Navn: _____ Dato: _____ Poeng: _____

Analyse av skadevare og reduksjon av trusler Guide

Trojanere, løsepengevirus, spionvare, rootkits, virtualiseringssandkasser, inneslutning

LÆRINGSOVERSIKT: ANALYSE AV SKADEVARE

SIKRET

DATAKRYPTERING

256-bits AES-standard

I SAMSVAR

GLOBALE STANDARDER

Rammeverk for GDPR og CCPA

ZERO TRUST

TILGANGSPOLICY

Flerfaktorautentisering

Velkommen! Dette aktivitetsheftet veileder deg gjennom analyse og forebygging av skadevare. Du utforsker spionvare, trojanere, løsepengevirus-nyttelaster, verktøy for reverse engineering, rootkit-atferd og strategier for inneslutning.

KONTROLLPUNKTER I ARBEIDSARKET

- [ ] **Del 1-4: Behersk cybersikkerhet og forebygging av trusler.**
- [ ] **Del 5-7: Løs kryssord og ordsøk.**
- [ ] **Del 8-9: Løs casestudier og chifferutfordringen.**
- [ ] **Del 10: Gå gjennom sidene med grunnleggende og avanserte vanlige spørsmål.**
- [ ] **Del 11: Utforsk 10 interessante fakta fra virkeligheten.**
- [ ] **Bonus: Tenk raskt-utfordring.**

Åpne VPN.coms veiledning om cybersikkerhet

URL: https://www.vpn.com/no/cybersikkerhet/skadevare/

Din læringsveiledning for håndtering av skadevare

- Skill mellom skadevaretypene trojaner, orm og rootkit.
- Innfør kjøring i virtualisert sandkasse for kodeanalyse.
- Utform planer for inneslutning og sanering av aktive løsepengevirus-nyttelaster.

INSTRUKSJONER FOR GUIDE TIL ANALYSE AV SKADEVARE

Svar på flervalgsspørsmålene og sant/usant-spørsmålene, fyll ut setningene med ordbanken, koble sammen definisjoner, og løs kryssordet og ordsøket. Bruk kunnskapen din på begrensning av skadevare. Avslutt med bonusaktiviteten Tenk raskt.

ANALYSE AV SKADEVARE OG INNDEMMING AV TRUSLER (INNLEDNING)

Skadelig kode som trojanere, ormer og løsepengevirus utgjør trusler med stor innvirkning for endepunkter og servere. Sikkerhetsteam analyserer skadevare i virtuelle sandkasser og iverksetter raske nettverksisolasjonstiltak for å begrense spredningen av nyttelasten.

LES HVERT KONTROLLPUNKT NØYE OG VELG ELLER SKRIV DET RIKTIGE SVARET.

Kontrollpunkt 1: Flervalgsutfordring

1. **1. Hva er det definerende kjennetegnet ved en trojansk hest?**
   - A. Den utgir seg for å være legitim programvare for å lure brukere til å kjøre den
   - B. Den replikerer seg automatisk over lokale nettverkslinjer
   - C. Den infiserer filer i isolerte virtuelle sandkasser
   - D. Den avskjærer trafikk fra internettleverandøren

2. **2. Hvilken type skadevare krypterer filer og krever betaling?**
   - A. Løsepengevirus
   - B. Spionprogram
   - C. Rootkit
   - D. Reklameprogramvare

3. **3. Hva representerer spionvare?**
   - A. Skadevare utformet for å i det skjulte overvåke brukerens tastetrykk og nettleseraktivitet
   - B. Programkode som kjører i en virtuell container i sandkasse
   - C. Oppdateringer mot skadevare lastet ned fra databaseregistre
   - D. Automatisk justering av skjermlysstyrke

4. **4. Hvorfor bruker utviklere av skadevare rootkits?**
   - A. Å skjule aktive prosesser og skadelige filer fra operativsystemet
   - B. Å øke CPU-prosesseringshastigheten på endepunkter
   - C. For å sikkerhetskopiere databasefiler til sikre skyhvelv
   - D. For å forbedre batteritiden på bærbare datamaskiner

5. **5. Hva betyr sandboxing i analyse av skadevare?**
   - A. Å kjøre mistenkelige filer i et isolert virtuelt hvelv for å observere atferden trygt
   - B. Å skanne filhasher mot databaser over kjente trusler
   - C. Å gjenopprette databasesikkerhetskopier etter et innbrudd
   - D. Å koble lokale nettverksrutere fra offentlige linjer

