For første gang sier PST at Kina står bak et dataangrep

nrk.no/norge/pst_-har-etterretning-om-at-kinesisk-gruppe-stod-bak-dataangrep-mot-statsforvaltere-1.15540601

Øyvind Bye Skille, Tormod Strand, Espen Kjendlie

PST mener Kina står bak et omfattende angrep på statsforvalterne i Norge.

Statsforvalteren i Oslo og Viken var ett av statsforvalterembetene som ble direkte rammet av dataangrepet i 2018. PSTs Hanne Blomberg forteller at de nå har etterretning som peker mot Kina.

Foto: Øyvind Bye Skille / NRK

Samtidig er det klart at dataangrepet mot statsforvalterne blir henlagt, selv om PST mener de har funnet etterretningsspor som peker mot Kina.

Litt over 2,5 år etter at Politiets sikkerhetstjeneste (PST) startet en etterforskning av dataangrep mot flere statsforvalterembeter går de nå ut med ny informasjon om hvem som kan stå bak.

– Vi har i denne konkrete saken etterretningsinformasjon som peker i en tydelig retning mot at det er aktøren APT31 som står bak operasjonen mot statsforvaltningsembetene, sier sjef for kontraetterretning Hanne Blomberg i PST til NRK.

– *Hva er APT31?*

– Akkurat APT31 er en aktør som vi knytter til kinesiske etterretningstjenester, svarer Blomberg.

APT31 er en hackergruppe som er kjent for å ha gjennomført dataangrep både i Norge, Finland, USA og andre steder i verden.

Kontraetterretningssjefen Hanne Blomberg i PST sier at de har opplysninger som peker mot Kina etter angrepet mot statsforvalterne.

Foto: Øyvind Bye Skille / NRK

Kontraetterretningssjefen forklarer at PST både samler inn informasjon for å lage trusselvurderinger og forebygge, men også driver med etterforskning. Etterretningen som peker på Kina kunne ikke nødvendigvis vært brukt i en straffesak.

– *Hvor sikre er dere på at det er APT31 og Kina?*

– Dette er utfordringen med å være en hemmelig tjeneste. Vi har ofte gradert informasjon som vi kan ha samlet inn selv og ikke kan avgradere. Vi kan ha kilder vi ønsker å beskytte eller vi kan ha fått informasjon fra samarbeidende tjenester som vi ikke kan bruke i en etterforskningssak. I denne konkrete saken har vi informasjon som konkret peker i retning av at det er APT31 som står bak, og det er vi ganske sikre på, svarer Blomberg.

– Ubegrunnede anklager

I en e-post sendt til NRK tilbakeviser Kinas ambassade i Norge PSTs opplysninger.

«Kina har aldri deltatt i eller støttet noen i nettangrep, og har alltid resolutt motarbeidet og slått ned på slik oppførsel. Vi er sterkt imot de ubegrunnede anklagene mot Kina».

Videre hevder kineserne i e-posten at Kinas teknologiske utvikling ikke er «avhengig av å stjele eller plyndre, men resultatet av vårt eget harde arbeid».

De anklager PST for å opptre «uansvarlige» i tilsvaret som er sendt fra ambassadens presseavdeling.

«PST innrømmet i intervjuet at det er vanskelig å spore kilden til nettangrep, og bevisene er utilstrekkelige. Det er veldig uansvarlig å spre anklager om «antagelse om skyld» uten å legge frem klare bevis».

Angripere hentet ut data

Det var sommeren 2018 at flere statsforvalterembeter ble utsatt for et omfattende og avansert dataangrep.

Statsforvalterne het den gang fylkesmenn, og angriperne kom seg først inn i datasystemene hos Fylkesmannen i Aust- og Vest-Agder. Derfra klarte de så å ta seg videre til systemer hos fylkesmannsembetene i Hedmark og Oslo og Akershus. Der kom de seg inn i datasystemer som rammet statsforvalter-embeter over hele landet.

Med bakgrunn i omfanget ble saken tatt veldig alvorlig. PST startet etterforskning for å finne ut om det var snakk om spionasje for å stjele statshemmeligheter.

– Statsforvalterne håndterer en rekke ulike opplysninger – både av personsensitiv karakter og også opplysninger om rikets sikkerhet. Det er opplysninger knyttet til forsvar og beredskap for eksempel. Det er noe av grunnen til at man har vært bekymret, og grunnen til at PST har etterforsket denne saken, sier politiadvokat Kathrine Tonstad i PST.

Statsforvalterne behandler blant annet nordmenns helseopplysninger fordi fylkeslegens kontor er en del av embetet. Også sensitive opplysninger fra barnevernssaker behandles der, og statsforvalterne har et koordinerende beredskapsansvar.

