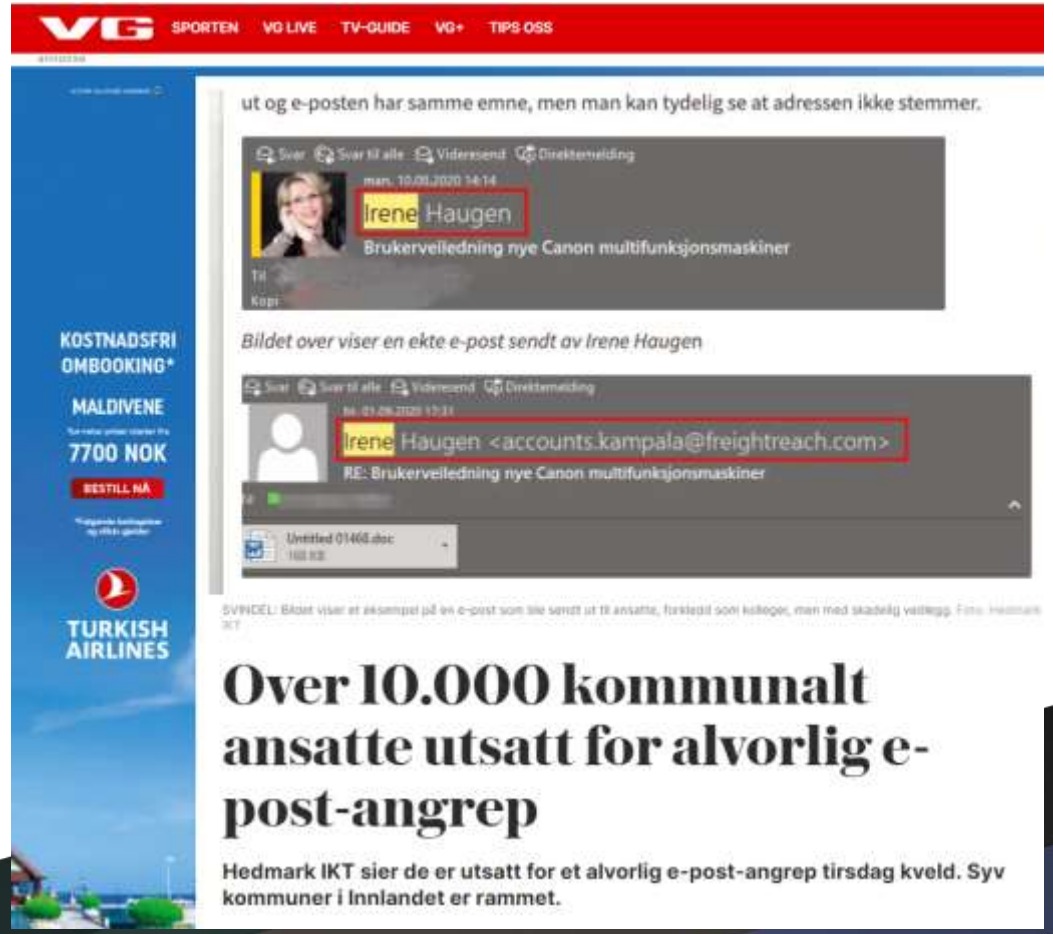
Hei! VI ER PÅ VG?!

