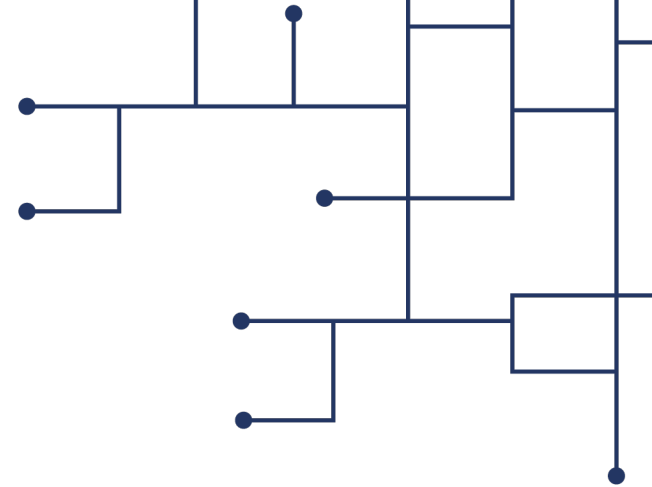




# Erfaringer med cybersikkerhet i VA-sektoren

*Bjørn T. Tveiten, Kommune-CSIRT*

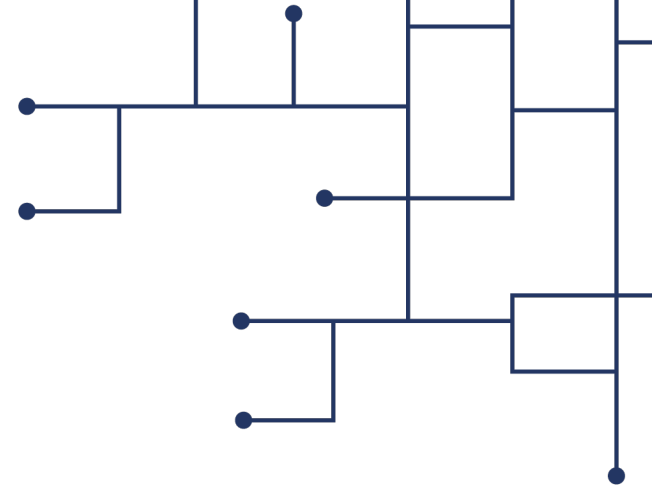
*28.oktober 2021*



## Innhold

- Situasjonsbilde
- Digitalisering/automasjon
- CISA situasjonsbilde og anbefalinger
- Egne erfaringer





## Kommune-CSIRT så langt (oktober-21)

- Nå nær 40 medlemmer, inkludert én fylkeskommune
- Deltar fullt ut i SRM-samarbeidet (NSM er vertskap)
- Onboardingsprosess i gang for nesten alle
- Leverer rapporter, varsler, trusseletterretning, rådgivning og situasjonsbilde
- Medlemsmøte med erfaringsutveksling 2-3 ganger per år
- Opptapping av ressurser – 2 nye ansatte i aug/sep



## Vannforsyning/vannverk er

- kritisk tjeneste for innbyggere, offentlige forvaltning og virksomheter
- (og dermed også) kritisk infrastruktur
- grunnleggende nasjonal funksjon?
- kommunenes ansvar
- definert som kritisk tjeneste av EU (NIS/GDPR)



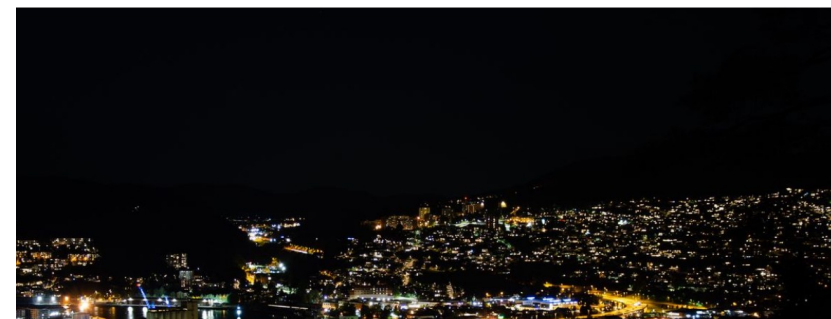


## Skandaløs datasikkerhet i kommune-Norge - Østre Toten fikk Norges strengeste bot



RAMMET AV PYSA: Politiet har opplyst kommunedirektør Ole Magnus Stensrud om at den avanserte IT-banden opererte fra servere i Nederland og Tyskland da den angrep Østre Toten kommune 9. januar i år. Foto: Illustrasjonsbildearkiv

## Politiet etterforsker hackerangrep mot vann- og avløp i Drammen kommune



## Rørledningen Colonial Pipeline ble angrepet via bortglemt konto

Passordet ble delt på den mørke weben.



