FHS/Cyberingeniørskolen

Cyberoperasjoner

17. des. 2024

Fordypningsoppgave

Gruppe to

ING3510 CYBEROPERASJONER

AV:

J. Ovidt Bardal, J. Granviken og

T. Valen Spångberg

Vinter 2024

Inbrief

Beskrivelse:

Ola Fernandez er ansatt som lege hos Norsk Helse Institutt. Han har fått en e-post av kompisen Pioter som sier at han har blitt hacket. Ola tror han også kan ha fått virus på datamaskinen sin ettersom han husker å ha lastet ned en fil fra en e-post fra Pioter som ikke fungerte.

Ola tok med pc-en sin til den lokale nettverksadministratoren på sykehuset, som har tilgjengeliggjort nettverkslogger fra pc-en til Ola og Ola har gitt både e-postkontoen og den private datamaskinen «Klient_NHI_W10_Ola» til disposisjon.

Ditt hendelsesteam sin oppgave er å etterforske funksjon og omfang av angrepet, finne ut hvem som står bak, identifisere angrepsvektorene og hvis mulig få tilbake tapt data. En analyseklient ved navn «Malware-Analyse_Win7» er tilgjengelig under gjennomføringen.

Innlogging:

Tabell 1, brukernavn og passord

Tjeneste	Brukernavn	Passord
vSphere	ING3510-Gr2-user01	ThisIs!Hard_24
vSphere	ING3510-Gr2-user02	ThisIs!Hard_24
vSphere	ING3510-Gr2-user03	ThisIs!Hard_24
Gmail	ola.fernandez.1990@gmail.com	GooPassword!2024
Klient_NHI_W10_Ola	Guest	GooPassword!2024
Malware-Analyse_Win7	REM	malware

Avgrensninger:

- Det er ikke mulig å benytte tidspunkter for å stadfeste hendelser

Mål for oppgaven:

- **Identifisere trusselaktøren** – Bruke digitale spor for å identifisere og bekrefte trusselaktøren bak cyberangrepet.
- **Vurdere skadeomfanget** – Benytte seg av ferdigheter i å analysere og vurdere konsekvenser av et cyberangrep. Utvise nøyaktighet ved innhenting av informasjon og vurdering av konsekvenser.
- **Kartlegge angrepet** – Forstå hvordan trusselaktøren benyttet seg av en angrepsvektor for å få tilgang til systemet, samt se sammenhengen mellom de ulike delene av angrepet.

Læringsutbytte:

Etter fullført case skal deltakerne kunne identifisere trusselaktøren, analysere konsekvensene av cyberangrepet og forstå angrepsvektoren.

Hint under gjennomføring

Her følger noen hint til gjennomføringen av casen. Hintene er ment som veiledning for å peke i riktig retning, uten å avsløre løsningen. De gis i samsvar med tidspunktene som angis i Tabell 2 nedenfor. T representerer tidspunktet ved start av casen, så for eksempel betyr «T+90m» at hintet skal bli gitt en time og 30 minutter etter start.

Tabell 2, Hint under gjennomføring

Hint	Tidspunkt
e-post	
Hva har Ola fått gjennom e-post-korrespondanse?	T+15m
Kanskje det ikke gjør noe om dere ikke får lastet ned viruset?	T+30m
Kryptering	
Er det noe som er kryptert på datamaskinen?	T+40m
Er det egentlig mulig å finne ut av hvilken kryptering som er benyttet for filer? Kan det bruteforces?	T+60m
De krypterte filene er kryptert med XOR-kryptering	T+110m
Malware	
Er det mistenksomme strings i skadevaren?	T+30m
Er det noen strings i skadevaren som peker til en nettside?	T+45m
Trusselaktør	
Er det noen suspekte IP-adresser i noen av filene der har å forholde dere til?	T+90m
Er det noe i filen som kan indikere hvilken APT det er snakk om?	T+105m
Hvilket språk er benyttet på google?	T+110m
Passordcracking*	
Står Olas navn noe sted i dokumentene i folderen?	T+75m
Er det noe relevant på nettsiden som Pioter sendte?	T+80m
Kan man lage en ny ordliste av kombinerte ord?	T+85m
Bruteforcing på noen få tall bruker å fungere.	T+95m
Keylogger	
Det ikke er noe mer her.	T+110m
Nettverkslogg	
Hvilke nettverksprotokoller har synlige pakker?	T+60m
Kan man sjekke innholdet på http POST?	T+75m
Kan være fint å vite hvor Ipen er fra.	T+100m

*Må gis ordre om å gjennomføres, dersom det ikke blir påbegynt.