Fra epoststorm til mediestorm

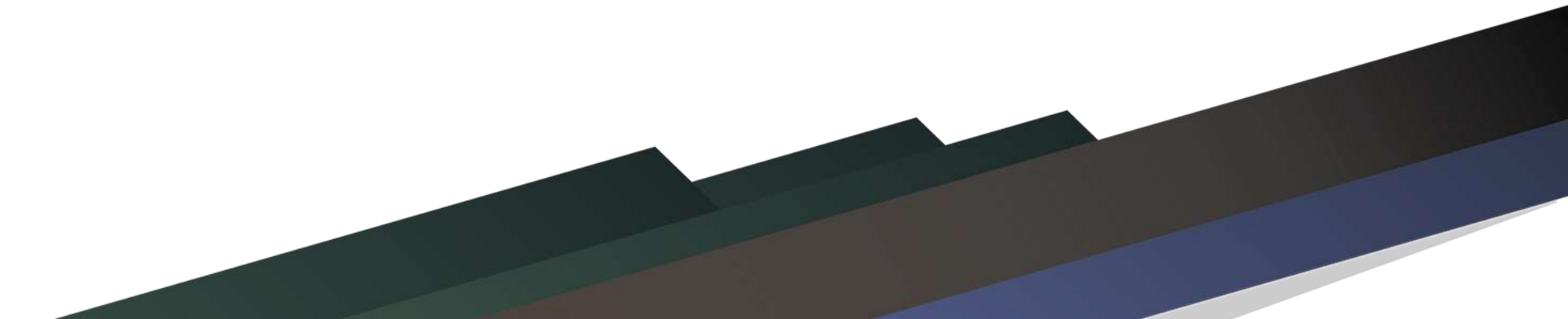
En oversikt og analyse av hendelsen 01.09.2020



Hedmark IKT

Hva var det som traff oss? Den perfekte storm?

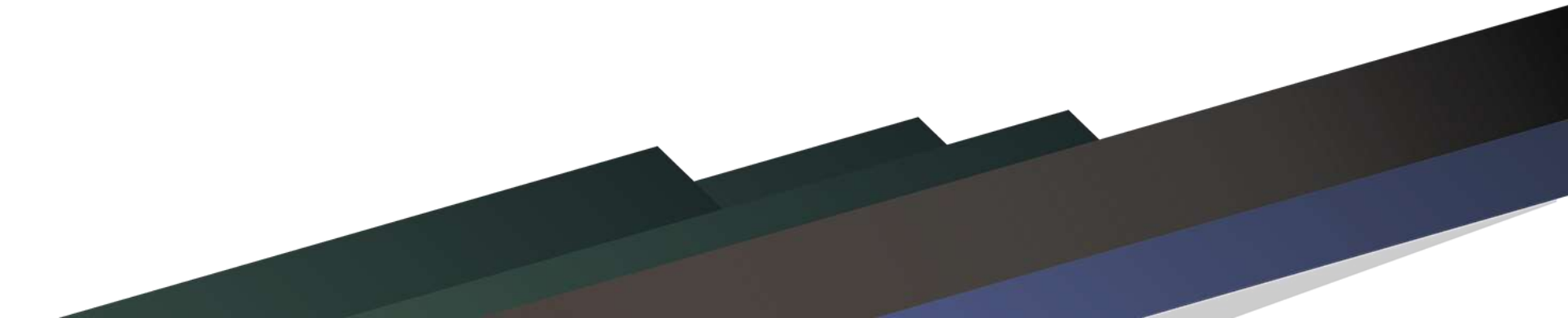
Var Norge under angrep – først Korona, Stortinget – så oss?



