Oppgave 1.a

Tomra meldte i sin pressemelding fra 27. juli (Tomra, 2023) at en aktør hadde benyttet seg av legitime passord. Det blir også nevnt senere i pressemeldingen fra 29. september (Tomra, 2023), noe av det de mener er nøkkeldetaljer fra sin «forensics report». Tomra sier at aktøren klarte å oppnå eskalerte privilegier og utnyttet allerede innebygde verktøy fra Windows for å traversere i systemet og utføre ondsinnede handlinger. Ut ifra opplysningene biter jeg meg fast i utsagnene om at aktøren lagde: bakdører, beveget seg lateralt, modifiserte passord, skadelige payloads i PowerShell og ondsinnede binaries.

Tiltak fra NIST sitt rammeverk (NIST, 2018, s. 23) kunne avverget eller dempet omfanget på angrepet. Ut ifra opplysningen vi fikk om angrepet er de tre tiltakene som er mest aktuelle: Access Control, Segmentation and Network Security og Continuous Monitoring. Selv om det kan virke som at det har vært en menneskelig faktor med i bildet i saken til Tomra, grunnet at det ble tatt i bruk legitime passord, har jeg valgt å la vær å inkludere Training and Awareness. Grunnet at dersom, eller heller når, det menneskelige svikter vil det være andre tiltak til stede for å hindre eller i verste fall dempe omfanget.

Gjennom implementeringen av prinsippet om en robust tilgangskontroll sikres det at brukere som allerede er inkorporert i systemet, opplever begrensninger i sine tilgangsrettigheter. Dette skaper en barriere som reduserer mulighetene for aktører som har oppnådd uautorisert tilgang til en brukerkonto, eller i tilfelle av en intern aktør, begrenser potensialet for skade som kan påføres systemet. En vanlig bruker vil ikke ha behov for å kjøre flere av verktøyene som aktøren hos Tomra benyttet seg av, slik som PowerShell eller å installere binaries.

Ved forsøk fra en bruker på å utføre laterale bevegelser og skaffe seg tilgang til andre deler av systemet, en praksis kjent som «lateral movement,» anbefales det å implementere prinsippet om «Segmentation and Network Security.» Dette prinsippet involverer en struktur der nettverket er oppdelt i flere soner, hvor enheter og tjenester med sammenlignbar kritikalitet er gruppert innen hver enkelt sone. Dette arrangementet sikrer at en aktør som befinner seg i en sone ikke har direkte tilgang til andre soner. Bruk av indre og ytre brannmurer bidrar til å etablere en barriere mellom sonene, som aktøren må passere. Dette kan gjerne utløse en form for

deteksjon, som igjen gir forsvarsteamet muligheten til å plukke opp og reagere på hendelsen.

Samtidig med implementeringen av segmentering og nettverkssikkerhet, anbefales det å innføre kontinuerlig overvåkning av systemet gjennom et SIEM-system. Dette gir mulighet til sanntidsanalyse og aggregasjon av loggdata, samt lagring av data for fremtidig analyse ved behov. Konfigurasjonen av SIEM inkluderer overvåking av nettverkstrafikk, systemlogger, brannmurer mellom sonene og brukertrender. Dette gir bedre evne til å oppdage avvik fra normal oppførsel i systemet.

Oppgave 1.b

Brannmurlogger, og spesielt denne er interessant for Tomra angrepet. Pressemeldingen fra 27. juli (Tomra, 2023) opplyste om at aktøren begynte rekognosering 10. juli, før de iverksatte angrepet 15. juli. Ved hjelp av brannmur og nettverkstrafikk loggene som en kilde mot SIEM-en kunne vi potensielt detektert når aktøren var i prosessen med å kartlegge systemet. Denne loggen vil vise blant annet port scan, mislykkede påloggingsforsøk samt gi informasjon om eventuelle IP-adresser som blir brukt i denne sammenhengen. Dersom dette hadde vært implementert sammen med segmentering av nettverket kunne det vært mulig å detektere unormal og uautorisert tilgang gjennom segmenter.