Kontrollpunkt 2: Utfordring med sant eller usant

6 Spørsmål 6

6. Dataormer krever menneskelig brukerinteraksjon for å spre seg over lokale nettverk.

○ Sant ○ Usant

7 Spørsmål 7

7. Reklamevare er alltid harmløs og sporer ikke brukeratferd eller nettleserhistorikk.

○ Sant ○ Usant

8 Spørsmål 8

8. Gjenoppretting av rene offline-sikkerhetskopier lar ofre få tilbake krypterte filer uten å betale løsepengene.

○ Sant ○ Usant

9 Spørsmål 9

9. Signaturbasert antivirus stopper pålitelig zero-day-skadevare før det finnes noen signatur for den.

○ Sant ○ Usant

10 Spørsmål 10

10. Filløs skadevare kjører skadelige skript i systemminnet og unngår å skrive filer til disken.

○ Sant ○ Usant

Kontrollpunkt 3: Sett inn nøkkelbegreper

Les hver setning nedenfor og fyll ut det tomme feltet med riktig begrep fra ordbanken.

1. Skadevare forkledd som et trygt verktøyprogram er en _____ .
2. Skadelig nyttelast som låser databasesystemer for penger, er eksempler på _____ .
3. Tastaturloggere som i det skjulte registrerer passord, er eksempler på _____ .
4. Å skjule seg dypt i operativsystemets kjerner krever et _____ .
5. Å analysere mistenkelige filer i et isolert hvelv bruker en virtuell _____ .
6. Å stanse spredningen av aktive skadevarenyttelaster krever umiddelbar _____ i nettverket.

ORDBANK

DATAMASK FILLØS INNDEMMING RISIKO FOR LØSEPENGEVIRUS ROOTKIT SANDKASSE SPIONVARE TROJANER

Skriv svarene dine her:

1.
2.
3.
4.
5.
6.

Kontrollpunkt 4: Koble sikkerhetsbegreper

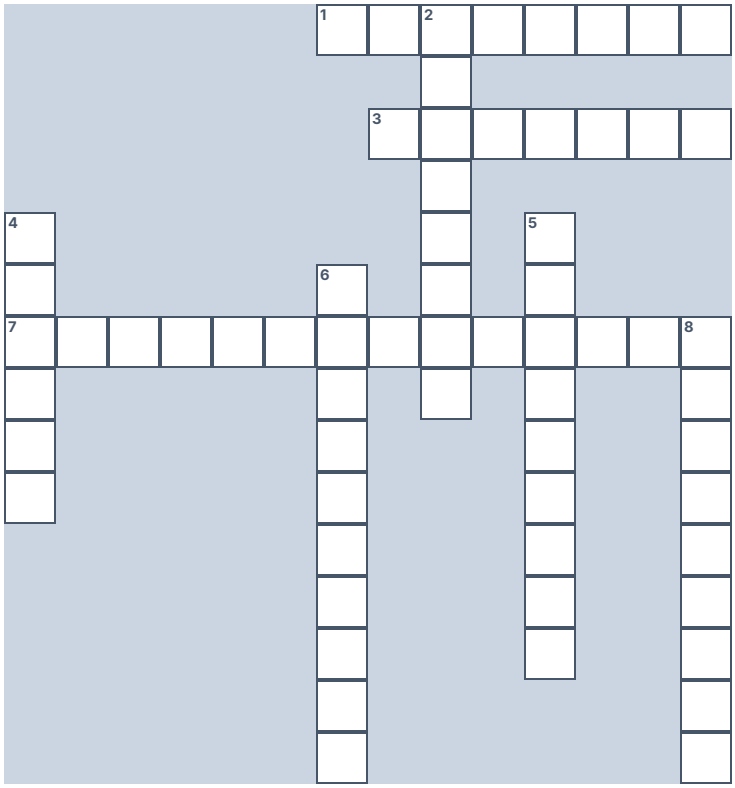
KOBLE DEFINISJONER

Koble hvert fagbegrep til venstre med riktig definisjon til høyre ved å skrive den tilhørende bokstaven (A-H) i det utfyllbare feltet.

