Skreddersydd dobbeltangrep mot Hydro

By Henrik Lied, Peter Svaar, Dennis Ravndal, Anders Brekke, Kristine Hirsti

Published: 2019-03-19 · Archived: 2026-04-05 22:01:29 UTC

Etter det NRK får opplyst, har Nasjonalt Cybersikkerhetssenter (NorCERT) sendt ut et varsel til en rekke samarbeidspartnere om dagens dataangrep på Hydro.

Alle offentlige virksomheter i Norge er nå satt i beredskap for å se etter ytterligere spredning av denne typen løsepengevirus.

- **NRKbeta forklarer:** Løsepenge-viruset «WannaCry»

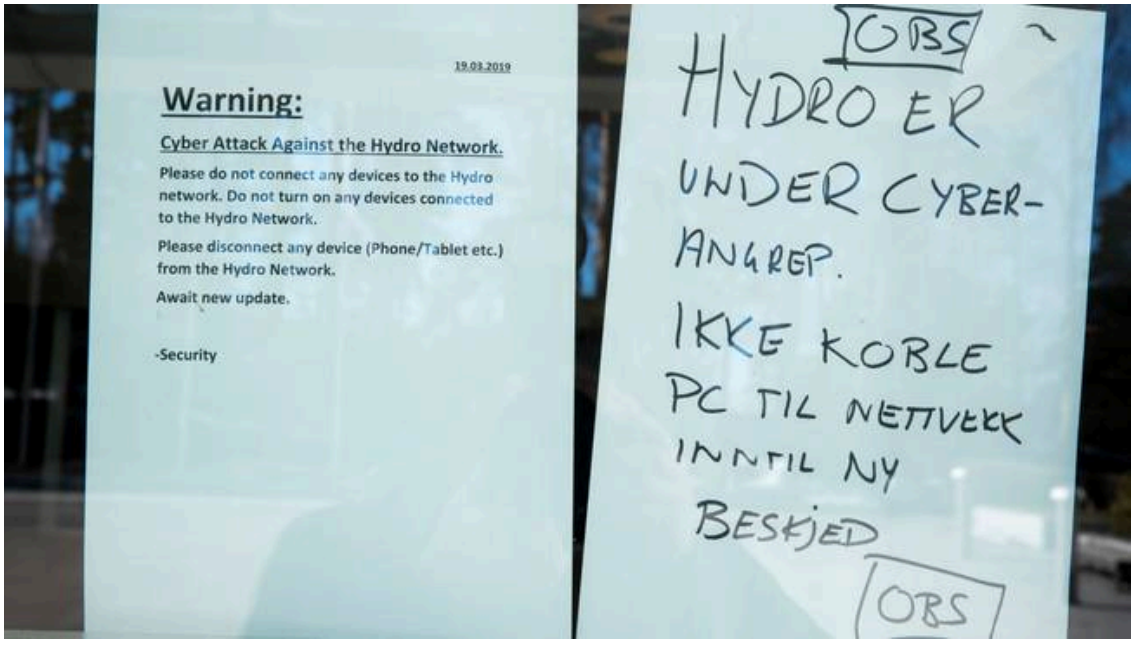
Løsepenge-virus

«NorCERT varsler om at Hydro er utsatt for et ransomwareangrep (LockerGoga). Angrepet ble kombinert med et angrep mot Active Directory (AD).

NorCERT ber om informasjon om andre er rammet av tilsvarende hendelser. NorCERT bistår Hydro og hendelsen regnes som pågående», står det i varselet.

I klartekst betyr dette at data-angriperne både har brukt et såkalt løsepengevirus (ransomware), som gjør alt innholdet på datamaskinen utilgjengelig, samtidig som det foregår et angrep mot Hydros bruker- og påloggingssystemer (active directory).

– Jeg vil ikke bekrefte at det dreier seg om et active directory-angrep, sier Håkon Bergsjø, leder for NorCERT.



Hydro har varslet alle ansatte om å ikke skru på datamaskinene sine eller koble til nettverket.