Sikkerhetslogger, her vil både suksessfulle og mislykkede påloggінger, brukere som logger av og endringer i innstillingene til en bruker dukke opp. Dette vil kunne oppdage blant annet endringer av brukerpassord og endring av privilegier, som begge inngikk i angrepet på Tomra, som rapportert 29. september (Tomra, 2023). Dersom det er brannmurer på plass, vil disse loggene også fange opp eventuelle endringer i brannmur reglene, som kan være veldig aktuelt ved videre traversering av nettverket etter at aktøren har oppnådd eskalerte privilegier.

Logger for brukeraktivitet, ved å følge med på aktiviteten til brukere i systemet vil en SIEM kunne ha oversikt og analysere hvilke brukere som interagerer med forskjellige filer. Dersom en er klar over hvordan vanlig aktivitet ser ut for hver enkelt bruker kan en lettere oppdage unormale hendelser, hvor en eventuell uautorisert aktør er inne på en bruker og leser av, endrer, lager eller sletter filer i systemet.

Oppgave 1.c

Kontinuerlig overvåking: Ved å følge med på brukere og oppførselen til systemer i nettverket kan vi identifisere unormale hendelser. Dette kan blant annet være at en bruker begynner å logge inn på tidspunkter som ikke har vært vanlig tidligere, en bruker har fått tilganger som de ikke trenger eller har hatt tidligere eller annet. Ved å monitorere dette kan sikkerhets teamet i selskapet ha en raskere respons og håndtere hendelser før de rekker å bli et større problem eller før det sprer seg.

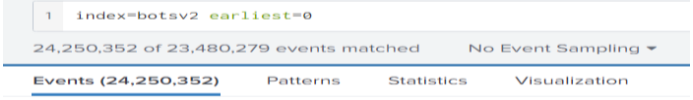
Tofaktorautentisering: Ved å implementere 2FA vil bedriften legge til enda et element for å autentisere en brukeren i systemet. Selv om en aktør skulle fått tilgang til brukernavn og, som nevnt i pressemeldingen fra 27. juli (Tomra, 2023) legitime passord, vil det ikke være mulig å oppnå tilgang til brukeren uten tilgang på en 2FA. For eksempel en tidsbegrenset kode, generert i en app.

Least Privilege Access: I Tomra sitt tilfelle mener jeg dette er viktigere enn segmentering, fordi ut ifra rapporten fra 20. juli (Tomra, 2023) klarte de å holde angrepet forholdsvis inneholdt og det var hovedsakelig Montreal avdelingen som ble påvirket direkte. Prinsippet vil gi alle brukere I systemet kun tilgang som er strengt nødvendig. Dette vil resultere i at, dersom en aktør først kommer seg forbi tiltakene for å sikre en bruker, vil aktøren ha minst mulig muligheter for å utføre videre angrep og muligheter for potensiell skade vil bli redusert.

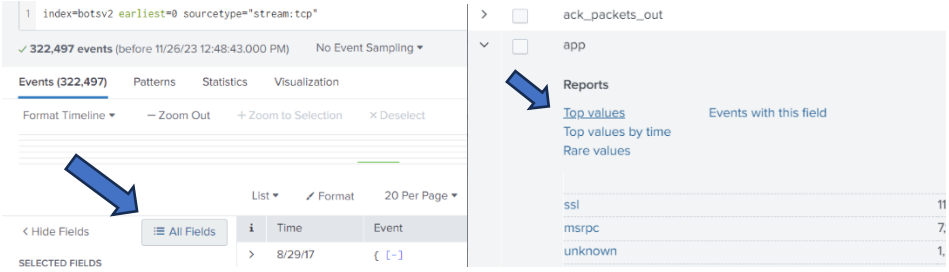
Oppgave 2.a

Først hentet jeg filen med wget i CyUbuntu VM. Deretter validerte md5 summen. Deretter pakkes filen i directory til splunk, /opt/splunk/etc/apps. Dette gjorde jeg med kommandoen: **sudo tar -xvzf botsv2_data_set_attack_only.tgz -C /opt/splunk/etc/apps**