## Dataangrep på deler av Volues virksomhet

Onsdag ble deler av Volues virksomhet utsatt for dataangrep. Utover kvelden onsdag ble det klart at dette i første rekke påvirket Volue Technology, tidligere Powel. Det er snakk om et løsepenger-angrep.



## Digitalisering av teknisk sektor og VA

- Parallelle digitaliseringsløp i kommunen
- Uavhengighet/selvråderett
- VA er ingeniørdrevet med høy faglig stolthet
- Ofte ikke synkronisert med IT-avd på cybersikkerhetsområdet
- Kraftig økning av kompleksiteten og automatiseringen (SCADA, kartverk, alarmsystemer, målinger, kontinuerlig rapportering)
- Leverandører og automatikere har ofte ekstern tilgang og høyeste mulige rettigheter

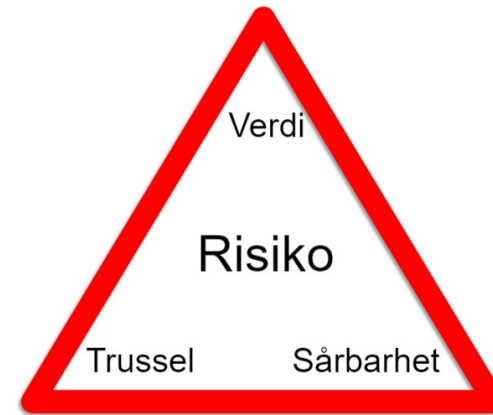


## CISA vurdering av trusler mot ICS (datert 2021-10)

- Spearphishing-angrep inkludert ransomware
- Utnyttelse av usupportert eller utdatert operativsystem og programvare
- Utnyttelse av kontrollsystemer med sårbar firmware



RISIKOTREKANTEN



$$\text{Risiko} = \text{Trussel} \times \text{Sårbarheter} \times \text{Verdi}$$



En liste over dobbelt-utpressergrupper

By administrator

June 15, 2021

For sale company data

<https://www.sincor.org.br/>

Random SAMPLES

Status: For Sale

//

By administrator

June 15, 2021

Status: Company paid, data is not for sale

//

By administrator

June 14, 2021

Status: Company paid, data is not for sale

//

By administrator

June 11, 2021

For sale company data

<https://www.elmich.com/>

Random SAMPLES

Status: SOLD

Eksempel på leak site på det mørke nettet

Id.	Name	No. of Victims	Estimated Earnings	Confirmed Earnings	Onion Site	Status
1	Conti	444		\$12,720,000	<a href="#">Link</a>	Up
2	REvil	282	\$100,000,000	\$12,130,000	<a href="#">Link</a>	Down
3	MAZE	266			Shutdown	-
4	Egregor	206	\$75,000,000	\$3,120,000	Shutdown	-
5	DoppelPaymer	203			<a href="#">Link</a>	Up
6	Pysa	190			<a href="#">Link</a>	Down
7	Avaddon	182			<a href="#">Link</a>	Down
8	NetWalker	144		\$27,350,000	Shutdown	-
9	DarkSide	99	\$90,000,000	\$4,670,000	<a href="#">Link</a>	Down
10	CL0P	67			<a href="#">Link</a>	Up
11	Prometheus	48			<a href="#">Link</a>	Up
12	BABUK LOCKER	43			<a href="#">Link</a>	Up
13	Everest	41			<a href="#">Link</a>	Down
14	Nefilim	40			<a href="#">Link</a>	Up
15	LV	40			<a href="#">Link</a>	Up
16	Marketo	39			<a href="#">Link</a>	Down
17	Ragnarok	33			<a href="#">Link</a>	Down
18	Ragnar_Locker	29		\$4,540,000	<a href="#">Link</a>	Down
19	RansomEXX	23			<a href="#">Link</a>	Up
20	Suncrypt	22			<a href="#">Link</a>	Down
21	Grief	22			<a href="#">Link</a>	Up
22	Mount Locker	20		\$4,220,000	<a href="#">Link</a>	Down
23	XING LOCKER	20			<a href="#">Link</a>	Up
24	Lorenz	19			<a href="#">Link</a>	Up
25	Astro Team	16			<a href="#">Link</a>	Down
26	Cuba	12			<a href="#">Link</a>	Up
27	Vice Society	12			<a href="#">Link</a>	Up
28	LockBit	12			<a href="#">Link</a>	Down
29	AKO	9			Shutdown	-
30	SynACK	7			<a href="#">Link</a>	Down
31	Sekhmet	6			Shutdown	-
32	Pay2Key	6			<a href="#">Link</a>	Up
33	Team Snatch	6			Shutdown	-
34	Noname	6			Shutdown	-
35	AvosLocker	6			<a href="#">Link</a>	Up
36	Hive	5			<a href="#">Link</a>	Up
37	N3tw0rm	4			Shutdown	-
38	Ranzy Locker	3			<a href="#">Link</a>	Down
39	Payload.bin	2			Shutdown	-
40	NEMTY	1			Shutdown	-

