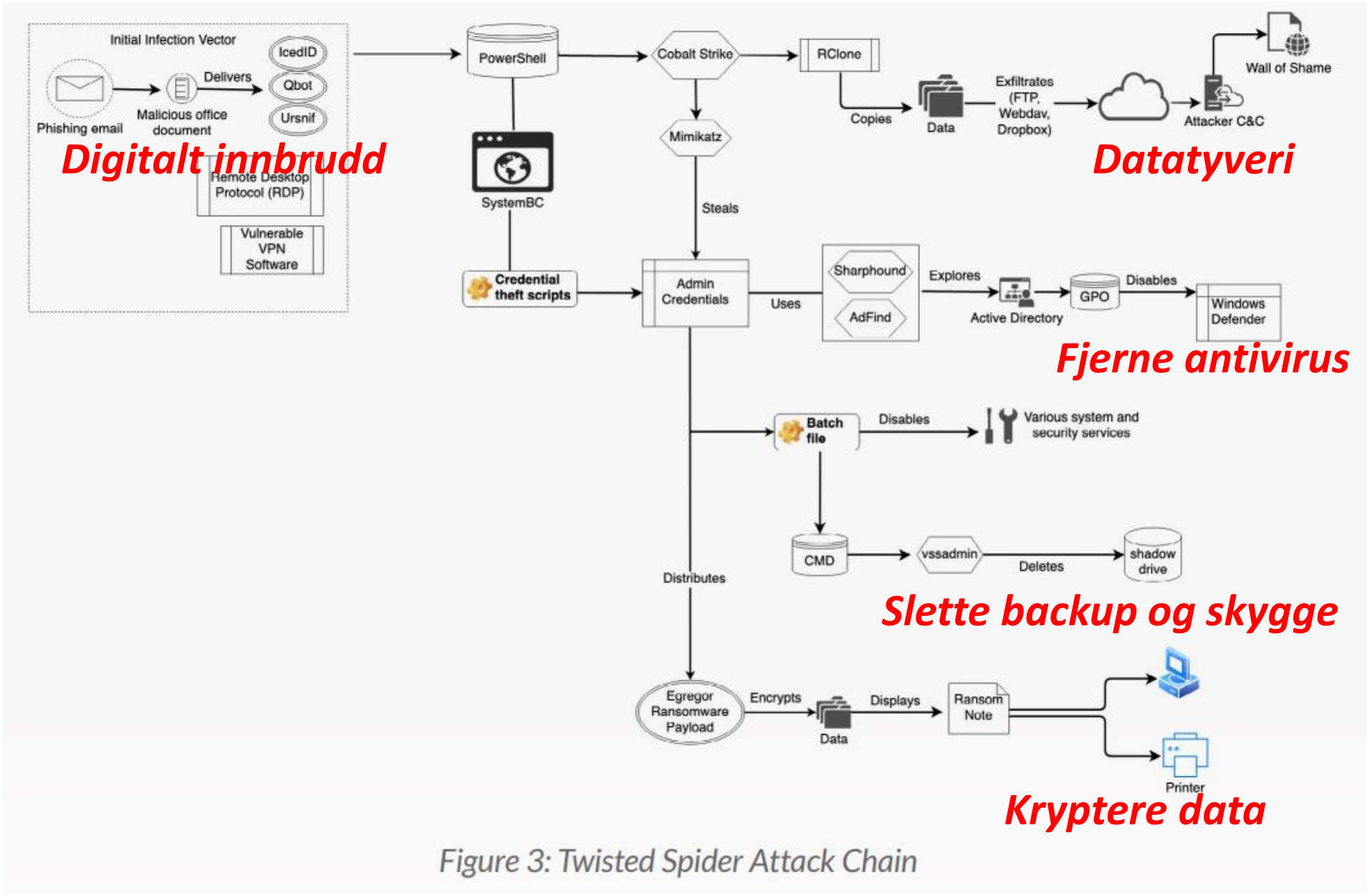