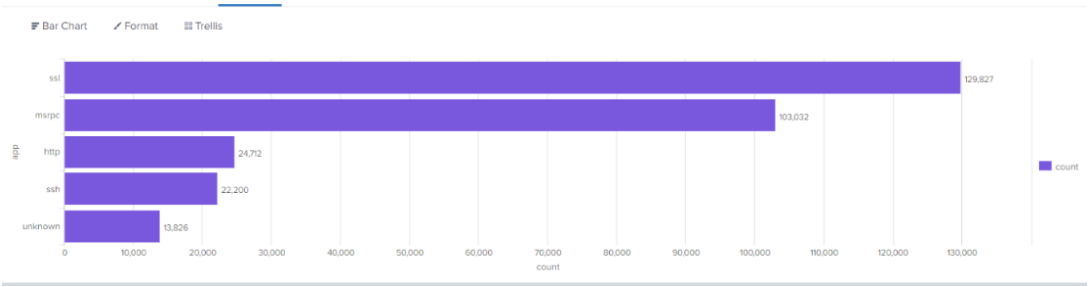
Etter å ha pakket ut datasettet i directory kjørte jeg en enkel spørring med «**index=botsv2 earliest=0**» med filteret for «All Time» og får eventene i datasettet.



Gjorde først et generelt søk etter alt som var på TCP strømmen, med spørringen «index=botsv2 earliest=0 sourcetype="stream:tcp"»
Trykket på «All Fields» og ser etter TCP protokoller. Under «App» finner jeg en liste over TCP protokoller. Velger da valget «Top Values».

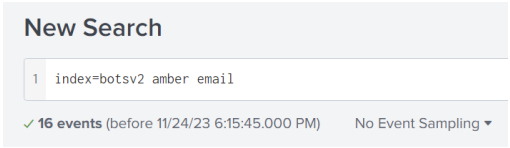


Da fikk jeg syntaksen «index=botsv2 earliest=0 sourcetype="stream:tcp"| top limit=20 app» endrer limit til 5. Dette ga følgende visualisering:



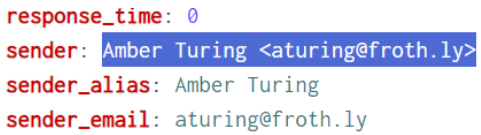
Oppgave 2.b

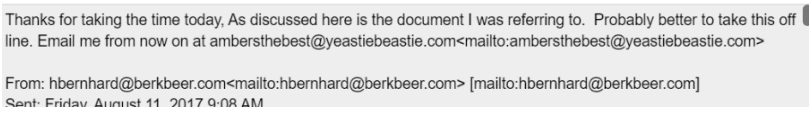
Starter med å søke løst etter eposter og etter navnet Amber. Jeg bruker syntaxen: «index=botsv2 amber email»



Jeg finner raskt en epost-adresse som tilhører en Amber Turing. Ettersom søket kun gir 16 events velger jeg å gå gjennom alle manuelt.

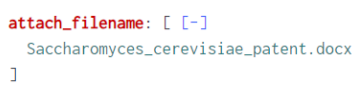
Jeg manuelt sjekker content_body til eventet datert 8/30/17 5:08:00.075 PM finner jeg straks noe som ligner Base64. Jeg oversetter fra Base64 til vanlig tekst of får:





Vi har nå enda en epost for Amber. Ambersthebest2yeastiebeastie.com. I bodyen på denne finner jeg også en delt opp e-post som er «amberk@berkbeer.com» Jeg beholder syntaxen over, kun Amber og Email og klikker på All Fields. Der får finner jeg frem til attach_filename{}. Åpner denne og får syntaxen:

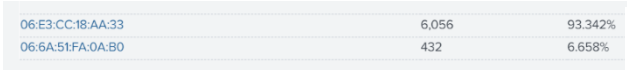
«index="botsv2" earliest=0 amber email "attach_filename{}"="*"» og finner filnavnet på attachementet som Amber har sendt, slik:



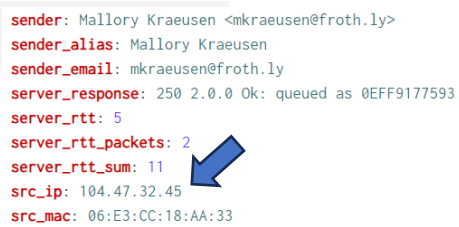
Jeg bruker syntaxen «index="botsv2" earliest=0 sourcetype=stream:smtp amber» for litt manuell snoking i smtp protokollen etter Amber og får en rekke e-poster: amber_hsu94@yahoo.com.tw, amber_honey_and_roses@yahoo.com.tw, amber_yu@yahoo.com.tw, amber.eeeee@yahoo.com.tw, amber.h@yahoo.com.tw, amber_luoluo@kimo.com, silvern_amber@yahoo.com.tw.

Matar er et host-name. Jeg søker på «* host=matar app=smtp». I feltene så varierer IP-adressene, så jeg velger å se på Mac-Adressen i stedet. Her er det tydelig 1 som skiller seg ut.

Jeg søker på denne med «index="botsv2" earliest=0 src_mac="06:E3:CC:18:AA:33" sender="*"».



Jeg får 1 event, og det er kun 1 e-post knyttet til dette søket.



Resultatet er at det er mkraeusen@froth.ly er knyttet til «matar» og sender mail til maxneckb3ard@gmail.com.

E-postene til amber: ambersthebest@yeastiebeastie.com, aturing@froth.ly, amberk@berkbeer.com, amber_hsu94@yahoo.com.tw, amber_honey_and_roses@yahoo.com.tw, amber_yu@yahoo.com.tw, amber.eeeee@yahoo.com.tw, amber.h@yahoo.com.tw, amber_luoluo@kimo.com

Hun sender e-post til: hbernhard@berkbeer.com, mberk@berkbeer.com, jsmythe@froth.ly, jacobsmythe111@gmail.com

Vedlegg fra Amber: Saccharomyces_cerevisiae_patent.docx

Hvilken epost er knyttet til «matar»: mkraeusen@froth.ly

Hvem sender «matar» epost til: maxneckb3ard@gmail.com

Oppgave 2.c

Når det gjelder fordelene, er ELK primært et open-source rammeverk, som muliggjør gratis bruk av løsningen. I tillegg til økonomisk gunstige aspekter, gir en open-source løsning mulighet for spesifikk tilpasning av ELK i samsvar med organisasjonens krav samt integrasjon med andre løsninger og verktøy. Rammeverket er velegnet for håndtering av store datamengder, og kombinert med dets tilpasningsdyktighet

muliggjør det en sømløs skalering i takt med bedriftens vekst og endrende behov. ELK støtter både lokal implementering («on-prem») og skybaserte løsninger.

Ulempene ved ELK Stack stammer også fra dens open-source karakter. Implementerings- og konfigurasjonsprosessen kan være kompleks og krever spesialisert kompetanse. Videre kan det resultere i betydelig bruk av ressurser og lagringskapasitet, spesielt avhengig av dataenes volum og arkiveringsbehov. Selv om det finnes tjenesteleverandører som tilbyr Elastic som en administrert tjeneste, kan dette øke kostnadene og redusere noen av fordelene knyttet til ELK. En bratt læringskurve er også en utfordring, og organisasjonen må opparbeide seg betydelig kunnskap og forplikte seg til kontinuerlig vedlikehold for å sikre systemets stabilitet.

Organisasjoner som bør vurdere å implementere ELK er de med robust teknisk ekspertise, som kan forstå verdien av open-source konsepter og effektivt drifte løsningen. Dette gjelder spesielt for organisasjoner som ønsker å unngå høye kostnader knyttet til lisenser som følger med andre kommersielle løsninger. De som søker en høyt tilpasningsdyktig løsning bør også vurdere ELK, da rammeverket gir betydelige muligheter for skreddersydd tilpasning av SIEM-løsningen i henhold til spesifikke behov.