Hedmark IKT

Mer om oss på

https://www.hedmark-ikt.no/



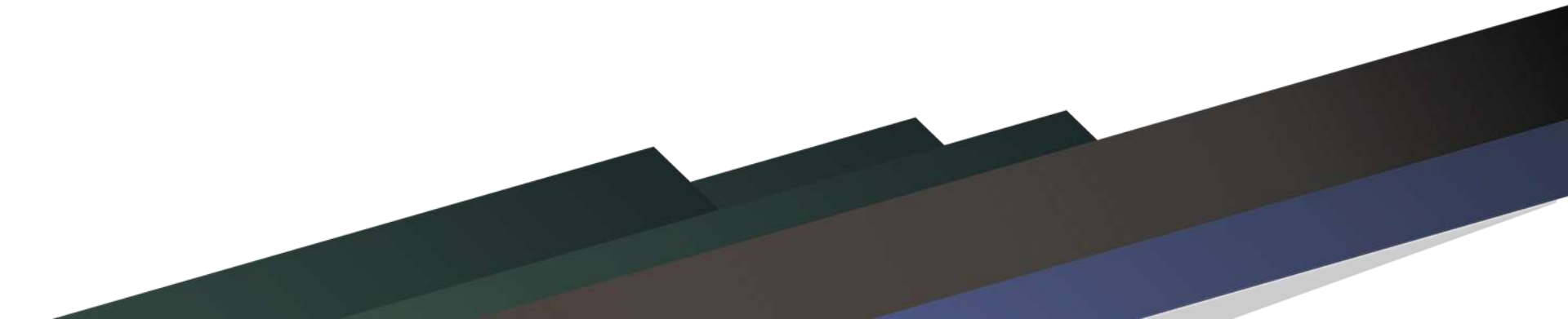
Hedmark IKT

31. AUGUST 2020

HVORDAN SER VERDEN UT, OG
HVORDAN ER VÆRMELDINGEN

- HelseCert med advarsel om virusangrep
- Den største virusfaren var korona

- ..vanlig dag på jobben..



Hedmark IKT

1.SEPTEMER 2020

HVORDAN SER VERDEN UT, OG
HVORDAN ER VÆRMELDINGEN

- Vi legger ut informasjon på egen nettside om at epostvirus er på vei.
- Vi har en virushendelse som vi håndterer som vanlig
- Så:
- Stortinget rammet av dataangrep

Stortinget utsatt for et omfattende IT-angrep

STORTINGET (NRK): Stortinget har blitt utsatt for et omfattende IT-angrep. Det er registrert innbrudd på e-post-kontoene hos et mindre antall stortingsrepresentanter og ansatte. Saken er anmeldt til PST.

SE VIDEO: Pressemøtet på Stortinget om IT-angrepet.

Pedja Kalajdzic
Journalist

Hallvard Norum
Journalist

Bjørnar Hjellen
Journalist

Julia Kirsebom Thommessen
Journalist

Line Tomter
Journalist

Helge Carlsen
Journalist

Tore Tollersrud
Journalist

Olav Døvik
Journalist

Knut Røsrud
Journalist

Espen Alnes
Journalist

Publisert 1. sep. kl. 15:00
Oppdatert 1. sep. kl. 21:25

Dette er alvorlig!

Utenlandske aktører… !

Kanskje med fremmede land som en del av en cyberkrig..?

Angrep på demokratiet…?

..

Er det krig..?

Og så smalt det hos oss..

Fra vår interne kundeportal

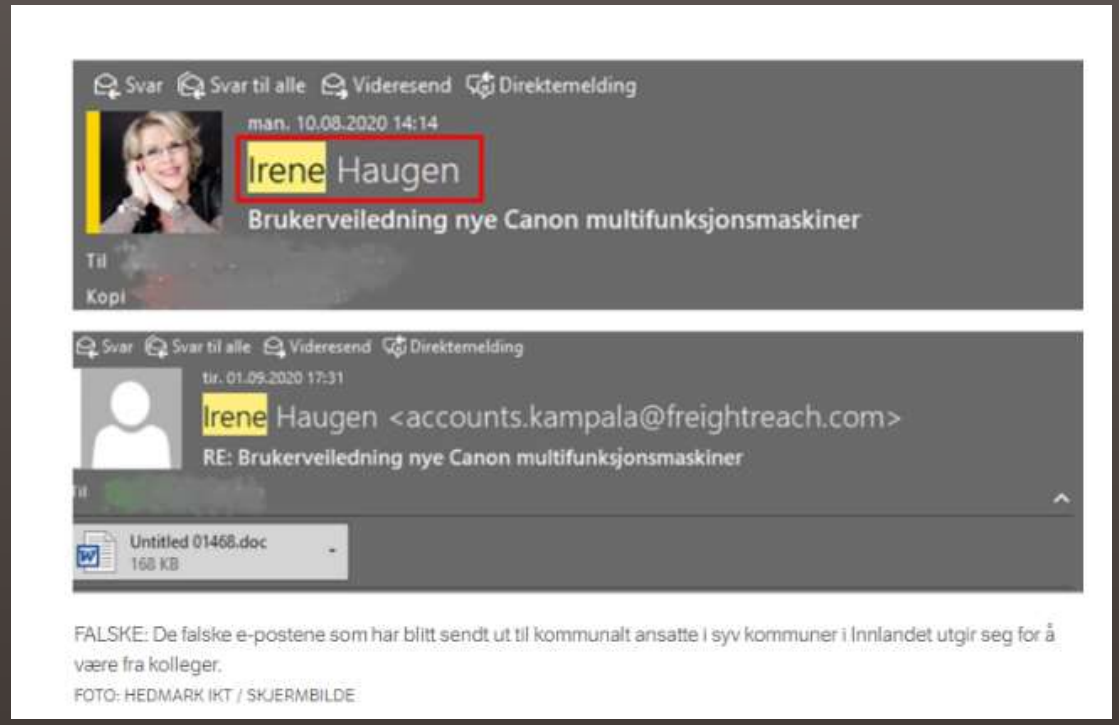
Den første var den originale, sendt ut dagen før.