Innholdsfortegnelse

1. Innledningen

I en tid der verdenssamfunnet står overfor økende geopolitiske spenninger, har cyberangrep blitt et avgjørende verktøy i statlige aktører. Helsesektoren, som allerede er presset av krav om digitalisering og høy grad av tilgjengelighet, har blitt en stadig mer attraktiv målskive for trusselaktører [1]. Denne oppgaven fokuserer på et simulert angrep mot Norsk Helse Institutt (NHI), der en datamaskin tilhørende en lege som har mange høyprofilerte kunder har blitt kompromittert, sensitive data er kryptert og eksfiltrert.

Situasjonen illustrerer hvordan cyberangrep ikke bare påvirker teknologiske systemer, men også utgjør en betydelig trussel mot nasjonal sikkerhet og samfunnsfunksjoner. Angrep rettet mot helseinstitusjoner kan lamme kritiske tjenester, spre usikkerhet i befolkningen og undergrave tillit til myndigheter og helsevesen.

Denne casen peker på hvordan moderne trusselaktører, som statssponsede grupper, kan utnytte sårbarheter i individers og organisasjoners digitale hverdag. Oppgaven er designet for å utvikle ferdigheter innenfor skadevareanalyse, etterretning, og passordcracking, samtidig som den setter hendelsen i kontekst av en større sikkerhetspolitisk situasjon. Ved å analysere dette angrepet er det mulig å identifisere trusselaktøren, vurdere skadeomfanget, og foreslå tiltak for å forhindre lignende fremtidige hendelser.

1.1 Geopolitisk kontekst

Cyberangrep mot kritisk infrastruktur, inkludert helsesektoren, har blitt en del av den hybride krigføringen som preger dagens sikkerhetslandskap. Dette er særlig relevant i lys av økende spenninger mellom NATO og Russland, hvor statssponsede aktører som APT28 (Fancy Bear) spiller en sentral rolle [2]. Gruppen er kjent for målrettede angrep mot helsevesenet, militære institusjoner og politiske mål i vestlige land, og deres handlinger er en integrert del av Russlands strategi for å styrke sin maktposisjon og svekke motstandere.

Ved å koble denne casen til den bredere geopolitiske situasjonen, ser vi hvordan tilsynelatende lokale angrep kan være brikker i et større spill. De viser hvordan avanserte cyberoperasjoner brukes til å oppnå strategiske fordeler, samtidig som de illustrerer sårbarheten i samfunnets kritiske systemer. Oppgaven er dermed ikke bare et teknisk tilnærming, men også et bidrag til å forstå de sikkerhetspolitiske implikasjonene av cybertrusler i dagens verden.

1.2 Hjelpemidler benyttet

I Tabell 3 presenteres en oversikt over de ulike hjelpemidlene som er benyttet for å utvikle denne casen. Valget av verktøy er i hovedsak basert på programmer og tjenester som allerede er introdusert i tidligere forelesninger. Dette er gjort for å sikre at deltakerne som skal analysere og løse casen, får en tilpasset utfordring basert på kjente inngangsverdier og metoder.

Valget av verktøy reflekterer også en praktisk tilnærming til realistiske scenarier innen cybersikkerhet. Fra generering av fiktive data til simulering av skadelig programvare og kommando- og kontrollinfrastruktur, har hvert verktøy spilt en spesifikk rolle i å gjenskape et troverdig cyberangrep.