Oppgave 3.a

I likhet med tradisjonell e-post-phishing, benytter e-post-quishing seg også av falske e-poster med hensikt å forlede potensielle ofre. Dette inkluderer bruken av forfalskede e-postadresser og etterligninger av autentiske avsendere. Begge metodene har til hensikt å dirigere offeret mot en falsk, ofte klonet, nettside, der nettstedet fremstår som legitim, men der informasjonen blir avslørt til en ondsinnet aktør. I visse tilfeller kan QR-koden initiere nedlasting av skadelig programvare, parallelt med visse ondsinnede URL-er.

Den største forskjellen fra tradisjonell phishing ligger i bruken av QR-koder i stedet for hyperlenker. Dette innfører ekstra utfordringer på flere nivåer. Tradisjonell phishing har vært utbredt over lengre tid, og økt oppmerksomhet har ført til forbedret evne til å identifisere mistenkelige URL-er blant allmennheten. Mange e-posttjenester har innebygde filtre, og selskaper har implementert interne sikkerhetskontroller for å avdekke slike trusler. Problematikken med quishing ligger i begrensningene enkelte verktøy møter i deteksjon av skadelige elementer i form av

bilder, enten de er «embedded» eller som vedlegg i en e-post. Ved å inkorporere disse lenkene i et bilde reduseres offerets evne til å identifisere skadelige lenker før QR-koden skannes.

Siden QR-koder krever scanning av et kamera, kan det oppstå scenarioer der interne sikkerhetsinfrastrukturer i et selskap kunne ha identifisert den skadelige lenken og blokkert den. Imidlertid kan dette omgås dersom offeret bruker en privat telefon og skanner med sitt eget kamera som ikke er med av infrastrukturen og sikkerheten til selskapet.

Oppgave 3.b

Kjørte først en FILE kommando på filen for å se hva det var. Deretter Strings for å lese av.

```
cyb2100@ubuntu-vm:~/eksamen23/3_b$ file RevisedContract.eml
RevisedContract.eml: SMTP mail, ASCII text, with CRLF line terminators
cyb2100@ubuntu-vm:~/eksamen23/3_b$ strings RevisedContract.eml > readables.txt
cyb2100@ubuntu-vm:~/eksamen23/3_b$ gedit readables.txt
cyb2100@ubuntu-vm:~/eksamen23/3_b$
```

```
Content-Disposition: attachment; filename="Personal Contract.docm"
Content-Type: application/vnd.ms-word.document.macroEnabled.12;
        name="Personal Contract.docm"
```

Etter å ha lest gjennom .eml filen fikk jeg vite at passordet for krypteringen er eposten til mottaker, «johnny@123.com», og ser at den har et vedlegg som .docm. Jeg laster opp filen i en EML viewer, og laster ned vedlegget herifra. Deretter dekrypterer jeg docm filen som jeg fikk med et Office-verktøy, passordet vi fikk opplyst i eml filen, og kjører en «strings» kommando på filen for å få en fil. Her får jeg info om at det er et bilde samt litt tekst i filen, og ikke mye annet interessant.

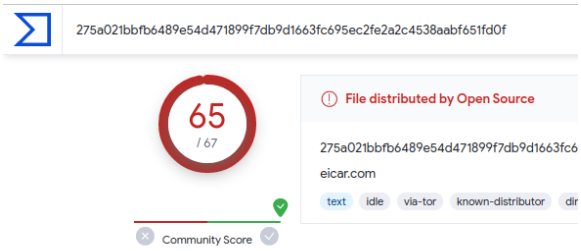
```
36 word/media/image1.png
decrypted_file.docm  encrypted_file.txt  readables.txt
cyb2100@ubuntu-vm:~/eksamen23/3_b$ msoffcrypto-tool Personal+Contract.docm Personal+Contract_nopass.docm --password=johnny@123.com
cyb2100@ubuntu-vm:~/eksamen23/3_b$ strings -a Personal+Contract_nopass.docm > personal_contract_strings.txt
cyb2100@ubuntu-vm:~/eksamen23/3_b$ gedit personal_contract_strings.txt
```

Etter å ikke ha funnet noe skadevare eller makroer på selve filen åpner jeg den og finner en QR-kode.