Den andre er den forfalskede

.. Se på vedlegget – der er viruset.

Media fikk bruke dette bildet

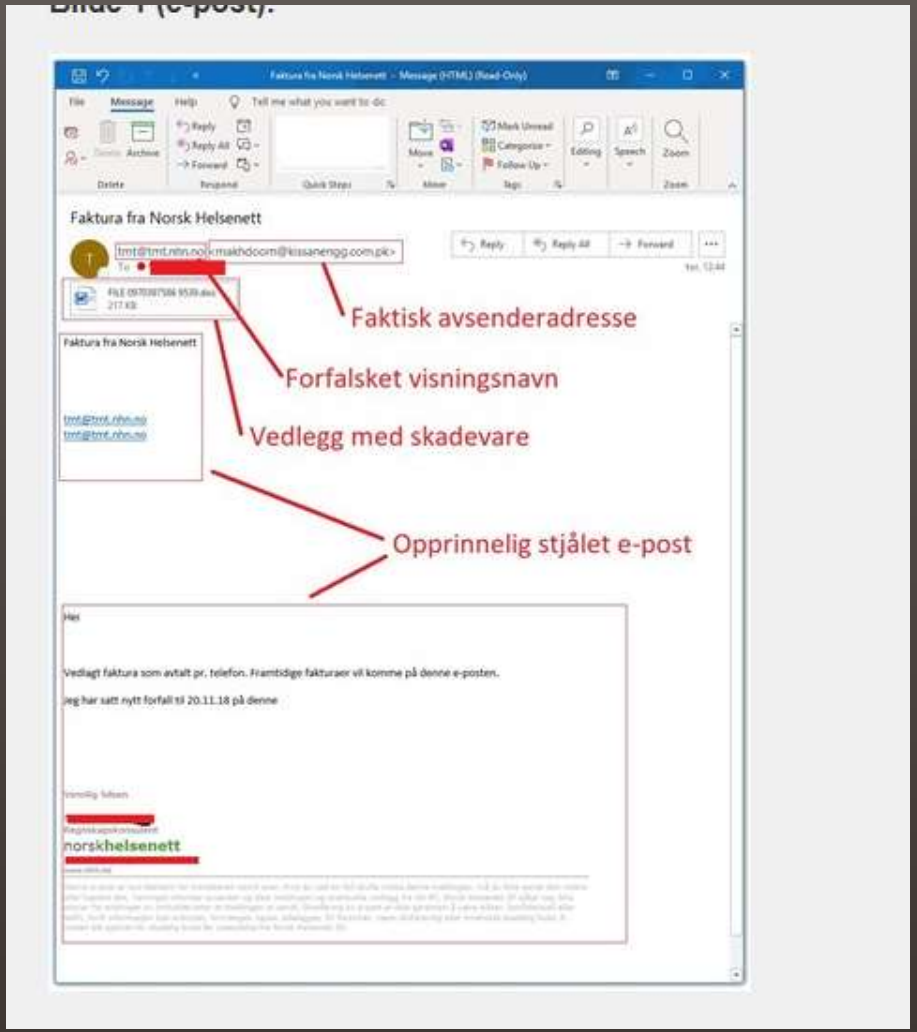
..Canon satte krisestab …



FALSKE: De falske e-postene som har blitt sendt ut til kommunalt ansatte i syv kommuner i Innlandet utgir seg for å være fra kolleger.