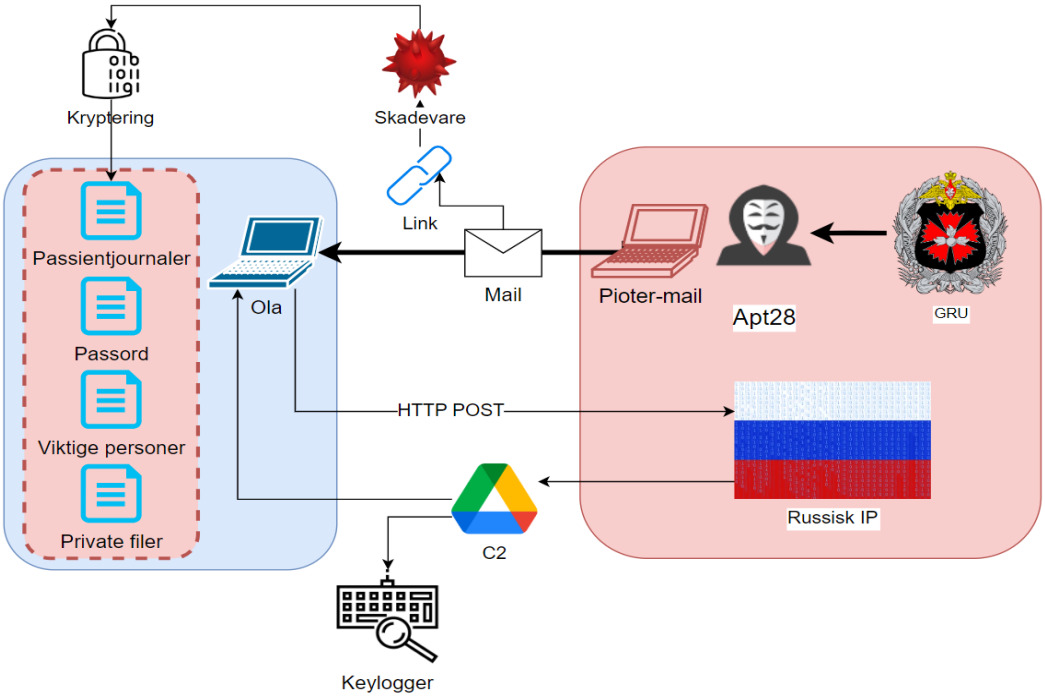
Tabell 3, Hjelpemidler

Hjelpemidler	Formål
ChatGPT	Generere realistiske fiktive profiler, data og bilder, samt testing av ulike scenarier i cybersikkerhet.
Visual Studio Code (VSCode)	Utvikle keylogger og implementere XOR-kryptering for beskyttelse av sensitiv informasjon.
Gmail	Lage e-postadresser og simulere målrettede phishing-angrep med manipulerte avsenderidentiteter.
Google Drive	Etablere en kommando- og kontroll (C2) infrastruktur for å simulere dataeksfiltrasjon og systemkontroll.
Wireshark	Generering av nettverkstrafikk.
WireEdit	Redigering av nettverksloggfiler.
PeStudio	Utføre statisk analyse av programvare.
Registry Editor	Undersøke og modifisere Windows-register.
Kali Linux	Cracking av passordhash.
VSphere	Implementere virtuelle maskiner for å simulere angrepsmiljøer og teste sikkerhet.

Filer og programvare som har vært produsert, samt andre vedlegg som er benyttet under casen er tilgjengelig på GitHub ved å benytte følgende link: https://github.com/obireb/Cyberops/tree/main.

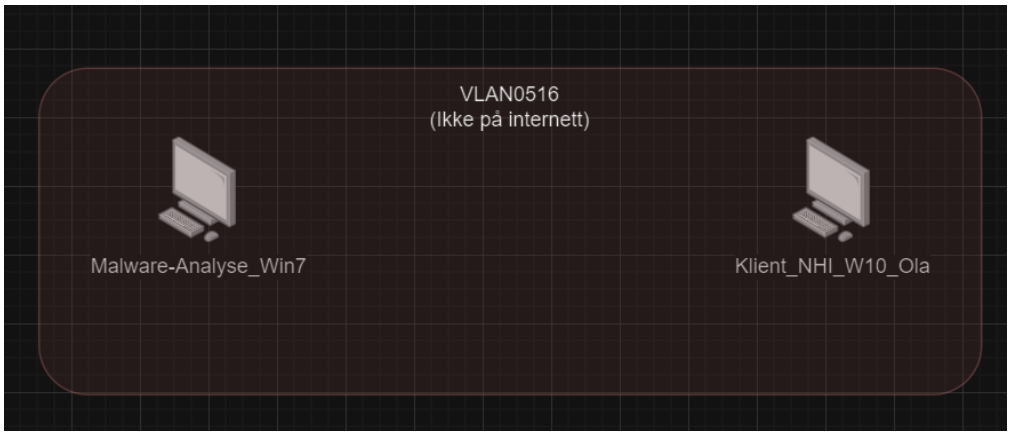
1 Systeme

Systemet som angripes i denne casen er en privat datamaskin til en lege med navnet Ola Fernandez. Han benytter denne datamaskinen til både jobb- og fritidsformål. Den er brukt som lagringsplass for bilder, lister og viktige dokumenter. Det er ingen ekstra beskyttelse av datamaskinen og tilkoblet nettverk. I figur 1 under, er det totale systemet skissert. Det er skissert både hvordan aktøren har satt opp angrepet, og systemet som benyttes av DCO-teamet (Defensive Cyber Operations-team) med en beskrivelse av hvordan angrepet har foregått.



Figur 1, fullstendig systemskisse

Figur 2 viser en praktisk implementasjon av systemoppsettet gjennom VSphere. Oppsettet består av to virtuelle maskiner, tilkoblet samme VLAN (Virtual Local Area Network). Dette konfigurasjonsvalget muliggjør sikker filoverføring mellom maskinene, samtidig som det eliminerer risikoen for at skadevare fra analyseklienten kan spre seg til internett.