Etterforskningen har ifølge PST vist at det ble hentet ut data, men de kan ikke slå fast om det var informasjon som berører rikets sikkerhet.

– Vi ser at aktøren har tatt seg inn i ulike statsforvalterembeter, skaffet seg tilgang til data og stjålet ut noe data. Vi tror det de har stjålet ut er brukernavn og passord til ansatte hos statsforvalterne, sier politiadvokat Tonstad.

Ifølge en gjennomgang av dataangrepet ble det hentet ut 1,2 gigabyte med data, viser en rapport laget av Forsvarets forskningsinstitutt (FFI), på oppdrag fra Justisdepartementet.

Henlegges

Nå er etterforskningen avsluttet og saken henlegges på bevisets stilling.

Begrunnelsen er at PST ikke har nok åpne opplysninger om hvilken aktør som står bak til at de kunne tatt saken til retten**.**

Politiadvokat Kathrine Tonstad i PST forteller at de ikke har bevis som gjør at de strafferettslig kan ta saken videre.

Foto: Øyvind Bye Skille / NRK

– Beviskravene i strafferetten er strenge, og for at vi skal kunne peke på en aktør i en straffesak må vi ha sikre holdepunkter. Det har vi ikke i denne saken, sier PSTs politiadvokat Kathrine Tonstad.

– *Hvorfor er det så vanskelig å bevise?*

– Det vi ser er at det er tale om et avansert og profesjonelt dataangrep. Det er det ofte i disse tilfellene, og det er ofte vanskelig å følge spor som går gjennom mange land og det er sofistikert utført. Derfor er det vanskelig å kunne bevise hvem som står bak, svarer Tonstad.

Kom seg inn via hjemmekontor-løsning

PST opplyser til NRK at man antar at angriperne kom seg inn i datasystemene til statsforvalterne via et system for fjernpålogging. Dette nevnes også i FFI-rapporten om angrepet.

Slike systemer kan for eksempel være VPN-løsninger, som det siste året har blitt brukt av stadig flere på grunn av mer hjemmekontor under pandemien.

– Denne aktøren, APT31, er kjent for å bruke luremeldinger på e-post, omtalt som «phishing», for å få ansatte til å oppgi brukernavn og passord. Så kan de igjen bruke de opplysningene for å logge på VPN-løsninger, forklarer leder for sikkerhetstjenester Erik Alexander Løkken i det norske sikkerhetsselskapet Mnemonic til NRK.

Løkken forklarer at slike avanserte statlige digitale trusselaktører, ofte omtalt som APT (advanced persistent threat), bruker tid på å kartlegge de som skal angripes. De undersøker hvem som jobber der, hvilke type datasystemer som brukes og om det er noen systemer som har sikkerhetshull som ikke er fikset ennå.

På samme måte som angriperne kartlegger ofrene sine fører Mnemonic oversikt over kjennetegn ved kjente hackergrupper. Her sees noen spor fra APT31 fra andre dataangrep.

Foto: Tore Linvollen / NRK

Mnemonic driver både med forebyggende sikkerhet for en rekke ulike bedrifter, men bistår også selskaper etter at de har vært utsatt for et dataangrep. Derfor følger de nøye med på hva fienden har av metoder og kjennetegn for å finne måter å beskytte seg på.

– Det er kjent at APT31 bruker en bakdør-programvare som har mulighet til å laste opp data til kjente fildelingstjenester som Dropbox, Microsoft OneDrive og tilsvarende, sier Løkken til NRK.

Dette stemmer også med de få opplysningen som er kjent om angrepet mot statsforvalterne.

I FFI-rapporten om dataangrepet kommer det fram at angriperne stjal data og kopierte dem ut til Dropbox.

Dataangrep mot fylkesmennene

I 2018 ble fylkesmennene rammet av et alvorlig dataangrep. Her kan du se tidslinjen over angrepet.

- **Midten av juli 2018**

  Forsøk på inntrenging

  En trusselaktør forsøkte å få tilgang til datasystemene i fylkesmannsembetene. Det ble gjort forsøk på inntrenging gjennom fjernaksess hos både fylkesmannsembetene i Agder, Oslo og Akershus, Vestfold og Trøndelag. To-faktorautentisering (2FA) stoppet aktøren.

- **18. juli 2018**

  Angriperne kommer seg inn

  Forsøkene på angrep fortsatte, og kom seg til slutt inn via en fjernaksess-løsning hos Fylkesmannen i Aust- og Vest Agder.