FOTO: HEDMARK IKT / SKJERMBILDE

Dette er måten skadevaren jobber på -



Hedmark IKT

KL 23:55
SENDTE VI UT
DENNE
PRESSE-
MELDINGEN
TIL
LOKALAVISER
OG NRK

Pressemelding fra Hedmark IKT vedrørende data-angrep.

Kvelden 1. september fanget vi opp et angrep rettet mot våre e-postservere, som potensielt kan være skadelig for våre datasystemer.

Angrepet går ut på at svindlere prøver å få tilgang til våre brukeres e-postkontoer, for deretter å sende ut skadelige vedlegg til andre ansattes e-postkontoer. E-postene som da sendes har emner og avsender som framstår som riktige, slik at det er vanskelig for andre brukere å fange opp at e-posten de mottar er falsk.

Da angrepet ble oppdaget, stengte vi for alle innkommende e-poster for alle våre brukere. Det jobbes videre med å kartlegge omfanget og metoder, slik at vi kan stoppe videre angrep og avgrense omfanget av angrepet.

Kommunalt ansatte tilknyttet Hedmark IKT har blitt varslet om angrepet via SMS, med en klar oppfordring til å ikke åpne noen vedlegg de har mottatt på sin e-post knyttet til arbeid. Vi kommer til å fortsette arbeidet utover natten. For ytterligere informasjon, ta kontakt med Daglig leder Edvard Lysne på telefon: 90 02 87 42 eller Informasjonsrådgiver Petter Berg på telefon: 90 17 01 78.

Aktualności

Atak hakerów na norweskie serwery. Ofiarami Storting i konta 10 000 pracowników gmin

Monika Pianowska
02 września 2020 11:01

Udostępnij na Facebooku

Hakerzy obrali sobie za cel konta mailowe zarówno posłów, jak i pracowników parlamentu. adobe stock/ fot. Dmitry Naumov/ licencja standardowa

W ubiegłym tygodniu norweski parlament padł ofiarą rozbudowanego

I tillegg var daglig leder i alle kanaler

- NRK – innlandet
- NRK – nyhetsmorgen
- Intervju med VG og Dagbladet, Aftenposten
- NRK TV, TV2, og mange andre

- ..og vi fikk mange hyggelige og medfølende meldinger fra leverandører og kontakter.

Vi er blitt en referanse for dataangrep

En analyse fra britiske Royal United Services Institute peker på flere utfordringer ved strategien både EU og Norge har valgt.

▶ Et minimumskrav er at man har klart å identifisere nøyaktig hvilke datamaskiner og nettverk som sto bak angrepet.
▶ I tillegg må operasjonen kunne knyttes til konkrete personer.

«Ofte mangler grunnleggende bevis. Enten fordi myndighetene ikke har tilgang til ugjendrivelige bevis, eller fordi de ikke ønsker å legge det frem», skriver forsker Sasha Erskine i RUSI.

Hun peker på at det er gode grunner til å holde bevis tilbake. Åpenhet kan føre til at et land avslører sitt forsvar.

På den andre siden er det også lett å skjule bevis eller endre IP-adresser.

En russisk hacker forsøkte for eksempel i 2018 å gi Nord-Korea skylden for å hacke vinter-OL i Sør-Korea.

– Vi ser at det er flere lignende hendelser. Men vi klarer ikke koble dette til det som skjedde ved Stortinget.

Det gjelder blant annet omfattende angrep, som ble oppdaget samme dag som innbruddet på Stortinget ble politianmeldt. Denne gang var målet kommunene Løten, Nord-Odal, Sør-Odal, Grue, Kongsvinger, Stange og Hamar.

Spionprogrammer

Flere tusen ansatte fikk tilsendt en e-post med et vedlegg. E-posten ble oppdaget på 270 datamaskiner. Ansatte som trykket på lenken, fikk installert spionprogrammer.

– Skaden skjedde ikke før man klikket på vedlegget. Vi greide å oppdage det raskt, stoppe spredningen og sperre e-postene, sier daglig leder i Hedmark IKT Edvard Lysne.

– Om lag 20 maskiner var ble infisert, men vi klarte å stoppe det før det spredte seg. Skadepotensialet var betydelig.