☐	1. TROJANER	A	Program utformet for å overvåke og registrere brukeraktivitet og inndata i det skjulte.
☐	2. RISIKO FOR LØSEPENGEVIRUS	B	Skadevare som kjører direkte i RAM for å unngå oppdagelse av diskskannere.
☐	3. SPIONPROGRAMVARE	C	Begrensning av infiserte endepunkter for å hindre spredning av trusselnyttelast.
☐	4. ROOTKIT	D	Skadelig programvare som utgir seg for å være et ufarlig eller nyttig verktøyprogram.
☐	5. SANDKASSE	E	Selvspredende skadevare som sprer seg over nettverk uten menneskelig handling.
☐	6. BEGRENSNING	F	Skadevare som krypterer systemlagring og krever betaling for å levere nøkkelen.
☐	7. WORM	G	Isolert virtuelt miljø som brukes til å analysere skadelige filer på en trygg måte.
☐	8. FILLØS	H	Skjult skadevare som gjemmer seg dypt i systemkjerner for å beholde administrativ kontroll.

Kontrollpunkt 5: Kryssord

Løs kryssordet ved å skrive bokstaver i de aktive hvite rutene. Tallene tilsvarer hintene nedenfor.



VANNRETT

1. Selvreplikerende skadevare som sprer seg over nettverk uten menneskelig handling. (8)

3. Skjult skadevare som gjemmer seg dypt i systemkjerner for å beholde administrativ kontroll. (7)

7. Skadevare som krypterer systemlagring og krever betaling for å levere nøkkelen. (14)

LODDRETT

2. Skadelig programvare forkledd som et harmløst eller nyttig verktøyprogram. (8)

4. Skadevare som kjører direkte i RAM for å unngå oppdagelse av diskskannere. (6)

5. Program utformet for å i det skjulte overvåke og registrere brukeraktivitet og inndata. (9)

6. Begrensning av infiserte endepunkter for å hindre at trusselnyttelast sprer seg. (10)

8. Isolert virtuelt miljø som brukes til å analysere skadelige filer trygt. (9)

Kontrollpunkt 5, alternativ: Tilgjengelige kryssordhint

Brukere av skjermleser og tastatur kan skrive inn kryssordsvarene direkte i tekstfeltene nedenfor.

VANNRETT

1 vannrett: Selvreplikerende skadevare som sprer seg over nettverk uten menneskelig handling. (8 bokstaver):

3 vannrett: Skjult skadevare som gjemmer seg dypt i systemkjerner for å beholde administrativ kontroll. (7 bokstaver):

7 vannrett: Skadevare som krypterer systemlagring og krever betaling for å levere nøkkelen. (14 bokstaver):

LODDRETT

2 loddrett: Skadelig programvare forkledd som et harmløst eller nyttig verktøyprogram. (8 bokstaver):

4 loddrett: Skadevare som kjører direkte i RAM for å unngå oppdagelse av diskskannere. (6 bokstaver):

5 loddrett: Program utformet for å i det skjulte overvåke og registrere brukeraktivitet og inndata. (9 bokstaver):

6 loddrett: Begrensning av infiserte endepunkter for å hindre at trusselnyttelast sprer seg. (10 bokstaver):

8 loddrett: Isolert virtuelt miljø som brukes til å analysere skadelige filer trygt. (9 bokstaver):

Kontrollpunkt 6: Skjult ordsøk

Finn de 8 sentrale ordforrådsbegrepene som er skjult i rutenettet nedenfor. Ordene kan stå vannrett, loddrett eller diagonalt.

J U Å U G S Y S F A A S Q O R

W R Æ S L T W P U D S O Ø B G

G E S U Z Z K I A T A Å Ø Ø M

N N Ø H R J O O T L N N N V Q

I A L I O S S N H Å D A Q X G

M J L X O C Ø V T Ø K B I N Å

M O I H T K P A R P A Z C N Å

E R F Ø K G Æ R Q Y S X M X R

D T B P I Y V E N H S X D Ø X

N L T B T Z Å Æ N T E S Æ J Q

N L Ø S E P E N G E V I R U S

I E A D L S Y Z Z M K I W I G

B F D A T A M A S K J L V U Y

T Å F I F U C A M R C Å N L Y

T W A U Z K N N H I O I T G M

ORDLISTE

TROJANER LØSEPENGEVIRUS SPIONVARE ROOTKIT SANDKASSE INNDEMMING DATAMASK FILLØS

Kontrollpunkt 6, alternativ: Tilgjengelig ordkobling

Koble hvert av de 8 fagbegrepene fra ordsøket til riktig definisjon ved å skrive bokstaven (A-H) i det tomme feltet.