Figur 2, praktisk implementasjon i VSphere

2 Trusselaktøren

Trusselaktøren vi har tatt utgangspunkt i denne oppgaven er APT28, også kjent som Fancy Bear eller Sofacy [3]. Dette er en russisk, statlig sponset hackergruppe med sterke bånd til militære og etterretningsorganisasjoner som GRU (Main Directorate of the General Staff of the Armed Forces of the Russian Federation) [3]. Gruppen har vært aktiv i flere år og er kjent for sine omfattende cyberangrep rettet mot kritisk infrastruktur, politiske institusjoner og militære mål i vestlige land. Deres operasjoner har særlig blitt knyttet til geopolitisk spenning, inkludert konflikten i Ukraina, hvor de har spilt en nøkkelrolle i Russlands hybridkrigføring [4].

I vår case har APT28 trengt seg inn på en klient som benyttes av en ansatt i Norsk Helse Institutt ved å benytte seg av spear-phishing som angrepsvektor. Angrepet startet med at en e-post som så ut til å komme fra en bekjent ble sendt til en ansatt ved Norsk Helse Institutt. E-posten inneholdt et ondsinnet vedlegg som førte til at skadevaren ble lastet ned og kjørt på mottakerens maskin.

Skadevaren som ble benyttet av APT28 i denne casen er en skadevare som har muligheten til å kryptere dokumenter og hente ut informasjon fra systemet. Dette gjøres ved at skadevaren har kommunisert med en C2-server i form av en Google Drive, noe som er en kjent strategi som APT28 tidligere har benyttet seg av. Skadevaren har også forsøkt å kjøre HTTP POST-instrukser opp mot en adresse som eies av trusselaktøren for å hente ut filer fra den kompromitterte datamaskinen.

I tillegg til at dette foregår, har skadevaren endret på lokale registernøkler, slik at den alltid vil starte opp når datamaskinen skrus på, som er et tiltak for å sikre persistens. Dette etterligner handlingsmønsteret til APT28 særdeles godt [5].

3.1 Aktørens mål

APT28 har som mål å fremme Russlands geopolitiske interesser gjennom cyberspionasje, desinformasjon og sabotasje. Gruppen retter angrep mot vestlige land, militære institusjoner, politiske mål og kritisk infrastruktur for å svekke motstandere og styrke Russlands posisjon [6].

De samler inn sensitiv informasjon for strategiske fordeler, påvirker politiske prosesser gjennom desinformasjon og kan utføre sabotasje mot kritisk infrastruktur for destabilisering. Aktivitetene inngår i Russlands hybridkrigføring, med fokus på å undergrave NATO, EU og andre opplevde trusler mot russiske interesser [7].

3.2 Aktørens historie

I Ukraina har APT28 stått bak flere betydelige cyberangrep som har hatt som mål å destabilisere nasjonen og støtte Russlands strategiske mål i regionen [4]. Dette inkluderer blant annet angrep på Ukrainas elektrisitetsnett i 2015 og 2016, som førte til strømbrudd i flere regioner. Ved å bruke spesialutviklet skadevare som "BlackEnergy" og "Industroyer," viste APT28 sin evne til å kombinere sofistikerte teknologiske metoder med militære mål. Disse angrepene var ikke bare rettet mot fysisk infrastruktur, men også mot Ukrainas evne til å opprettholde offentlig tillit og nasjonal sikkerhet.

I tillegg har APT28 brukt spear-phishing som en inngangsmetode for å infiltrere ukrainske myndighetsnettverk og militære systemer [8]. De har stjålet kritisk informasjon som ble brukt til å undergrave forsvarsoperasjoner og å spre desinformasjon. Ved å utnytte troverdige e-poster med ondsinnede vedlegg, har de klart å oppnå vedvarende tilgang til sensitive systemer, noe som gir dem muligheten til både å overvåke og manipulere kritisk informasjon.

APT28s aktiviteter i Ukraina illustrerer deres taktiske tilnærming til cyberangrep, som kombinerer strategiske mål med teknisk ekspertise. Gjennom angrepene søker gruppen å oppnå flere mål, inkludert undergraving av Ukrainas politiske stabilitet, svekkelse av NATO-allierte og styrking av Russlands posisjon i regionen. Disse angrepene er en del av en bredere strategi der cyberoperasjoner fungerer som en integrert del av Russlands hybridkrigføring.

3.2 Cyber Kill Chain

Et effektivt cyberangrep følger en strukturert prosess der tekniske sårbarheter og menneskelige feil utnyttes for å oppnå målet. Dette delkapittelet gir en trinnvis gjennomgang av det målrettede angrepet i denne casen, fra initial rekognosering til eksfiltrasjon av sensitive data.