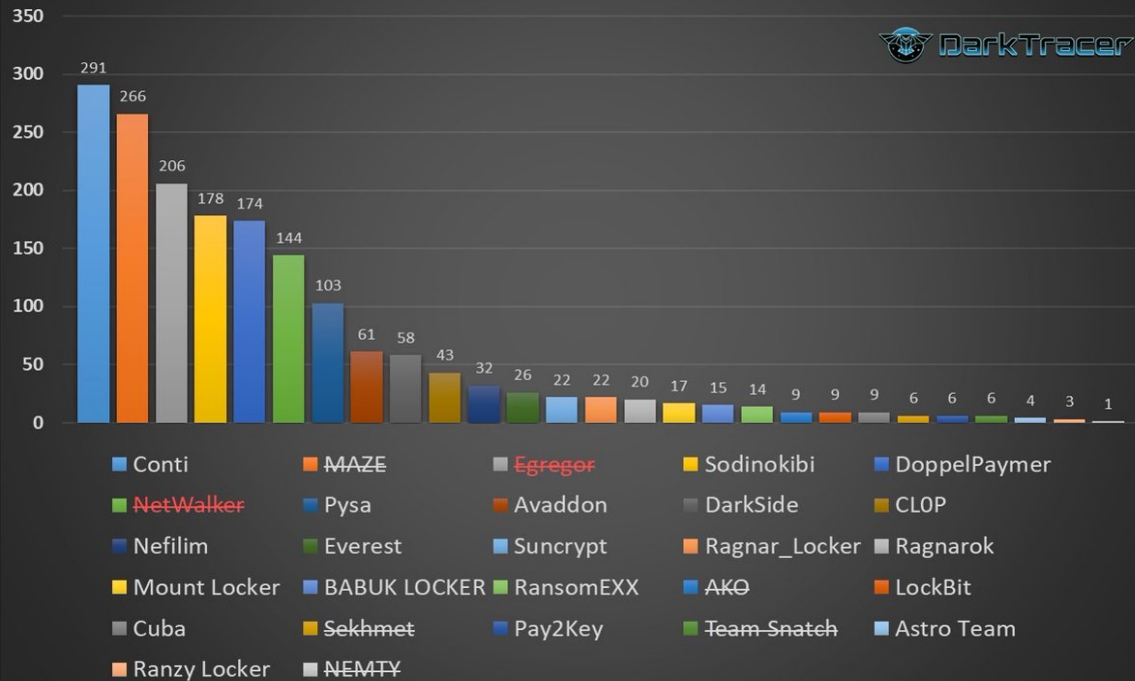
Kommune-CSIRT IKS - et felles løft for informasjonssikkerhet i kommunesektoren