BEGREPER
A. TROJANER
B. LØSEPENGEVIRUS
C. SPIONVARE
D. ROOTKIT
E. SANDKASSE
F. INNDEMMING
G. DATAMASK
H. FILLØS

DEFINISJONER OG TILHØRENDE FELT
[ ] 1. Skjult skadevare som gjemmer seg dypt i systemkjerner for å beholde administrativ kontroll.
[ ] 2. Begrensning av infiserte endepunkter for å hindre at trusselnyttelast sprer seg.
[ ] 3. Skadevare som kjører direkte i RAM for å unngå oppdagelse av diskskannere.
[ ] 4. Selvreplikerende skadevare som sprer seg over nettverk uten menneskelig handling.
[ ] 5. Skadevare som krypterer systemlagring og krever betaling for å levere nøkkelen.
[ ] 6. Program utformet for å i det skjulte overvåke og registrere brukeraktivitet og inndata.
[ ] 7. Skadelig programvare forkledd som et harmløst eller nyttig verktøyprogram.
[ ] 8. Isolert virtuelt miljø som brukes til å analysere skadelige filer trygt.

Kontrollpunkt 7: Utfordring med blandede ord

Sett bokstavene nedenfor sammen i riktig rekkefølge for å avsløre sentrale begreper innen cybersikkerhet. Skriv svarene dine i svarboksene.

1. **EJATNRRO**
2. **ESROPVANI**
3. **SAKASEDSN**
4. **ASKAMDAT**
5. **VSRØGEPSEIN LUE**
6. **IOKRTTO**
7. **NDIMMINGEN**
8. **LSFØLI**

Bonusaktivitet: Tenk raskt

3 SVAR PER KATEGORI. DEN SOM FYLLER UT LISTEN FØRST, VINNER.

1	Steder å laste ned trygge apper			
2	Enheter som kan hackes			
3	Ting du tar sikkerhetskopi av			
4	Advarselstegn i en e-post			
5	Tegn på at en telefon har skadevare			
6	Typer skadevare du kjenner til			
7	Filtyper du bør være forsiktig med			
8	Måter skadevare kommer seg inn på en PC			
9	Trygge vaner du kan begynne med i dag			
10	Ord knyttet til cybersikkerhet			
11	Ting å gjøre etter en datalekkasje			
12	Grunner til å oppdatere programvare			
13	Dyr eller figurer med navn som ligner på skadevare			
14	Ting skadevare kan stjele			
15	Ting å gjøre hvis du klikket på feil lenke			

Kontrollpunkt 8: Casestudier om cybersikkerhet

Bruk begrepene du har lært til å løse de virkelige scenarioene nedenfor.

CASESTUDIE 1: BEGRENSNING AV LØSEPENGEVIRUS-NYTTELAST I BEDRIFTER



Scenario: Et lokalnett i en bedrift er brutt opp av aktivt løsepengevirus. Sentrale filservere har begynt å vise filtypene .locked. Fastsett retningslinjer for inneslutning.

Diskusjonsspørsmål: Beskriv i detalj trinnene for inneslutning, og skisser protokollen for datagjenoppretting.

CASESTUDIE 2: MINNEINJEKSJON AV FILLØS SKADEVARE



Scenario: En analytiker oppdager mistenkelige skriptmønstre som kjøres direkte i systemets flyktige RAM ved hjelp av vanlige administrative verktøy, men det finnes ingen skadelige filer på disken.

Diskusjonsspørsmål: Forklar strategien for minneanalyse, og angi verktøy for å blokkere filløs kjøring.

Kontrollpunkt 9: Knekk chifferet

En cybersikkerhetsekspert beskytter nettverksressurser mot trusselaktører på nettet. Bruk nøkkelen med bokstaver og tall nedenfor til å dekryptere meldingen ved å skrive de tilhørende bokstavene i de tomme feltene.

NØKKEL FOR KRYPTERING AV BOKSTAV TIL TALL

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26 Æ=27 Ø=28 Å=29

6	9	14	14		19	11	1	4	5	12	9	7	
14	25	20	20	5	12	1	19	20		13	5	4	
1	20	6	5	18	4	19	15	22	5	18	22	29	11	9	14	7

Dekodet melding:

TIPS: HVERT TALL REPRESENTERER BOKSTAVENS PLASS I ALFABETET (F.EKS. 1 = A, 2 = B, 29 = Å).