Foto: Terje Pedersen / NTB scanpix

– Alvorlig

Hydro holdt en pressekonferanse tirsdag ettermiddag, der finansdirektør Eivind Kallevik bekreftet at systemet er rammet av et krypteringsvirus.

– Situasjonen er alvorlig. Hele det globale nettverket er nede. Vi jobber hardt for å begrense viruset og løse situasjonen. Det har ikke ført til noen andre sikkerhetsrelaterte hendelser, sier Kallevik.

Hydro vet ikke hvem som står bak eller når systemene kan bli friskmeldt. Ifølge Kallevik er det ikke et tema å etterkomme eventuelle krav om løsepenger.

– Vi har gode backup-rutiner. Hovedstrategien er å reinstallere data fra backupsystemene, sier han.

Anleggene er nå isolert fra systemet for å hindre spredning, og Hydro har fått hjelp fra eksterne eksperter til å identifisere og analysere viruset.

– Vi jobber døgnet rundt til problemet er løst. Produksjonen går som normalt, og vi gjør det vi kan for å minimere konsekvensene for kundene, sier Kallevik.

Hydros finansdirektør Eivind Kallevik.

Foto: Fredrik Hagen / NTB scanpix

«Nytt» virus

Løsepenge-viruset som er blitt brukt i angrepet mot Hydro heter LockerGoga, og ble oppdaget for første gang i januar. Den gang ble det brukt mot det franske konsulentfirmaet Altran.

– Dette var et løsepengevirus som brukte en helt ny kode. Denne kunne ikke oppdages selv med den beste type brannmur og datasikkerhetsløsninger, skriver de i en pressemelding.

Håkon Bergsjø i NorCERT.

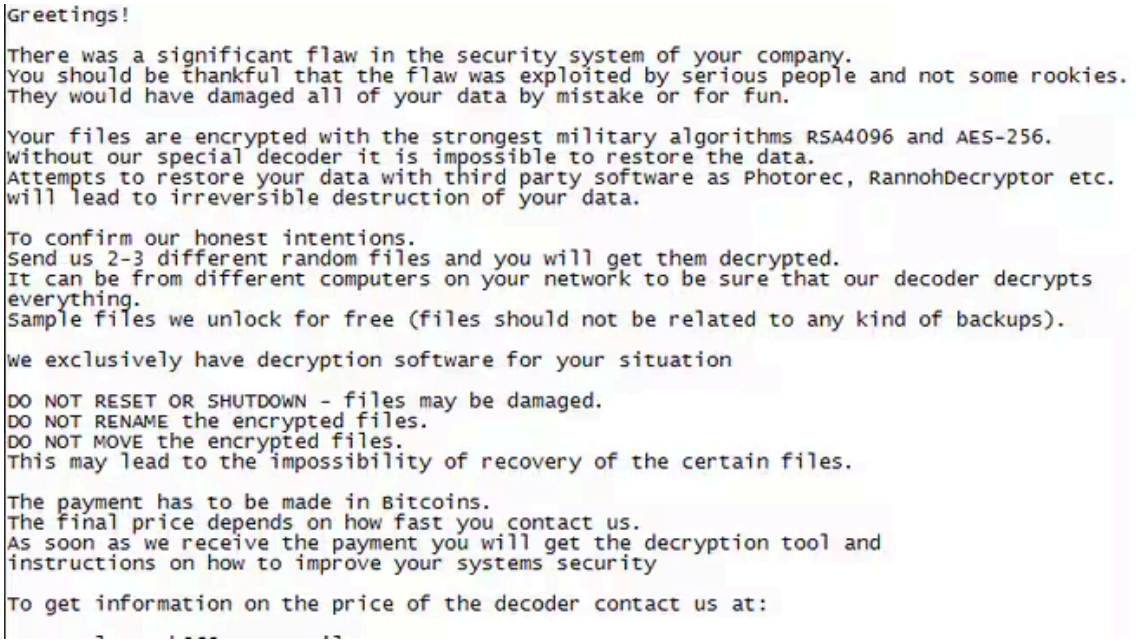
Foto: Siri Vålberg Saugstad /NRK

Samtidig skriver selskapet at man måtte skreddersy en løsning for å motstå dette angrepet og fjerne viruset.