9



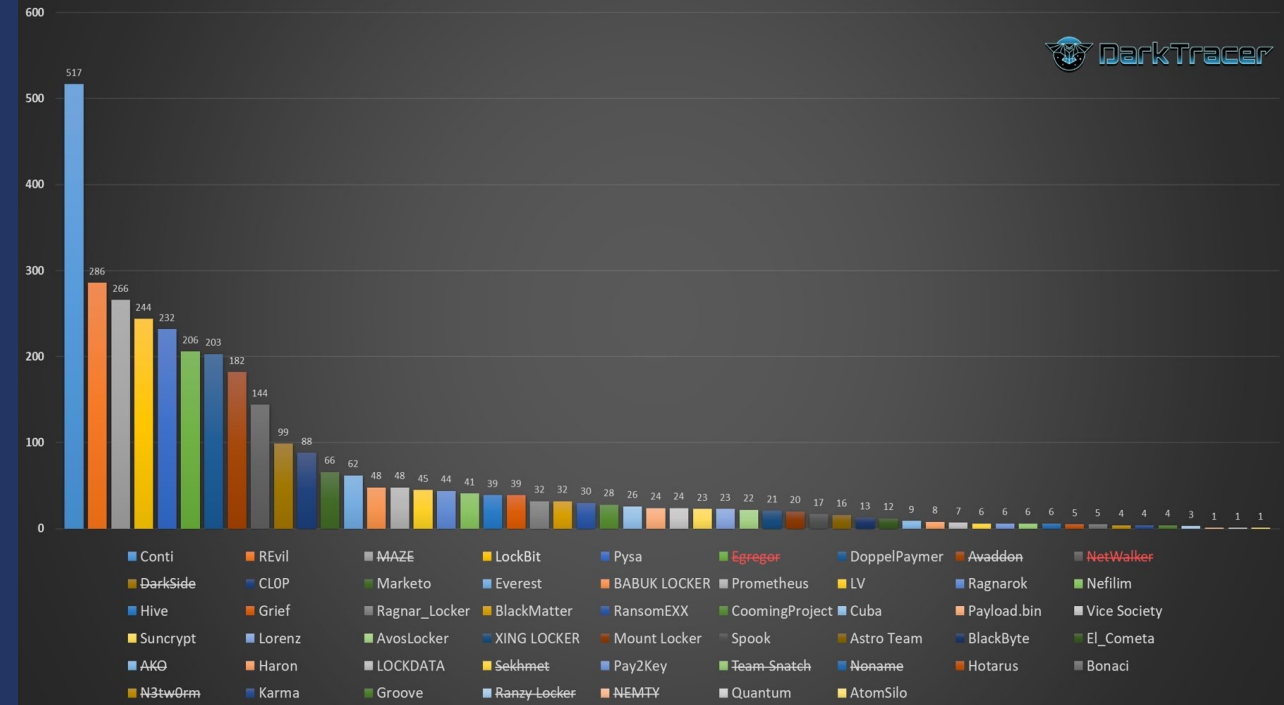
22.03.2021

Who is the King of Ransomware on the DarkWeb?  
(number of affected organizations)



08.10.2021

Who is the King of Ransomware on the DarkWeb?  
(number of affected organizations)





# Kriminell struktur





## Verdikjede-betraktning

1. Stjele login/passord

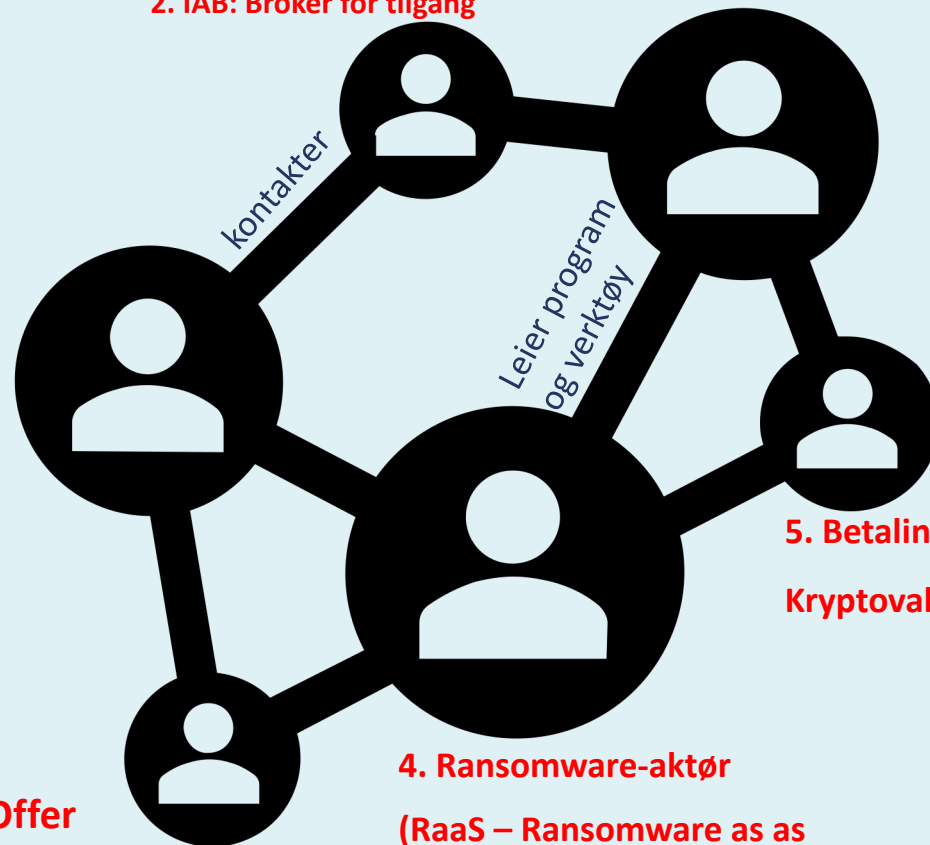
2. IAB: Broker for tilgang

3. Kjøper av tilgang, vil kjøre  
svindelprosessen

Offer

4. Ransomware-aktør  
(RaaS – Ransomware as  
Service)

5. Betalingsspesialist,  
Kryptovaluta (vasking)







## Twisted Spider angrepskjede og teknikker

(Kilde: Analyst1)