Kontrollpunkt 10: Grunnleggende vanlige spørsmål om cybersikkerhet (Del A)

Gå gjennom vanlige spørsmål og svar om å redusere trusler på nettet.

Q1: Hva er skadevare?

Skadelig programvare som er utformet av trusselaktører for å skade, kapre eller stjele data fra enheter og nettverk.

Q2: Hva er forskjellen mellom et virus og en orm?

Et virus krever menneskelig handling (som å åpne en fil) for å spre seg, mens en orm sprer seg automatisk over nettverk.

Q3: Hvordan infiserer en trojansk hest en datamaskin?

Den lurer brukere ved å utgi seg for å være et harmløst eller trygt program og skjuler den skadelige nyttelasten inni.

Q4: Hva er løsepengevirus?

En type skadevare som krypterer filer på målsystemet og krever økonomisk betaling i bytte mot dekrypteringsnøkkelen. [1]

Q5: Hva er spionprogramvare?

Skadelig programvare som i hemmelighet registrerer brukerens tastetrykk, passord og surfevaner for å sende dem til angripere.

Kontrollpunkt 10: Grunnleggende vanlige spørsmål om cybersikkerhet (Del B)

Gå gjennom vanlige spørsmål og svar om å redusere trusler på nettet.

Q6: Hva betyr sandboxing?

Å kjøre mistenkelige filer i et sikkert, isolert virtuelt miljø for å observere atferden deres uten risiko for produksjonssystemer.

Q7: Hva er filløs skadevare (fileless malware)?

Skadevare som kjører direkte i systemminnet (RAM) ved hjelp av legitime verktøy og unngår å skrive filer til disken for å omgå enkle skannere.

Q8: Hvordan beskytter et rootkit skadevare?

Den skjuler skadelige prosesser og filer, ofte ved å undergrave operativsystemets kjerne, så antivirusskannere kan gå glipp av dem.

Q9: Hva er dynamisk atferdsovervåking?

Antivirusskanning som overvåker aktive prosesser i sanntid for å blokkere handlinger som er typiske for skadevare, som massekryptering av filer.

Q10: Hvorfor haster det med inneslutning under hendelseshåndtering?

Isolering av kompromitterte endepunkter hindrer aktiv skadevarenyttelast i å spre seg til andre nettverksenheter.

Kontrollpunkt 10: Avanserte vanlige spørsmål om sikkerhet (Del C)

Utforsk avanserte tekniske sider ved sikkerhetsrammeverk, analyse av skadevare og etterlevelse av datakrav.

Q1: Hvordan omgår utviklere av skadevare signaturbaserte antivirusskannere?

De bruker polymorfisme, som endrer filens hash og kodestruktur for hver infeksjon mens den skadelige atferden forblir den samme.

Q2: Hva er risikoen ved verktøy med dobbelt bruksområde i kampanjer med skadevare?

Angripere bruker legitime administrasjonsverktøy (som PowerShell eller Sysinternals) for å gli inn i vanlig nettverkstrafikk, noe som gjør oppdagelse vanskelig.

Q3: Hvordan utfører process hollowing skadelig nyttelast?

Den starter en legitim systemprosess i suspendert tilstand, erstatter minnekoden med skadevare og gjenopptar kjøringen.

Q4: Hva er rollen til en Command and Control-server (C2)?

En ekstern server som drives av hackere for å sende instruksjoner og nyttelaster til skadevare som kjører på kompromitterte maskiner.

Q5: Hvorfor er det vanskelig å oppdage tastetrykklogging (keylogging)?

Enkle keyloggere bruker minimalt med CPU-ressurser og skjuler prosessene sine i legitime verktøy i brukerområdet.

Kontrollpunkt 10: Avanserte vanlige spørsmål om sikkerhet (Del D)

Utforsk avanserte tekniske sider ved sikkerhetsrammeverk, analyse av skadevare og etterlevelse av datakrav.

Q6: Hvordan forsinker kodeobfuskering analyse av skadevare?

Den krypterer eller omorganiserer kildekoden og gjør den uleselig for analyseverktøy og sikkerhetsskannere.