- **Slutten av juli 2018**

  ### Rekognosering av nettverk og filer

  Etter å ha kommet seg inn på systemene hos Fylkesmannen i Aust- og Vest Agder starter angriperne rekognosering av nettverkene og filsystemene. De klarte også å skaffe seg høyere tilgang i systemene, og å komme seg inn hos andre fylkesmannsembeter via den første tilgangen.

- **24. juli 2018**

  ### Starter skadevare

  Angriperne installerer og starter skadevare på systemene til Fylkesmannen i Aust og Vest Agder. Det samme skjer også hos Fylkesmannen i Hedmark og Fylkesmannen i Oslo og Akershus i dagene etter. Skadevaren som ble benyttet kalles Trochilus.

- **30. juli 2018**

  ### Henter ut data

  Angriperne henter ut data i dagene fram til og med 30. juli 2018. Til sammen skal de ha hentet ut rundt 1,2GB med data via tjenesten Dropbox.

- **31. august 2018**

  ### Skadevaren mister kontakt med angrepsservere midlertidig

  Skadevaren var i kontakt med kommando- og kontrollservere fram til 31. august 2018. På dette tidspunktet skjer det en endring der domenet knyttet til angrepsserveren bytter ip-adresse og kommunikasjonen stopper midlertidig.

- **22. oktober 2018**

  ### Fylkesmannen i Oslo og Akershus varsles av NorCERT

  Sikkerhetseksperter ved NorCERT hos Nasjonal sikkerhetsmyndighet (NSM) varsler Fylkesmannen i Oslo og Akershus om et mulig angrep. Ekspertene blir henvist videre til Fylkesmannen i Hedmark som driftet fellessystemer for fylkesmennene.

- **Slutten av oktober 2018**

  ### NSM setter opp sensorer

  NSM og Fylkesmannen i Hedmark starter kartlegging av det de trodde kunne være et mulig angrep. Det blir installert sensorer (VDI) fra NSM for å kunne følge med på trafikken i nettverkene.

- **November 2018**

  ### PST starter etterforskning

  Påtalemyndigheten beslutter at PST skal starte en etterforskning av dataangrepet selv om de ennå ikke har mottatt noen anmeldelse.

- **7. november 2018**

  ### Koordineringsgruppe opprettes

  En koordineringsgruppe opprettes for å bedre samarbeidet rundt håndtering av dataangrepet. I gruppen sitter representanter for Kommunal- og moderniseringsdepartementet, PST, NSM, Direktoratet for samfunnssikkerhet og beredskap (DSB) og fylkesmannsembetene.

- **13. november 2018**

  ### Alle fylkesmennene informeres

  Et informasjonsskriv om dataangrepet sendes ut til alle fylkesmannsembetene via gradert nett.

- **Midten av november 2018**

  ### Beslutter å ikke kaste angriperne ut

  I midten av november 2018 kartlegges det hva angriperne har gjort på datasystemene – så godt det lar seg gjøre. Etter en del diskusjon besluttes det å ikke kaste angriperne ut av systemene. Etter råd fra NSM ønsker man å følge med på angriperne for å finne ut mer, og at dette gjøres slik at de ikke skal oppdage at de er avslørt.

- **24. desember 2018**

  ### Skadevaren tar kontakt med angrepsserver på nytt

  Skadevaren på datasystemene hadde ikke hatt kontakt med angrepsserverne siden slutten av august. Denne dagen tar de skadelige programmene igjen kontakt med adressen knyttet til kommando- og kontrollserverne til angriperne. Den nye aktiviteten blir oppdaget etter 12 timer av NSM NorCERT.

- **24. desember 2018**

  Kobler systemer fra internett

  Etter varslingen om ny kontakt mellom datasystemene hos fylkesmennene og angripernes systemer blir det besluttet å koble ned internett-tilkoblingen. En medarbeider reiser til Fylkesmannen i Hedmark sine lokaler på Hamar og kobler fra systemene. Det viser seg senere at varselet var en falsk positiv fordi det ikke ble etablert fullstendig oppkobling til angriperne.

- **27. desember 2018**

  Dataangrepet blir kjent i media

  Nedkoblingen av datasystemer hos fylkesmennene fører til at dataangrepet blir kjent i media. PST bekrefter at de har hatt en etterforskning i gang siden november.

Gruppe med koblinger til Kinas statsapparat

Gruppen som PST nå peker på omtales som APT31, men har også fått andre navn som Zirconium, Bronze Vinewood og Judgement Panda.

Det siste navnet har gruppen fått av sikkerhetsselskapet Crowdstrike, som har ulike panda-navn på grupper de knytter til Kina. I sikkerhetsmiljøet internasjonalt har APT31 av noen blitt omtalt som styrt av det kinesiske departementet for statssikkerhet (Ministry of State Security MSS).