Hva skjedde egentlig

- Noen helseforetak og leverandører til disse, hadde blitt infisert av viruset «emotet» noen dager tidligere.
- Eposter fra disse ble brukt til å sende virus.
- En tilfeldig kommuneansatt med ansvar for kommunikasjon med andre helsevirksomheter var tidlig på jobb og forsøkte å åpne en slik.
- I løpet av dagen fikk mange flere den samme type stjålne epost fra mange ulike avsendere.
- Pc tok kontakt med C2 server kl 17 og sendte over også hans eposter
- Disse ble så sendt fra utenlandske avsendere tilbake til våre kommuner med virus.
- Kommunene reagerte og tok kontakt med oss, og vi så at vi måtte få kontroll
-

Hva gjorde Hedmark IKT

- Vi satte krisestab kl 19.30, fordelte oppgaver og ba samtidig om hjelp fra vår sikkerhetsleverandør BDO
- Vi stoppet all epostlevering inn, varslet NSM
- Vi søkte gjennom epostlogger for å finne kildene
- Vi sjekket antivirusprogram for meldinger
- Vi sjekket brannmurlogg for trafikk mot kjente c2 servere
- Vi isolerte rammede pcer og stengte brukerkonto
- Vi logget alt vi gjorde og fulgte mal fra NSM
- Kl 02:15 hadde vi kontroll og åpnet for epost uten vedlegg

Hva var vi redd for?

- Brukernavn og passord på avveie
- At brukere åpnet tilsendte virusvedlegg
- Aktiv skadevare i våre system
- At vi var under et målrettet angrep
- At filer og system kunne krypteres
- At det foregikk en annet angrep under dekke av denne hendelsen
- At vi ble brukt i et videre angrep

BDO har analyserte skadevaren fra e-poster og vedlegg mottatt fra HIKT.

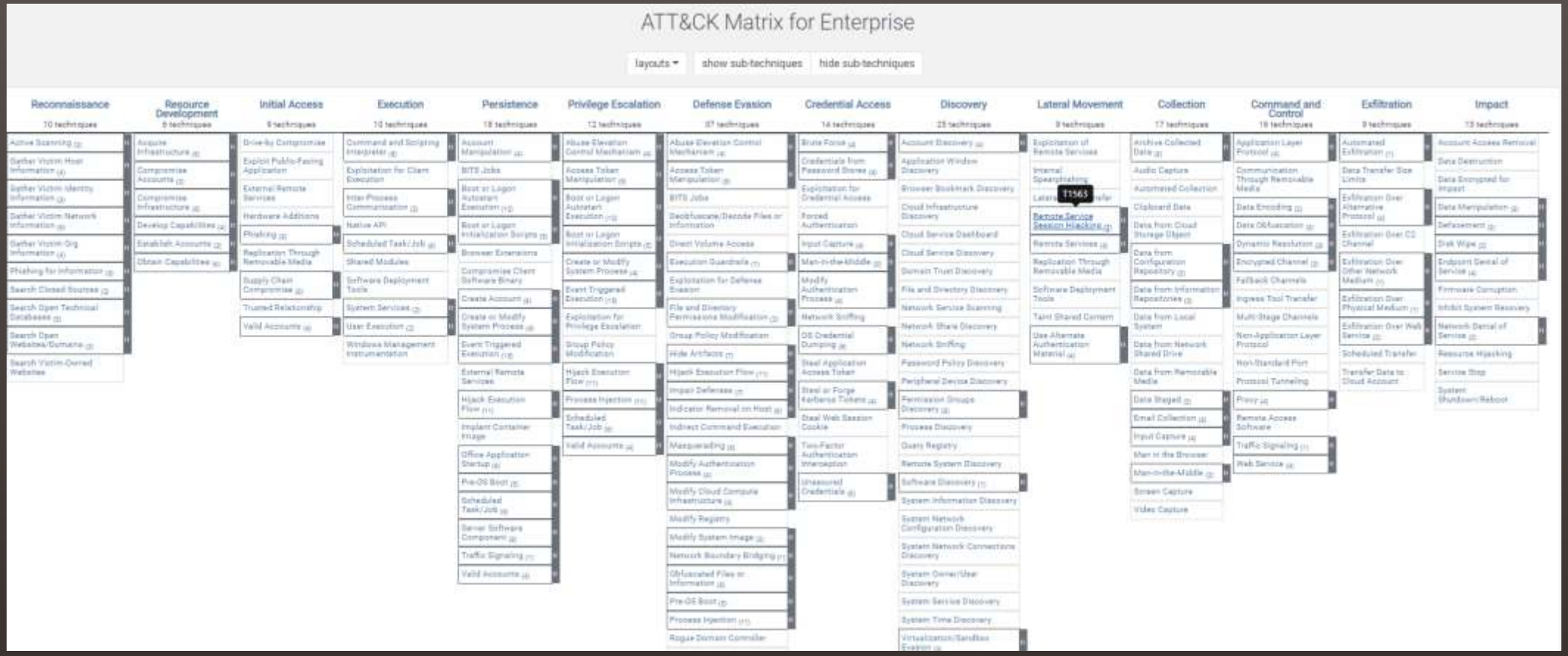
Første del av analyse bestod av indikatorsøk i HIKT sine interne systemer, og i åpne kilder. Dette for å gi en overordnet oversikt over situasjonen. Alle funn viste seg å kunne knyttes til den store Emotet-kampanje som har truffet flere virksomheter over hele verden.