Tabell 3, Cyber Kill Chain [9]

Trinn	Handling
Reconnaissance	Aktøren hadde på forhånd kjennskap til Olas rolle som en viktig lege for politiske aktører i Norge. Ved hjelp av OSINT-teknikker (Open Source Intelligence) klarte angriperen å finne et bilde av Ola og Pioter på sosiale medier, der de deltok sammen i et maraton. Dette muliggjorde identifisering av både deres navn og e-postadresser fra maratonets offentlige resultatlister.
Weaponization	Skadevaren er en applikasjon som etablerer persistens og C2-forbindelse. Den benytter XOR-kryptering for å kryptere data på systemet slik at det ikke er synlig hva som blir eksfiltrert.
Delivery	Pioter benyttet et svakt passord som aktøren klarte å brute-force, noe som ga dem tilgang til hans Google-konto (pioter.hornebo.1999@gmail.com). Fra denne kompromitterte kontoen sendte aktøren en målrettet spear-phishing e-post til Ola. E-posten inneholdt et ondsinnet vedlegg, forkledd som et påmeldingsskjema til et arrangement Ola hadde vist interesse for, og fremstod troverdig på grunn av avsenderens identitet.
Exploitation	Ved å trykke på vedlegget i e-posten, ble skadevaren eksekvert av Ola, noe som aktiverte dens hensikt.
Installation	Ola eksekverte filen manuelt. Skadevaren genererte en mappestruktur på systemet og dupliserte seg selv. Den dupliserte versjonen ble deretter tildelt en autorun-nøkkel i Windows-registeret for å sikre automatisk oppstart ved hver pålogging.
Command & Controll (C2)	Skadevaren benyttet HTTP POST-forespørsler for å eksfiltrere data til en ekstern C2-server kontrollert av APT28. Videre ble skadevaren fjernstyrt gjennom nedlastinger fra en Google Drive-konto som var kompromittert.
Action on Objectives	Etter at skadevaren var installert, ble sensitive filer kryptert og eksfiltrert, noe som hindret Ola i å få tilgang til sine egne data.

3 Hendelseshåndteringsscenarioet

4.1 Inbrief

Inbriefen gir minimalt med informasjon om casen til analyseteamet. Dette er bevisst gjort for å teste teamets evne til å kartlegge og planlegge selvstendig uten påvirkning fra forhåndsdefinerte inngangsverdier. Fra dette momentet i casen er det ønskelig at analyseteamet tar med seg følgende detaljer:

- Ola har med høy sannsynlighet kjørt filen som ble sendt til ham.

4.2 Undersøkelse av privat datamaskin

Det er plantet informasjon på den private datamaskinen for å teste teamets evne til å filtrere viktig fra uviktig informasjon. Fra dette momentet i casen er det ønskelig at analyseteamet tar med seg følgende detaljer:

- En del av malwaret ligger igjen på maskinen og har opprettholdt persistens gjennom registernøkler og skjult seg selv i en egengenerert mappestruktur.
- Private filer på pc-en er blitt kryptert.

4.3 Undersøkelse av e-postkonto

E-posten gir lite direkte informasjon, men bekrefter at Ola lastet ned viruset etter å ha trykket på en lenke sendt fra en tilsynelatende kjent avsender. Hendelsesforløpet indikerer at Ola ignorerte tegn på mistenksomhet på grunn av avsenderens identitet. Fra dette momentet i casen er det ønskelig at analyseteamet tar med seg følgende detaljer:

- Nettsiden nevnt i e-posten, relatert til Pioter som sier han er hacket, er nødvendig for å cracke passordet senere i gjennomføringen.
- Hendelsesforløpet vises ganske tydelig i e-postdialogen, hvor Ola har lastet ned en fil fra Pioter og kjørt den.

4.4 Undersøkelse av malware

Malwaret er ikke fullt funksjonelt og brukes til å teste hendelsesteamets ferdigheter i enkel statisk analyse (f.eks. ved bruk av PeStudio). Det er mye informasjon i strings, som fører til at nøyaktigheten til teamet blir testet her. Fra dette momentet i casen er det ønskelig at analyseteamet tar med seg følgende detaljer fra skadevaren:

- Flagger funksjon under imports som kan indikere keylogger:
  - GetAsyncKeystate
- Strings viser til en webadresse:
  - "shorturl.at/<input_string>"
  - "input_string=Wcl6N"
- Strings indikerer slutten på en webadresse til Google Drive. Kan settes sammen til en fungerende link ved å benytte ordinær Google-syntax:
  - 1eIPiiv7e4fRd6oyRDDOxOS8KkCIaqS1r?usp=drive_link

    - Manglende del: https://drive.google.com/drive/folders/
- Strings indikerer russisk IP-adresse:
    - 109.248.255.3
- Strings indikerer funksjoner som har selvforklarende navn:
    - _DownloadFile
    - _EncryptFolder
    - _UploadFiles

Etter eksekvering av skadevaren har det dukket opp en keylogger (Unnamed File.exe) i samme mappe som skadevaren har duplisert seg til. Ut av analysen av denne keyloggeren er det ønskelig at analyseteamet ser at dette er en keylogger.