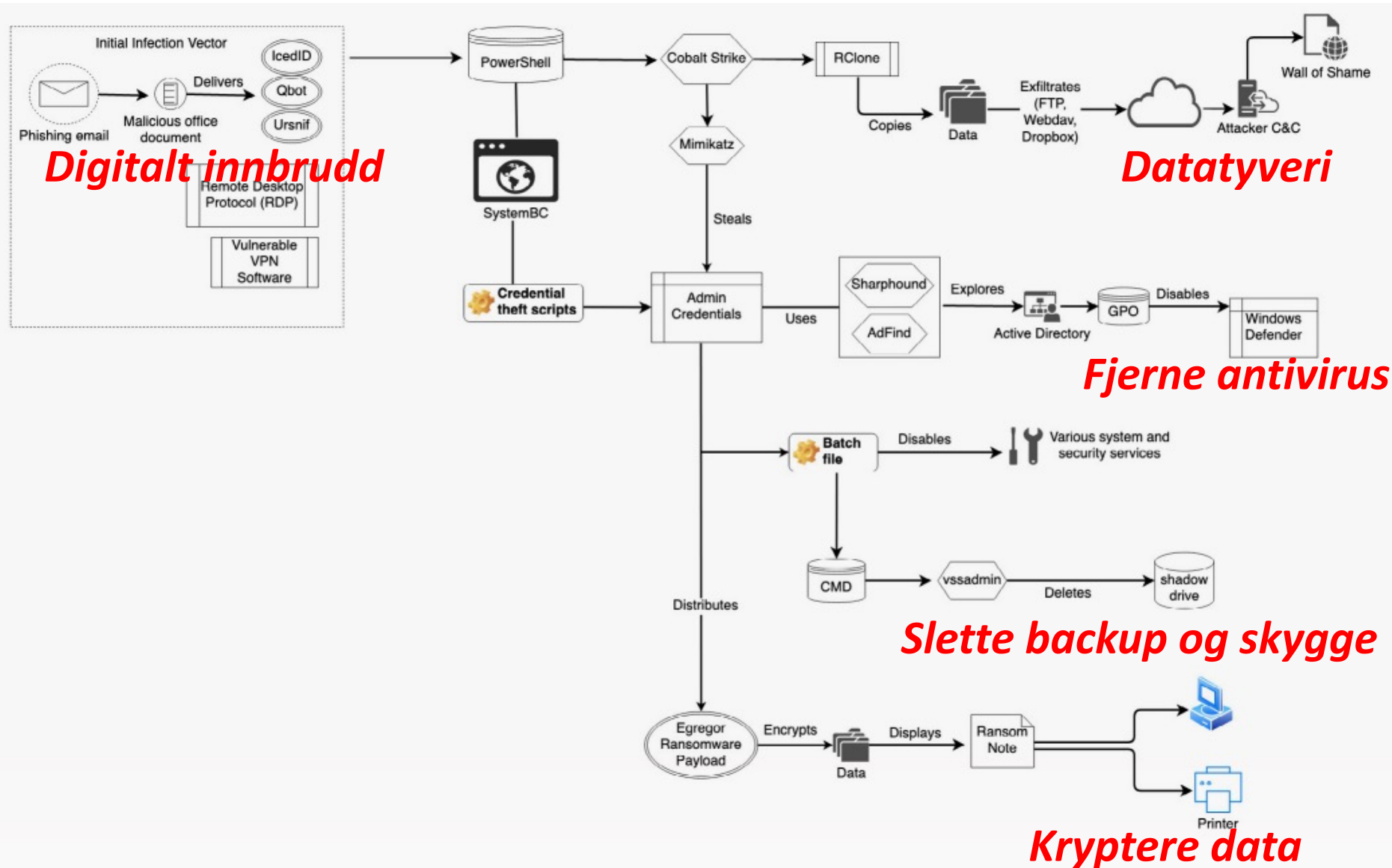


Figure 3: Twisted Spider Attack Chain



## Hvor holder skurkene til? Eller...



Russian - 419	Azerbaijani (Latin) - 42C	Uzbek (Latin) - 443	Uzbek (Cyrillic) - 843
Ukranian - 422	Georgian - 437	Tatar - 444	Arabic (Syria) - 2801
Belarusian - 423	Kazakh - 43F	Romanian (Moldova) - 818	
Tajik - 428	Kyrgyz (Cyrillic) - 440	Russian (Moldova) - 819	
Armenian - 42B	Turkmen - 442	Azerbaijani (Cyrillic) - 82C	

Kilde: Darkside/Cybereason/Krebsonsecurity



## Cl0p ransomware-bande arrestert?







Men nei, det var bare  
pengevaskerne som ble tatt!