Denne laster jeg opp i «QRCode Raptor» sin skanner og får url. som output. «https://secure.eicar.org/eicar.com». Jeg

åpner denne i et sikkert miljø og den laster automatisk ned en fil. Denne analyserer jeg med «file» og laster opp på VT og får info om at dette er skadevare (test-fil, men tar utgangspunkt i at dette er et realistisk scenario).

```
cyb2100@ubuntu-vm:~/eksamen23/3_b$ file eicar.com
eicar.com: EICAR virus test files
cyb2100@ubuntu-vm:~/eksamen23/3_b$
```



Konklusjon: Medarbeideren mottok en e-post med en passord beskyttet fil. Denne filen var ikke skadelig i seg selv, men innehold en QR-kode brukt for «Quishing». Denne QR-koden sender vedkommende til en skadelig nettside og laster ned skadevare straks en er inne på nettsiden. Denne slo ut som å være en Trojaner på VT. (Disclaimer. Dette var ikke en ekte skadelig fil, men en fil for simulering, men jeg går ut ifra at dersom dette var et realistisk scenario var det faktisk skadevare.)

Oppgave 3.c

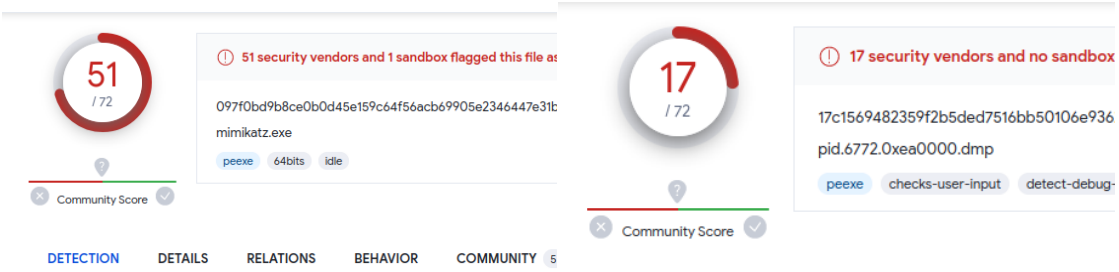
```
cyb2100@ubuntu-vm:~/eksamen23/3_c$ vol.py -f MSEDGEWIN10-20231107-184623.raw windows.pslist > prosesser.txt
```

Etter å ha gått gjennom tekstfilen med prosesser, bet jeg meg fast i to prosesser en som het mimikatz med pid 7068 og dumpit med pid 6772. Jeg kjørte kommandoen: «vol.py -f MSEDGEWIN10-20231107-184623.raw windows.pslist.PsList --pid 7068 –dump»

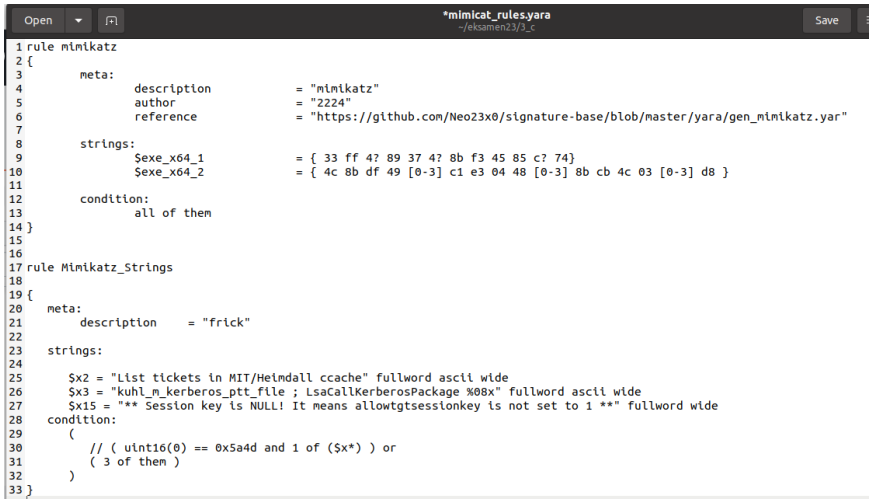
```
cyb2100@ubuntu-vm:~/eksamen23/3_c$ vol.py -f MSEDGEWIN10-20231107-184623.raw windows.pslist.PsList --pid 7068 --dump
Volatility 3 Framework 2.5.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File
 output

7068    4032    mimikatz.exe    0x9b82bbfe4540  3       -       1       False   2023-11-07 18:45:57.000000      N/A     pid.
7068.0x7ff60f0e0000.dmp
cyb2100@ubuntu-vm:~/eksamen23/3_c$
```