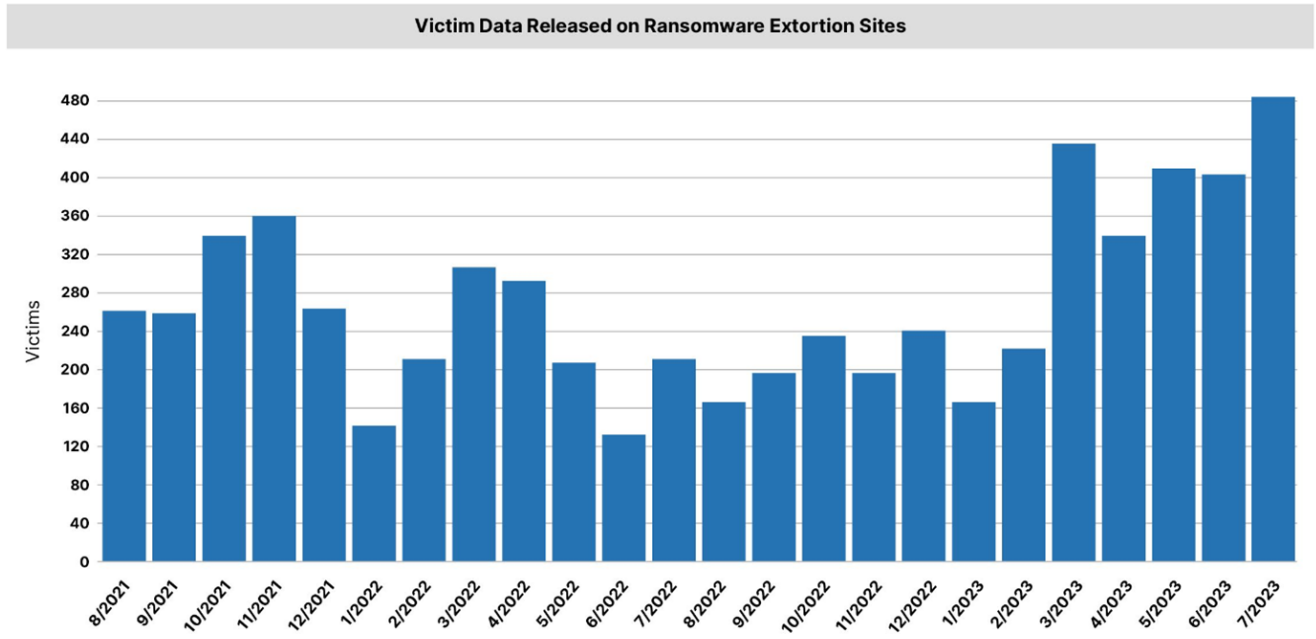