Flere åpne kilder listet også en rekke andre indikatorer, som ikke ble funnet igjen i BDO sin analyse. Dette gjelder i hovedsak domener benyttet til nedlasting og kommando- og kontrollinfrastruktur.

Funnene var i hovedsak filhasher, domener brukt til nedlasting, og kommando- og kontrollinfrastruktur. Nedenfor listes alle indikatorer observert i BDO sin analyse av skadevaren:

Nedlastings domener	C2 adresser
seattlebugsafari[.]com	62.210.90.75
sindicatodeseguridad[.]com	54.37.42.48
spanferkelgrill-verleih[.]com	51.75.33.122
snoeker[.]com	50.121.220.50
standontheedge[.]com	91.121.54.71
sedalaser[.]com	83.169.21.32
tjdengler[.]info	68.69.155.181
tinerservis[.]com	67.247.242.247
teleconx[.]com	213.197.182.158
thecomedycrowd[.]com	45.173.88.33
toby-warren[.]com	191.99.160.58
tierrasinsolitas[.]com	217.13.106.14
	111.67.12.221

Sjekk gjerne: https://attack.mitre.org/



Flaks og dyktighet..

- Vi stoppet epost inn raskt
- Vi fikk varslet brukerne med SMS
- Vi rullet ut ny Pc-policy i løpet av natta som gjorde det umulig å åpne vedlegg
- Vi fant den mest rammede PC og isolert øvrige rammede
- Vi hadde kompetente personer tilgjengelig
- Vi fikk hjelp fra sikkerhetsleverandør BDO
- Vi hadde patchet PC og servere til siste versjoner
- Vi fikk beskjed fra NSM om at det ikke var sammenheng mellom vår hendelse og Stortingets hendelse – Vi var et «tilfeldig» offer

Og nei, disse sikkerhetsmekanismene hadde ikke stoppet hendelsen

- MFA (to-faktor-pålogging) – fordi angriper aldri logget på en konto
- DMARC, Dkim, etc, fordi avsenderadressene var reelle
- Firewall – fordi de aktuelle C2 servere var helt nye
- Antivirus – fordi det var en ny versjon av emotet
- AntiSpam – selve eposten var helt reell
- Men det finnes andre sikkerhetsmekanismer som ville stoppet angrepet. De fleste får konsekvenser for brukerne.

Og nå, da?

- Vi har fått en påminnelse om alvorlighetsgraden i trusselbildet
- Vi har anmeldt saken til politiet
- Vi har gjennomført flere sårbarhetsreduserende tiltak, og planlegger flere
- Våre eiere og kunder har fått en forståelse av viktigheten av IKT-sikkerhet
- Vi må planlegge for å være robuste og tåle nye angrep
- Vi har vært på riksdekkende media en gang. Det holder.

Takk for meg!

Håvard Helland

Sikkerhetsansvarlig Hedmark IKT

Havard.helland@hedmark-ikt.no