Q7: Hva er funksjonen til et bootkit?

Et rootkit som infiserer oppstartsprosessen (MBR, oppstartssektoren eller UEFI-firmware), slik at det kjører før operativsystemet lastes.

Q8: Hvordan identifiserer heuristisk skanning zero-day-trusler?

Den skanner etter mistenkelige kodemønstre og administrative kommandoer i stedet for å lete etter en samsvarende hash i en database.

Q9: Hva er trusselen fra DLL-kapring (DLL hijacking)?

Å tvinge et legitimt program til å laste et skadelig DLL-bibliotek (dynamic link library) ved å plassere det i programmets katalogsti.

Q10: Hvordan bruker automatiserte analysepipelines for skadevare virtualisering?

De kjører mistenkelige filer på tvers av flere virtuelle maskiner med ulike operativsystemer og genererer automatisk atferdslogger og PCAP-filer for nettverket.

Del 11: 10 fakta om cybersikkerhet fra virkeligheten og innsikt

Gå gjennom virkelighetsnære fakta om sikkerhetsbrudd, forsvarsmekanismer og samsvarsstandarder.

1. SIKKERHETSINNSIKT

Trojanske hester er fortsatt en vanlig infeksjonsmetode fordi de skjuler skadelig kode i programmer som ser harmløse ut.

2. SIKKERHETSINNSIKT

FBIs IC3 mottok over 3 600 klager på løsepengevirus i 2025, med rapporterte tap på over 32 millioner dollar. [3]

3. SIKKERHETSINNSIKT

Ormer kan spre seg raskt over nettverk ved å utnytte sårbarheter i protokoller som ikke er oppdatert, for eksempel EternalBlue i SMB.

4. SIKKERHETSINNSIKT

Filløs skadevare er vanskelig å oppdage fordi den kjører i minnet gjennom legitime verktøy og etterlater få spor på disken.

5. SIKKERHETSINNSIKT

Analysesandkasser går vanligvis tilbake til et rent øyeblikksbilde etter hver kjøring, slik at hver test starter fra en kjent tilstand.

6. SIKKERHETSINNSIKT

Rootkits kan endre systemkall i kjernen og rapportere falske diagnoseresultater til skanneprogrammer for skadevare.

7. SIKKERHETSINNSIKT

Kodeobfuskering bruker pakkeverktøy for å komprimere og skjule den sanne strukturen til skadevarens binære nyttelast.

8. SIKKERHETSINNSIKT

Polymorf skadevare endrer koden sin, og dermed filens hasj, for hver nye kopi for å unngå signaturkontroller.

9. SIKKERHETSINNSIKT

DLL-kapring utnytter søkerekkefølgen i vanlige operativsystemer som Windows.

10. SIKKERHETSINNSIKT

Sikkerhetsleverandører finner enorme mengder nye skadevareprøver hver dag, så signaturer må oppdateres hele tiden.

Tekniske referanser og kilder

Studieveiledningen og de interaktive oppgavene er satt sammen fra globale standarder fra NIST og OWASP og standarder for etterlevelse av personvern.

FAGLIGE REFERANSER OG BRANSJEREFERANSER

[1] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[2] CISA. (2023). #StopRansomware Guide.

https://www.cisa.gov/stopransomware/ransomware-guide

[3] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.

https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[4] FBI Internet Crime Complaint Center. (n.d.). Ransomware.

https://www.ic3.gov/CrimeInfo/Ransomware

[5] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.

https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

Fasit: Kontrollpunkt 1 – flervalg

1 Spørsmål 1

Riktig svar: A

MERKNAD TIL LÆREREN

Hva er det definerende kjennetegnet ved en trojansk hest? → Den utgir seg for å være legitim programvare for å lure brukere til å kjøre den

2 Spørsmål 2

Riktig svar: A

MERKNAD TIL LÆREREN

Hvilken type skadevare krypterer filer og krever betaling? → Løsepengevirus [1]

3 Spørsmål 3

Riktig svar: A

MERKNAD TIL LÆREREN

Hva representerer spionvare? → Skadevare utformet for å i det skjulte overvåke brukerens tastetrykk og nettleseraktivitet

4 Spørsmål 4

Riktig svar: A

MERKNAD TIL LÆREREN

Hvorfor bruker utviklere av skadevare rootkits? → Å skjule aktive prosesser og skadelige filer fra operativsystemet

5 Spørsmål 5

Riktig svar: A

MERKNAD TIL LÆREREN

Hva betyr sandboxing i analyse av skadevare? → Å kjøre mistenkelige filer i et isolert virtuelt hvelv for å observere atferden trygt

Fasit: Kontrollpunkt 2 – sant eller usant

6 Spørsmål 6

Riktig svar: Usant

MERKNAD TIL LÆREREN

Usant: ormer replikerer seg selv og sprer seg over nettverk uten at brukeren gjør noe.