Figure 3: Twisted Spider Attack Chain

Trender – 2023

- 2022 bar preg av usikkerhet og krigen i Ukraina, men fasit viser en betydelig nedgang i alvorlige kompromitteringer i Norge
- Det rapporteres likevel om høyere angrepsvolum i 2022 enn i 2021 fra utstyrsleverandører og sikkerhetsbransjen forøvrig
- Årsaken til nedgangen kan være en kombinasjon av redusert betalingsvilje hos ofrene, bedret sikkerhet og fragmentering av de kriminelle gruppene (pga krigen)
- Første kvartal 2023 preges av angrep mot norske kommuner i nord, og mer tjenestenektangrep fra russiske hacktivister mot sentrale norske nettjenester. Hacktivismen har fortsatt utover i 2. og 3. kvartal.
- Den globale statistikken for første halvår-23 viser en markant økning i antall tilfeller og omsetning fra digital utpressing/ransomware sammenliknet med fjoråret



The Record.
Recorded Future® News

Trusselbildet mot norske kommuner – 2023

- Digital utpressing mot kritiske funksjoner (f. eks. vannforsyning). Enkelte ransomware-aktører melder om økt innsats mot dette offersegmentet
- «Stealer»-skadevare øker i omfang, rammer også kommuner og fylkeskommuner
- Russiske hacktivist-gruppers tjenestenektangrep påvirker også kommunene – ref Ddos mot statlige tjenester påvirket ACOS sine tjenester
- To trender hos ransomware-aktørene:
  - Økt profesjonalisering
  - Mer opportunistiske angrep, dermed kan flere bli rammet
- Direktørsvindel og falske fakturaer vil fortsatt være utbredte kriminelle metoder for å skaffe penger.
- MFA-omgåelse vil øke i omfang, men MFA er fremdeles mye bedre enn singlefaktor-autentisering! Direktørsvindel vha MFA-omgåelse observert i norsk kommune.

Kommunenes evne til å bekjempe truslene

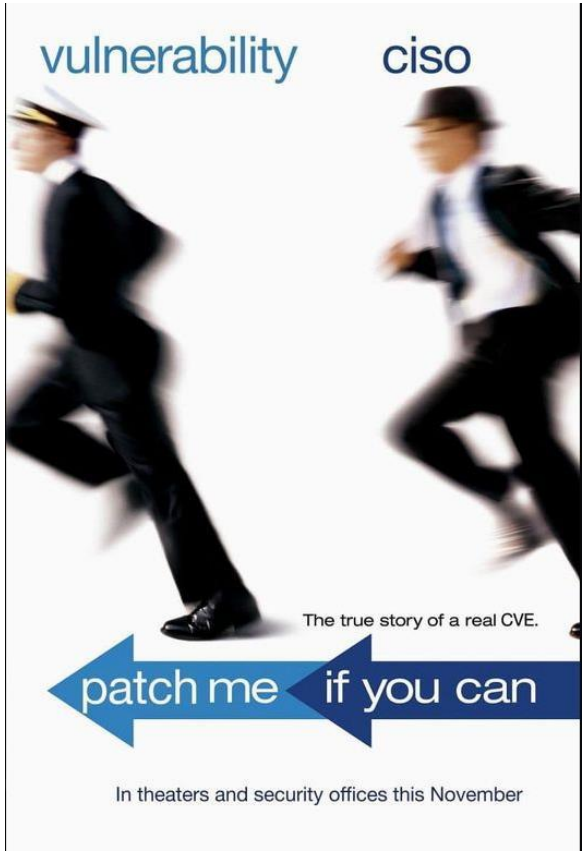
- Kommunene trenger
  - Kompetent personell
  - Gode prosesser, sikkerhetsbevissthet og -kultur
  - Egnede verktøy og støttefunksjoner
- Hva er tilstanden der ute?
  - Store kommuner: Ganske bra
  - Middels store kommuner: Det varierer mye
  - Små kommuner: Det varierer mye