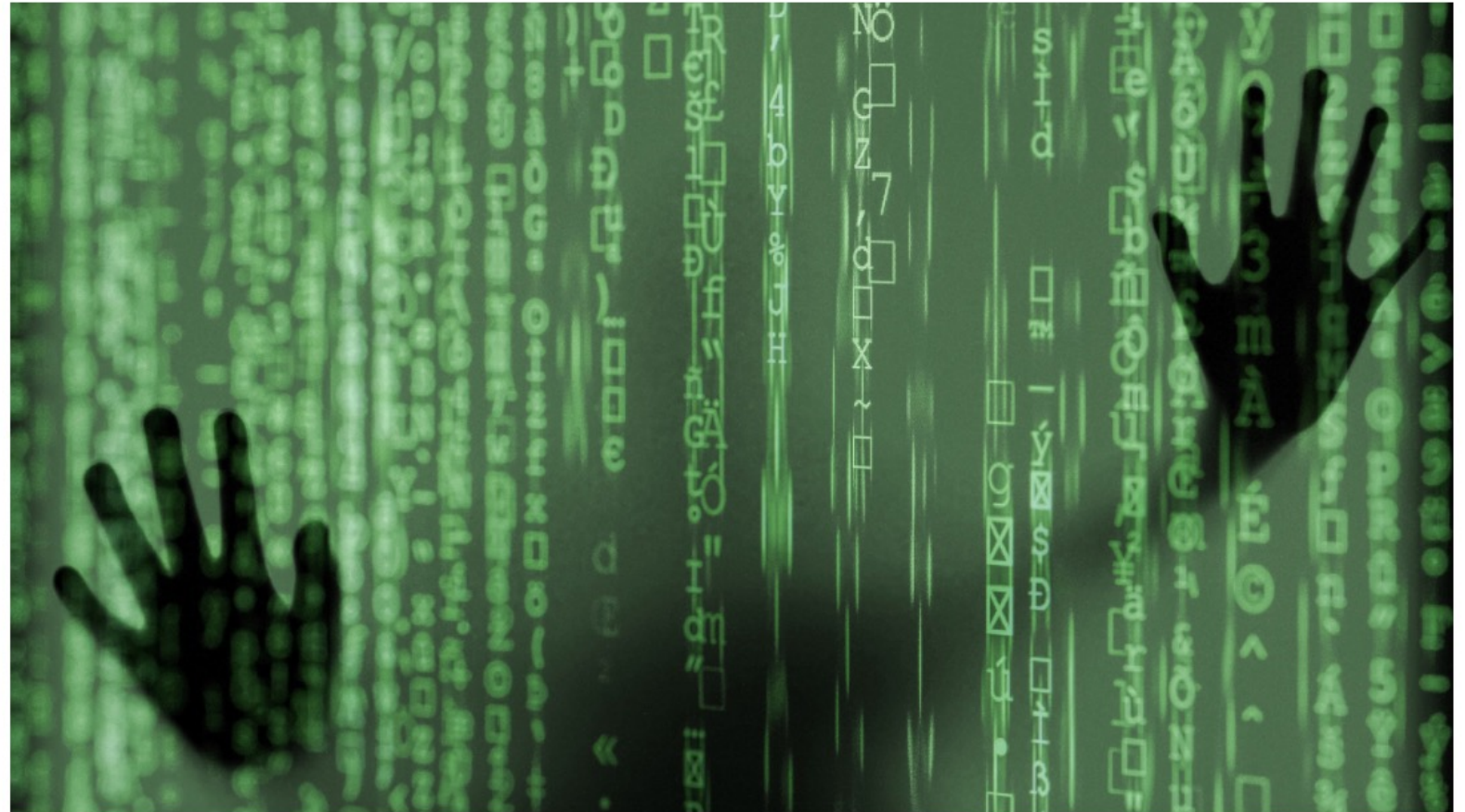
## Clop ransomware is back in business after recent arrests

By [Lawrence Abrams](#)