– Det er et krypteringsvirus som vi har sett brukt før i Europa, men det er alt jeg kan si på nåværende tidspunkt, sier Bergsjø.

Datasikkerhetsekspertene i selskapet Malwarehunter har lastet opp et løsepengekrav som har blitt fremmet i et angrep med det samme viruset tidligere i år.

Det er ikke kjent om Hydro har mottatt et lignende krav.



```
Greetings!

There was a significant flaw in the security system of your company.
You should be thankful that the flaw was exploited by serious people and not some rookies.
They would have damaged all of your data by mistake or for fun.

Your files are encrypted with the strongest military algorithms RSA4096 and AES-256.
Without our special decoder it is impossible to restore the data.
Attempts to restore your data with third party software as Photorec, RannohDecryptor etc.
will lead to irreversible destruction of your data.

To confirm our honest intentions.
Send us 2-3 different random files and you will get them decrypted.
It can be from different computers on your network to be sure that our decoder decrypts
everything.
Sample files we unlock for free (files should not be related to any kind of backups).

We exclusively have decryption software for your situation

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME the encrypted files.
DO NOT MOVE the encrypted files.
This may lead to the impossibility of recovery of the certain files.

The payment has to be made in Bitcoins.
The final price depends on how fast you contact us.
As soon as we receive the payment you will get the decryption tool and
instructions on how to improve your systems security

To get information on the price of the decoder contact us at:
```

KRAV: Hackere som angrep et annet selskap med det samme viruset tidligere i år, sendte et slikt krav.

Omfattende angrep

Kommunikasjonsdirektør Halvor Molland i Hydro sa tidligere tirsdag at de først oppdaget forstyrrelser i nettverket og opplevde problemer med noen av styringssystemene.

– Vi opplevde en unormal datatrafikk sent i går kveld. Det viste seg utover natta at vi er utsatt for et dataangrep, sier han.

Hydros nettsider er fortsatt nede for telling. Ved flere av fabrikkene må operatørene styre produksjonen manuelt, og mindre anlegg er stengt inntil videre.

De ansatte har fått beskjed om å ikke skru på datamaskinene sine eller koble seg på nettverket.

E-tjenesten koblet inn

Nasjonal sikkerhetsmyndighet (NSM) bekrefter at de også er orientert om angrepet.

Ifølge fungerende avdelingsdirektør for Nasjonalt cybersikkerhetssenter i Nasjonal sikkerhetsmyndighet, Bente Hoff, er både PST, Kripos og E-tjenesten er koblet inn i etterforskningen.

– Vår rolle er å støtte Hydro, få en oversikt over situasjonen og redusere skade, sier Hoff.

Næringslivets Sikkerhetsråd (NSR) er en medlemsorganisasjon med formål å forebygge kriminalitet i og mot næringslivet.

– Det er sjelden vi ser et slikt omfang, men det er veldig vanskelig å unngå slike hendelser. De kriminelle, uansett hvem dette måtte være, har stadig nye metoder. 40 prosent av næringslivet rammes av ett eller flere alvorlige

angrep hvert år, sier direktør Jack Fischer Eriksen i Næringslivets Sikkerhetsråd.

Det generelle rådet til Næringslivets Sikkerhetsråd er å ikke betale løsepenger.

– Å betale ut løsepenger er en farlig trend. Hvis de kriminelle tjener penger på dette, blir det motivasjon for andre, sier han.

- Les: Hydro utsatt for dataangrep: – Ikke opplevd lignende
- Les: IKT-Norge-direktør om dataangrepet mot Hydro: – En annen stat kan stå bak

Publisert 19. mars 2019 kl. 11:5219. mars 2019 kl. 11:52 Oppdatert 19. mars 2019 kl. 15:4719. mars 2019 kl. 15:47