2-delt tilnærming og strengere regelverk må til

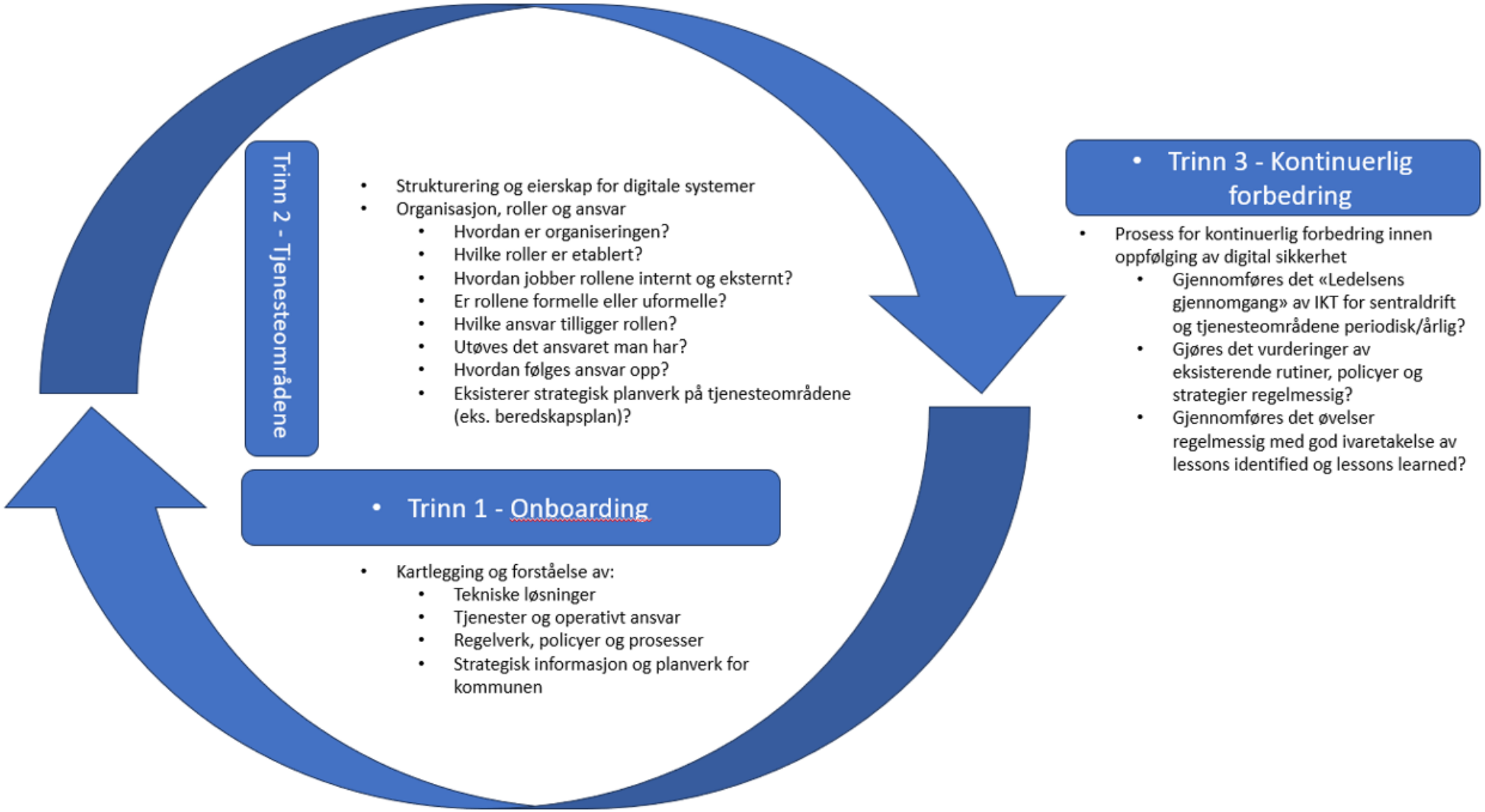
- 2-delt tilnærming
  - Akutt utbedring av sårbarheter – bottom up
  - Cyberstrategi-prosesser top-down, langsiktig
- Strengere styring
  - Krav (og ikke flere anbefalinger) fra statlige myndigheter
  - Oppfølging og kontroll internt/via partner
  - Ekstern revisjon av tilstanden

Mottiltak - akutt

- Bruk multifaktor-autentisering for ***all*** tilgang utenfra **(inkl. leverandører)**
- Unngå aktivering av innhold i e-poster!
- Sørg for reell offline backup
- Fjern utrangert utstyr
- Vær spesielt oppmerksom på sårbarheter i tekniske styringssystemer (VA, SD-anlegg)
- Vær oppdatert – sørg for et effektivt og raskt oppdateringsregime
- Kontinuerlig opplæring og øvelse av brukere i operativ cybersikkerhet – sikkerhetsbevissthet fra toppledelse til vanlig ansatte
- Vær forberedt!
    - Opprett, vedlikehold og tren på planer for å svare på et angrep og gjenopprette driften etter en krise



K-CSIRTs trinnvise prosess for økt modenhet



Takk for oppmerksomheten.

Spørsmål?

https://kommunecsirt.no

bjorn@kommunecsirt.no

T. 90 85 00 42