June 23, 2021

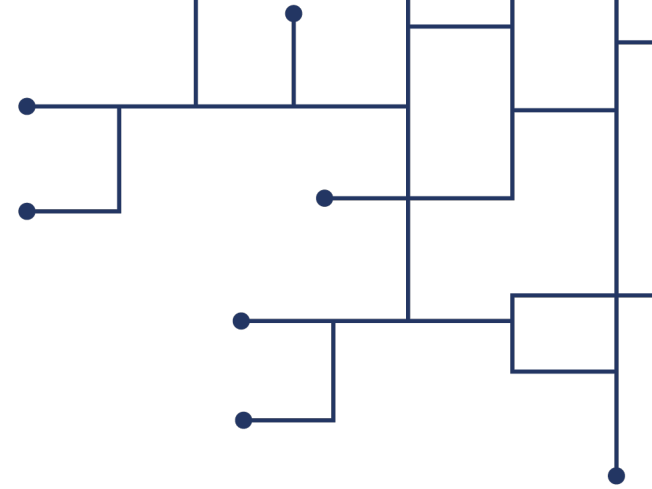
03:35 AM

0



The Clop ransomware operation is back in business after recent arrests and has begun listing new victims on their data leak site again.

Last week, a law enforcement operation conducted by the National Police of Ukraine, the Korean National Police Agency, and the USA led to the [arrest of Clop Ransomware gang](#) members.

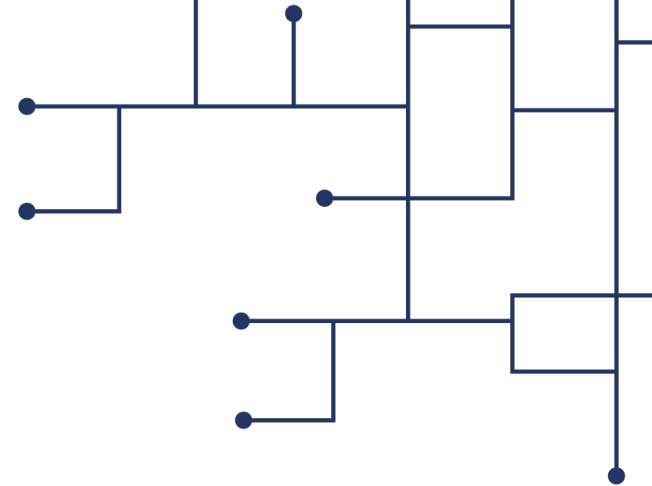


## Risikoelementene knyttet til cyberangrep

- Verdi
  - Leveranse av rene og uskadelige produkter iht behov
  - Graderte data, personopplysninger/helse, IP, forskning, konkurransesensitivitet ++
  - Krav om oppetid/tilgjengelighet, sikring av dataintegritet og konfidensialitet
  - Økonomi/kostnader
- Sårbarheter
  - Kontinuerlig rekke (nye produkter, mer komplekse, mer integrasjon, på alle enheter ++)
- Trusler
  - Mer avanserte. Flere. Raskere. -> Økende fare.

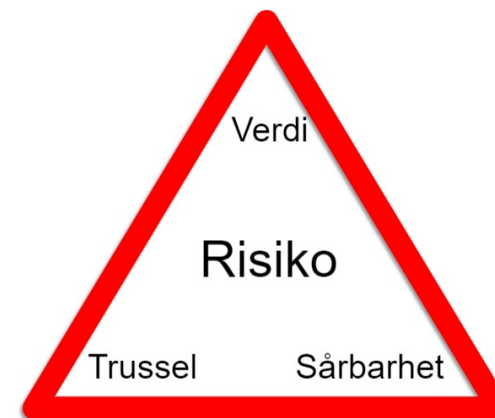
**Risiko = Trusler x Sårbarheter x Verdi (Konsekvens/skadeomfang)**





# Konsekvenser

RISIKOTREKANTEN

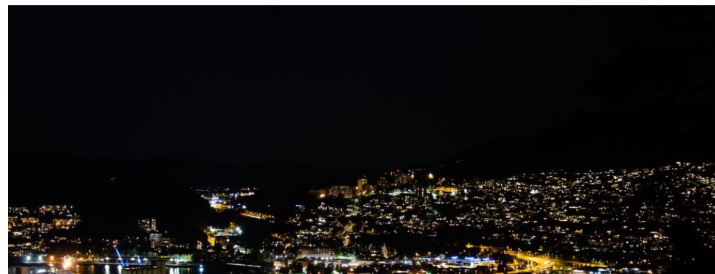






HACKERANGREP MOT DRAMMEN KOMMUNE

## Politiet etterforsker hackerangrep mot vann- og avløp i Drammen kommune



## Dataangrep på deler av Volues virksomhet

Onsdag ble deler av Volues virksomhet utsatt for dataangrep. Utover kvelden onsdag ble det klart at dette i første rekke påvirket Volue Technology, tidligere Powel. Det er snakk om et løsepenger-angrep.