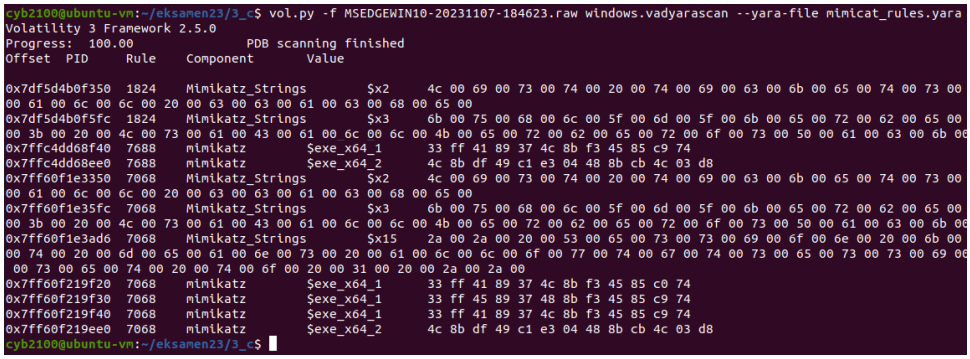
med hver respektive id og fikk to filer jeg lastet opp på VT. Filen for 7068 slo ut på 51/72 på VT som en Trojaner mens 6772 slo kun ut på 17/72, men også som en Trojaner.



Selv om DumpIt.exe slo ut hos noen aktører, virker dette som et legitimt verktøy, som kanskje muligens er brukt hos noen trojanere, men ikke nødvendigvis betyr at det er en skadelig prosess. Mimikatz derimot, er et anerkjent verktøy for å hente ut passord som er lagret i minnet og som også utfører exploits og jeg går videre med dette. Jeg lager en Yara regel som skal detektere Mimikatz prosessen i minnedumpen. Slik:



Denne bruker jeg med Volatility modulen Yarascan med kommandoen: vol.py -f MSEDGEWIN10-20231107-184623.raw windows.vadyarascan --yara-file mimicat_rules.yar og får flere treff. Det er en del False-positives men viktigst dukker prosessen 7068 opp, som vi er ute etter og kan se bort ifra resten.



(Bilde er klippet for å få plass)

Oppgave 3.d

Gjennom implementeringen av standardisering med NIS2 og CRA, kan det etableres krav til cybersikkerhet blant organisasjoner som leverer tjenester eller produkter innenfor EU. Dette kan skape insentiver for investeringer i sikkerhet, da brudd på disse normene kan føre til økte økonomiske konsekvenser for organisasjonene. Ved å pålegge produsenter ansvaret for cybersikkerheten til produktene «fra utviklings- og designfasen og inntil fem år fra produktet plasseres på markedet» (Regjeringen,

2023, 8. august), styrkes særlig sikkerheten til produkter som IoT-enheter. Dette initiativet har potensiale til å utbedre eksisterende og fremtidige sårbarheter og dermed skape et mer robust sikkerhetsmiljø for organisasjoner som benytter slike enheter.