– Denne trusselaktøren kobles av en del til det nasjonale departementet for statssikkerhet i Kina. Da vil de gjerne gjøre angrep på oppdrag fra dem, og gå mot spesifikke mål, sier Erik Alexander Løkken hos Mnemonic.

Erik Alexander Løkken er leder for sikkerhetstjenester i det norske sikkerhetsselskapet Mnemonic.

Foto: Øyvind Bye Skille / NRK

– *Hvordan har man klart å gjøre en slik kobling?*

– Flere sikkerhetsselskaper har koblet APT31 til kinesiske myndigheter i undersøkelsene av ulike dataangrep og hendelser der gruppen har vært involvert. Denne koblingen er ofte gjort ved at man ser at gruppen bruker de samme verktøyene som kinesiske myndigheter er kjent for å bruke, svarer eksperten fra Mnemonic.

Løkken forklarer at det er godt kjent at slike kinesiske hackergrupper har vært aktive de siste tiårene. De har systematisk stjålet informasjon som ledd i industrispionasje rundt våpenteknologi, medisiner og også angrep rettet mot enkeltpersoner.

APT31 har de senere årene blitt koblet til flere dataangrep i ulike land:

- Finland pekte i mars i år på APT31 etter dataangrep mot den finske nasjonalforsamlingen.
- Både Google og Microsoft har uttalt at gruppen målrettet seg mot ansatte i Joe Bidens valgkamp-apparat under valget i USA i 2020.
- Det norske programvareselskapet Visma ble utsatt for et angrep i 2018/2019, som sikkerhetseksperter mener APT31 kan stå bak.

APT31 er likevel ikke kjent for å bruke de mest kompliserte metodene.

– APT31 er ikke kjent for å være av de mest avanserte trusselaktørene, men en som kanskje jobber i tidligere faser med å innhente masse informasjon. Det kan hende denne informasjonen så brukes av andre grupper som er knyttet til det kinesiske statsapparatet i nye og mer avanserte angrep, sier Løkken.

NRK har bedt om en kommentar fra Kinas ambassade i Norge, men har enn så lenge ikke mottatt noe svar.

Finske myndigheter pekte også mot Kina og aktørene i APT31 etter at den finske riksdagen ble utsatt for et dataangrep.

Foto: Emmi Korhonen / AP/NTB

Nupi-forsker: – Voksende bekymring med angrep fra statlige aktører

Seniorforsker Karsten Friis ved Norsk utenrikspolitisk institutt (Nupi) forsker og følger med på dataangrep, cyberoperasjoner og forholdet mellom land i verden på feltet.

Nupi-forskeren forklarer at flere av verdens stormakter som Kina, Russland og andre land over tid har brukt dataangrep og hacking som digitale våpen mot hverandre og for å spionere.

– *Hvorfor gjør Kina dette angrepet mot statsforvalterne da?*

– Jeg vil anta at de kan være interessert i sentrale personer som jobber der. For det kan være sentrale personer i norsk politikk og samfunnsliv.

Karsten Friis forsker blant annet på cyberangrep i sitt arbeid ved Nupi.

Foto: Øyvind Bye Skille / NRK

– *Vil slike angrep være godkjent fra høyere hold i landet?*

– Vi må anta det, men vi vet det ikke sikkert. Siden dette er sikkerhetsorganisasjoner og sensitive spørsmål må vi anta at de ikke opererer helt fritt.

Han sier at bruken av hacking har blitt mer utbredt mellom stater.

– Det har vært en voksende bekymring rundt dataangrep over flere år. Tidligere var det mer kriminelle aktører, men nå er statlige aktører blitt en større sikkerhetsutfordring. De går på sikkerhetsinstitusjoner og demokratiske institusjoner. Det er en trend vi har sett de siste årene, sier Friis til NRK.

Kina har tidligere vært kjent for å stjele informasjon som kan hjelpe egne selskaper og egen teknologiutvikling. Friis forklarer at de gjerne har utnyttet mulighetene fordi spionasje gjennom datamaskiner er enklere enn på de mer gammeldagse metodene. Så i nyere tid har de også angrepet statsapparatet og parlamenter.

Nupi-forskeren mener det er riktig av Norge å peke tydelig på Kina om man har god nok info om at det kan være de som står bak.

Og han synes det er interessant at man for første gang peker så tydelig i en konkret sak.

– I Norge er det første gang Kina nevnes av myndighetene. Vi har hørt om Russland tidligere etter dataangrepet mot Stortinget, men ikke Kina. Det har bare vært spekulert tidligere om Kina kunne stå bak angrep, blant annet etter angrepet mot Helse sør-øst. Dette er derfor første gang Kina nevnes eksplisitt av norske myndigheter, sier Friis.