## Meat giant JBS pays \$11m in ransom to resolve cyber-attack

© 10 June



UTPRESSINGSVARE

## Rørledningen Colonial Pipeline ble angrepet via bortglemt konto

Passordet ble delt på den mørke weben.



## Skandaløs datasikkerhet i kommune-Norge - Østre Toten fikk Norges strengeste bot



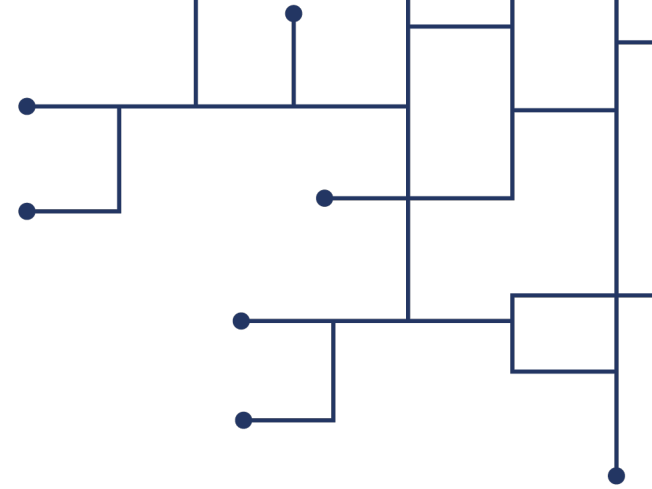
RAMMET AV PYSA: Politiet har opplyst kommunedirektør Ole Magnus Stensrud om at den avanserte IT-banden opererte fra servere i Nederland og Tyskland da den angrep Østre Toten kommune 9. januar i år. Foto: Illustrasjonsbilde/arkiv

KASEYA

## Selskaper verden over rammet: Svenske Coop-butikker stengt etter hackerangrep

Dagligvarekjeden Coop har stengt nesten alle sine 800 butikker i Sverige etter et IT-angrep med kobling til internasjonal hacking.



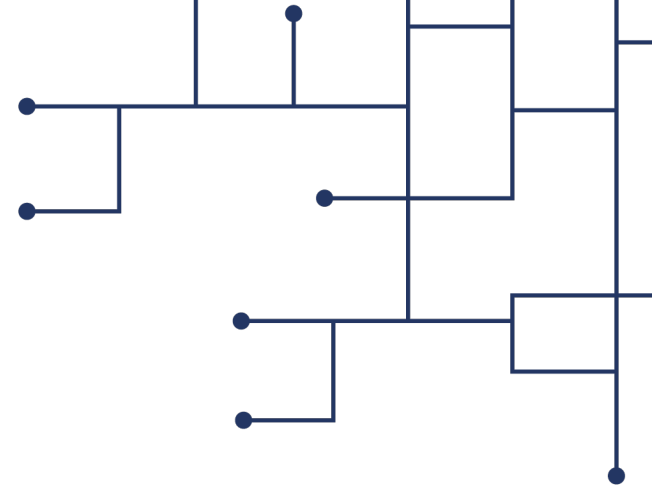


## Våre funn/observasjoner

(gjelder noen VA-org)

- Manglende sikkerhetskontroll for ekstern pålogging
- Manglende eller for svak oppdateringsprosess/patcheregime (for sjelden og ikke out-of-band)
- Manglende sikkerhetsrevisjoner/gjennomganger
- Manglende segmentering mellom tilgang, SCADA og DKS
- Liten eller ingen samkjøring av sikkerhetskrav og -løsninger med IKT-avd.





## Mottiltak

- Vær forberedt!
  - Opprett, vedlikehold og tren på planer for å svare på et angrep og gjenopprette driften etter en krise
- Sørg for reell offline backup
- Bruk multifaktor-autentisering
- Vær oppdatert – bygg et effektivt og raskt patcheregime
- Fjern utrangert utstyr
- Kontinuerlig opplæring og øvelse av brukere i operativ informasjonssikkerhet – sikkerhetsbevissthet fra toppledelse til vanlig ansatte



**Takk for oppmerksomheten.**

**Spørsmål?**

**<http://kommunecsirt.no>**

**[bjorn@kommunecsirt.no](mailto:bjorn@kommunecsirt.no)**

**T. 90 85 00 42**