4.5 Undersøkelse av nettverkslogg

Dette momentet tester analyseteamets ferdigheter i grunnleggende nettverksanalyse. HTTP POST-metoden er benyttet, noe som muliggjør identifikasjon av filopplastinger, i motsetning til HTTPS som er kryptert og vanskeligere å analysere. Ved nærmere undersøkelse av innholdet i de registrerte opplastningene, kan man identifisere hvilke filer som har blitt forsøkt lastet opp.

Nedlastinger via Google Drive er også observert, men det antas at det ikke er mulig å hente ut relevant informasjon fra disse aktivitetene, gitt at trafikken er kryptert. Ut fra denne analysen er det ønskelig at analyseteamet tar med seg følgende detaljer:

- Filopplastinger via HTTP POST til en russisk IP-adresse som samsvarer med en string funnet i malwaret
- Filene som er forsøkt opplastet er de samme som de krypterte filene som finnes på Ola sin datamaskin.

4.6 Dekryptering av filer

For å avklare trusselaktørens intensjon med angrepet, er det avgjørende å få dekryptert de krypterte filene. Nøklene som kreves for dekryptering finnes i mappen «c2» på en Google Drive, som er tilgjengelig via strings i malwareet. Basert på tilgjengelig informasjon er det ikke mulig å fastslå hvilken krypteringstype som er benyttet. Dette tyder på at ytterligere ledetråder er nødvendige for å fullføre dekrypteringsprosessen. De viktigste detaljene analyseteamet bør ta med seg videre er:

- Mappen «C2» indikerer at det kan være en C2-funksjon via Google Drive, som kan gi innsikt i hvordan trusselaktøren styrer kommunikasjon og dataoverføringer.
- Krypteringen kan reverseres, noe som tyder på at aktøren har hatt som intensjon å gjenskape og få tilgang til informasjonen i de krypterte filene, snarere enn å ødelegge den.

4.7 Hash cracking

Gjennom strings i malwareet blir man ledet til en Google Drive-mappe som inneholder en hash tilknyttet Ola, samt diverse hint som kan hjelpe til med cracking av hashen. Hvis hendelsesteamet identifiserer muligheten for å knekke hashen, men ikke prioriterer dette i første

omgang, bør det gis en ordre om å gjennomføre prosessen. Dette kan være en utfordrende oppgave som krever at teamet husker nettstedet som ble sendt fra Pioter i e-posten. De viktigste detaljene analyseteamet bør ta med seg videre er:

- Passorde kan crackes. Dette gir mulighet for å få tilgang til ytterligere informasjon knyttet til aktøren.
- Russisk språk i filene og hintene kan tyde på at russiske aktører er involvert i angrepet.

4.8 Kartlegging av aktør (APT28)

Gjennom analysen av ulike spor og hendelser i oppgaven, er det flere indikasjoner på at aktøren bak angrepet kan være APT28. Følgende detaljer er viktige for analyseteamet å ta med videre i kartleggingen av aktøren:

- Ordet “Bear” er nevnt på nettsiden på Google Driven og er et element i passordet som crackes. Dette er en referanse til navnet “Fancy Bear” som de også bruker.
- Ordet “FCY” er benyttet på filer, som hinter til ordet “Fancy”. Dette er en referanse til navnet “Fancy Bear” som de også bruker.
- En russisk IP-adresse ble observert på servere som mottok opplastinger av filer, og bekrefter ytterligere mistanke om at russiske aktører er involvert.
- Bruken av Google Drive for C2. APT28 er kjent for å bruke Google Drive, for å etablere kommunikasjon og kontroll over infiserte systemer.
- Fokusering på statlige interesser. Aktøren har vist interesse for sensitive opplysninger om viktige personer knyttet til statlige virksomheter, noe som tyder på at dette er et statlig drevet angrep med politiske mål.
- Bruk av spearphishing i kombinasjon med malware. Angrepet starter med spearphishing, som er en typisk tilnærming for APT28, etterfulgt av malware som utfører skade.
- Ingen interesse for løsepenger. Dette peker mot en politisk eller strategisk motivasjon for angrepet, fremfor enn økonomisk gevinst.

4 Øvingsmål

Dette kapittelet gir en strukturert gjennomgang av hvordan oppgaven har svart på de definerte øvingsmålene. Ved å analysere hendelsene, de tekniske komponentene og de sikkerhetspolitiske konsekvensene, er målet å utvikle en helhetlig forståelse av cyberangrepets kompleksitet og påvirkning.