Videre legges det vekt på behovet for «Incident Response Planning». Dette tiltaket har til hensikt å redusere omfanget av skade ved potensielle cyberangrep ved å pålegge organisasjoner å utvikle og implementere planer for håndtering av hendelser. Resultatet av en effektiv håndtering vil være en begrensning av virkningen angrepene har på organisasjonen, samtidig som det minimerer konsekvensene for tredjeparter avhengige av organisasjonens tjenester. Gjennom slike regulatoriske tiltak kan EU som helhet styrke sitt forsvar mot cyberangrep, og som en følge redusere ringvirkningene av slike angrep på innen EU.

Tiltak som en mellomstor norsk bedrift kan gjøre innebærer sikkerhetsopplæring, sikkerhetskopiering og gjenoppretting samt kartlegging og oppdatering av systemer.

En ufravikelig faktor er tilstrekkelig sikkerhetsopplæring, som forblir en fundamental nødvendighet for organisasjoner. Effektiviteten av sikkerhetstiltak vil betydelig reduseres dersom ansatte, uvitende omgår dem. Gjennom en tilstrekkelig Cybersikkerhet-Awareness kan organisasjonen redusere sårbarheten ved å forhindre at ansatte uvitende gir tilgang til ondsinnede aktører eller skadelig programvare.

Videre vil implementering av regelmessig sikkerhetskopi av systemer og data styrke organisasjonens beredskap mot angrep som resulterer i datatap eller ransomware, som har opplevd raskt økende utbredelse. En strategisk utformet gjenopprettingsplan vil ikke bare muliggjøre effektiv gjenoppretting av tapte data, men også minimere nedetiden og akselerere retur til normal drift.

Kartlegging av organisasjonens datastruktur og innføring av systematiske rutiner for oppdatering eliminerer potensielle sårbarheter i utdaterte datasystemer. En omfattende oversikt over organisasjonens enheter og systemer reduserer risikoen for at enheter, som for eksempel eldre servere, overses og dermed unnlater nødvendige oppdateringer. Sammen med etablerte rutiner for system- og programvareoppdateringer elimineres potensielle inngangspunkter for aktører som søker sårbarheter i systemet.

Litteraturliste:

Australian Signals Directorate's Australian Cyber Security Centre. (2023, 27. november). *What is Quishing?* https://www.cyber.gov.au/learn-basics/explore-basics/watch-out-threats/quishing

Arntz, P. (2023, 13. oktober). *Explained: Quishing.* https://www.malwarebytes.com/blog/news/2023/10/explained-quishing

Cloudflare. (u.å.) *Zero Trust security | What is a Zero Trust network?* Hentet 26. November 2023 fra https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/

Elastic. (2023, 28. november). *Free,open,and here's why.* https://www.elastic.co/about/free-and-open

EØS-notat. (2023, 08. august) *Cyber Resilience Act.* https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2022/juni/cyber-resilience-act/id2984059/

EØS-notat. (2023, 23. august) *NIS2-direktivet.* https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2021/feb/nis2-direktivet/id2846097/

National Institute of Standards and Technology (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. NIST. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Ramberg, H. (2023). *SIEM* [Lysbildepresentasjon]. Canvas. https://kristiania.instructure.com/courses/10846/files/1201829?module_item_id=416850

Ramberg, H. (2023). *Defendable Arkitektur* [Lysbildepresentasjon]. Canvas. https://kristiania.instructure.com/courses/10846/files/1245107?module_item_id=430268

Ramberg, H. (2023). *Security Basics.* [Lysbildepresentasjon]. Canvas. https://kristiania.instructure.com/courses/10846/files/1183491?module_item_id=406493

Tomra. (2023, 20. Juli) *TOMRA: July 20th update on cyberattack*. https://www.tomra.com/en/news-and-media/news/2023/tomra-july-20th-update-on-cyberattack

Tomra. (2023, 27. Juli) *TOMRA: July 27th update on cyberattack*. https://www.tomra.com/en/news-and-media/news/2023/september-1st-update-on-cyberattack

Tomra. (2023, 29. September) *TOMRA's swift response paves the way for normalization after cyberattack.* https://www.tomra.com/en/news-and-media/news/2023/tomras-swift-response-paves-the-way-for-normalization-after-cyberattack