5.1 Identifisere trusselaktøren

Et sentralt mål med oppgaven er å identifisere hvem som står bak angrepet. Dette innebærer å analysere tekniske detaljer som IP-adresser, metadata fra skadevaren, nettverkslogger og andre indikatorer på kompromittering (IOC-er). Ved å kartlegge disse sporene i sammenheng med etterretningskilder, kan deltakerne knytte angrepet til en spesifikk aktør. I denne casen peker metodene, som spear-phishing, målbildet, IP-adressen, og mange andre IOC-er på APT28 (Fancy Bear). Identifikasjon av trusselaktøren krever at deltakerne bruker både teknisk erfaringinger og forståelse av aktørens motivasjon, som å samle etterretning eller destabilisere kritisk infrastruktur.

Ved å analysere kontekstuelle faktorer som Russlands hybridkrigføring og tidligere dokumenterte angrep mot vestlige institusjoner, kan deltakerne sette angrepet i en bredere geopolitisk sammenheng. Denne prosessen fremmer en helhetlig forståelse av hvordan cybertrusler fungerer som et strategisk verktøy i dagens sikkerhetspolitiske landskap.

5.2 Vurdere skadeomfanget

For å forstå konsekvensene av angrepet, må deltakerne gjøre en grundig vurdering av skadeomfanget. Dette innebærer en teknisk analyse av krypterte filer, eksfiltrert informasjon og skadevarens funksjonalitet, samt en vurdering av hvordan dette påvirker Norges sikkerhetspolitiske situasjon. Dersom sensitiv pasientdata knyttet til politikere kommer på avveie, kan det skape usikkerhet i befolkningen– for eksempel ved at en leders helsetilstand avsløres. Samtidig kan slike lekkasjer svekke tilliten til helsevesenet og dets evne til å beskytte privat informasjon.

I denne oppgaven må deltakerne også analysere nettverksloggen for å identifisere hvilke filer som er lastet opp til eksterne servere, og hvilken informasjon som kan ha blitt eksfiltrert. Dette gir dem innsikt i skadepotensialet og viser hvordan cyberangrep kan eskalere fra isolerte tekniske hendelser til alvorlige nasjonale sikkerhetstrusler. En grundig vurdering av skadeomfanget inkluderer også en helhetlig analyse av hvordan slike hendelser kan påvirke samfunnet og dets stabilitet.

5.3 Kartlegge angrepsvektoren

Under gjennomgangen av angrepet ble flere angrepsvektorer identifisert, som gir innsikt i hvordan trusselaktøren kan utnytte sårbarheter i kritisk infrastruktur. Angrepet startet med målrettet phishing, hvor angriperen brukte e-poster tilpasset mottakeren for å oppnå tilgang. Dette ble fulgt opp av en kombinasjon av sosial manipulering. Videre benyttet angriperen

skadevare for å kryptere filer og eksfiltrere sensitiv informasjon. Analysen av angrepsvektorene kartlegger hvordan svakheter i sikkerhetsrutiner bidro til angrepets suksess.

5.4 Helhetlig læring

Denne casen gir deltakerne en unik mulighet til å forstå cyberangrep fra flere perspektiver, inkludert tekniske, taktiske og strategiske dimensjoner. Ved å identifisere trusselaktøren, vurdere skadeomfanget og foreslå tiltak, vil deltakerne ikke bare øke sin tekniske kompetanse, men også få innsikt i hvordan cybertrusler påvirker samfunnet som helhet. Casen understreker viktigheten av et helhetlig perspektiv der teknologisk ekspertise kombineres med sikkerhetspolitisk forståelse.

5 Kilder

[1] V. Mishra, «Cyberattacks on healthcare: A global threat that can’t be ignored,» United Nations, 2024 november 8. [Internett]. Available: https://news.un.org/en/story/2024/11/1156751. [Funnet 2024 desember 17].

[2] NATO, «Statement by the North Atlantic Council concerning malicious cyber activities against Germany and Czechia,» NATO, 03 Mai 2024. [Internett]. Available: https://www.nato.int/cps/en/natohq/official_texts_225229.htm. [Funnet 16 Desember 2024].

[3] MITRE, «MITRE ATT&CK - APT28,» 10 Oktober 2024. [Internett]. Available: https://attack.mitre.org/groups/G0007/. [Funnet 02 Desember 2024].

[4] Canadian Center for Cyber Security, «CYBER THREAT BULLETIN: Cyber Threat Activity Related to the Russian Invasion of Ukrain,» Canadian Centre for Cyber Security, 22 Juni 2022. [Internett]. Available: https://www.cyber.gc.ca/sites/default/files/cyber-threat-activity-associated-russian-invasion-ukraine-e.pdf. [Funnet 02 Desember 2024].

[5] MITRE, «MITRE ATT&CK - APT28 NAVIGATOR,» 10 Oktober 2024. [Internett]. Available: https://mitre-attack.github.io/attack-navigator//#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0007%2FG0007-enterprise-layer.json. [Funnet 02 Desember 2024].

[6] Radware, «CyberPedia / DDosPedia / Fancy Bear (APT28) Threat Actor,» Radware, [Internett]. Available: https://www.radware.com/cyberpedia/ddos-attacks/fancy-bear-apt28-threat-actor/. [Funnet 12 Desember 2024].

[7] P. Paganini, «NATO and the EU formally condemned Russia-linked APT28 cyber espionage,» security affairs, 05 mai 2024. [Internett]. Available: https://securityaffairs.com/162759/apt/nato-eu-condemned-apt28-espionage.html. [Funnet 17 desember 2024].

[8] Ziperium, «Zimperium > Glossary > APT28,» Ziperium, 27 Juni 2024. [Internett]. Available: https://www.zimperium.com/glossary/apt28/. [Funnet 12 Desember 2024].

[9] Lockheed Martin, «Cyber Kill Chain,» 2024. [Internett]. Available: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html. [Funnet 02 Desember 2024].

6 Debrief

7.1 Angrepsvektor

Angrepet ble initiert gjennom spearphishing, hvor en e-post ble sendt til Ola med en lenke til en ondsinnet fil. E-posten var nøye tilpasset offeret og utnyttet psykologisk press i form av tidspress, og ble sendt fra en avsender som fremstod som pålitelig. Etter at malwaret ble eksekvert, ble persistens etablert gjennom registernøkler. Angriperen benyttet Google Drive for C2-kommunikasjon og forsøkte å eksfiltrere sensitive filer via HTTP. Opplastningen via HTTP feilet, men det er fortsatt en mulighet for at filene ble potensielt sendt via Google Drive. I tillegg ble en keylogger funnet på systemet, selv om det er uklart hvordan den har havnet der. Malwaret har også forsøkt å skjule seg i systemet ved å bruke en tilsynelatende normal mappestruktur, noe som kan ha vært et forsøk på å unngå oppdagelse.

7.2 Trusselaktør

Angrepet er trolig utført av APT28 (Fancy Bear), basert på flere indikatorer, som ordet "Bear" på en Google Drive-relatert nettside, "FCY" brukt på filer, og russisk IP-adresse. Fancy Bear er kjent for sin bruk av spearphishing, malware og Google Drive som C2-kanal. Aktøren har tidligere vært involvert i målrettet innsamling av politisk og strategisk informasjon, spesielt relatert til statlige aktører, og har brukt keyloggere som en metode for spionasje. Dette indikerer et målrettet angrep mot høyprofilerte personer, fremfor økonomisk gevinst.

7.3 Skadeomfang

Angrepet kan ha hatt alvorlige konsekvenser, med risiko for at sensitiv informasjon, som pasientdata som ble eksfiltrert. Slike lekkasjer kunne ha skapt politisk usikkerhet og svekket tilliten til offentlige institusjoner. Ved å lekke og avsløre slik informasjon, vil Russland potensielt kunne skape ustabilitet og så tvil om høytstående personer i Norge, noe som kan skade Norges omdømme og påvirkningskraft internasjonalt over tid.

7.4 Konklusjon

Angrepet illustrerer hvordan statlige aktører, som APT28, benytter avanserte metoder som spearphishing, malware og C2-kommunikasjon gjennom plattformer som Google Drive for å infiltrere mål og stjele sensitiv informasjon. Selv om angrepet ikke førte til fullstendig eksfiltrasjon av data, belyser det hvordan både tekniske sårbarheter og menneskelige feil kan utnyttes av angripere. For å beskytte mot fremtidige trusler, er det avgjørende å implementere et flerlagers sikkerhetsrammeverk, som inkluderer robuste mekanismer mot phishing, regelmessige systemoppdateringer, og omfattende opplæring av ansatte i cybersikkerhet. En viktig lærdom fra angrepet er nødvendigheten av å skille mellom arbeidsrelaterte og personlige data for å unngå utilsiktet eksponering av sensitiv informasjon.

Angrepet understreker at cybersikkerhet ikke kun dreier seg om å håndtere tekniske trusler, men også om å forstå de geopolitiske og strategiske motivasjonene som driver disse angrepene. En helhetlig tilnærming, som kombinerer tekniske løsninger med dypere innsikt i trusselaktørenes mål og metoder, er essensiell for å møte de stadig mer komplekse og målrettede truslene.