7 Spørsmål 7

Riktig svar: Usant

MERKNAD TIL LÆREREN

Usant: reklamevare er ikke alltid ufarlig; mye av den sporer surfing for å målrette annonser.

8 Spørsmål 8

Riktig svar: Sant

MERKNAD TIL LÆREREN

Sant: rene offline-sikkerhetskopier gjenoppretter krypterte filer uten betaling, selv om stjålne data fortsatt kan lekke.

9 Spørsmål 9

Riktig svar: Usant

MERKNAD TIL LÆREREN

Usant: signaturskannere trenger et kjent eksempel, så splitter ny zero-day-skadevare kan slippe forbi dem.

10 Spørsmål 10

Riktig svar: Sant

MERKNAD TIL LÆREREN

Filløs skadevare kjører skadelige skript i systemminnet og unngår å skrive filer til disken.

Fasit for ordforråd og vurderingsmatrise

Rettemal for læreren: Gi 1 poeng for hver riktige kobling (totalt 8 poeng) og hvert kontekstbegrep (totalt 6 poeng).

KONTROLLPUNKT 4: FASIT – KOBLE BEGREPER

D 1. TROJANER	F 2. RISIKO FOR LØSEPENGEVIRUS	A 3. SPIONPROGRAMVARE	H 4. ROOTKIT
G 5. SANDKASSE	C 6. BEGRENSNING	E 7. WORM	B 8. FILLØS

KONTROLLPUNKT 3: FASIT – NØKKELBEGREPER

1 TROJANER	2 RISIKO FOR LØSEPENGEVIRUS	3 SPIONVARE	4 ROOTKIT
5 SANDKASSE	6 INNDEMMING		

KONTROLLPUNKT 6, ALTERNATIV: FASIT – KOBLE ORD

1 D – ROOTKIT	2 F – INNDEMMING	3 H – FILLØS	4 G – DATAMASK
5 B – LØSEPENGEVIRUS	6 C – SPIONVARE	7 A – TROJANER	8 E – SANDKASSE

DISKUSJONSNOTATER TIL LÆRERE

Nøkkelbegreper:
Kontroller at elevene kan forklare TROJANER, RISIKO FOR LØSEPENGEVIRUS og SPIONPROGRAMVARE med egne ord og gi et eksempel på hvert.

Casestudier:
Be elevene begrunne anbefalingene sine med fakta fra arbeidsarket i stedet for antakelser.

Kildevurdering:
La elevene kontrollere minst én påstand mot kildene i arbeidsarket, og drøft hvorfor tall, priser og regler kan endre seg over tid.

Fasit for oppgavene og merknader til læreren

LØSNING PÅ ORDSØKET

J	U	Å	U	G	S	Y	S	F	A	A	S	Q	O	R
W	R	Æ	S	L	T	W	P	U	D	S	O	Ø	B	G
G	E	S	U	Z	Z	K	I	A	T	A	Å	Ø	Ø	M
N	N	Ø	H	R	J	O	O	T	L	N	N	N	V	Q
I	A	L	I	O	S	S	N	H	Å	D	A	Q	X	G
M	J	L	X	O	C	Ø	V	T	Ø	K	B	I	N	Å
M	O	I	H	T	K	P	A	R	P	A	Z	C	N	Å
E	R	F	Ø	K	G	Æ	R	Q	Y	S	X	M	X	R
D	T	B	P	I	Y	V	E	N	H	S	X	D	Ø	X
N	L	T	B	T	Z	Å	Æ	N	T	E	S	Æ	J	Q
N	L	Ø	S	E	P	E	N	G	E	V	I	R	U	S
I	E	A	D	L	S	Y	Z	Z	M	K	I	W	I	G
B	F	D	A	T	A	M	A	S	K	J	L	V	U	Y
T	Å	F	I	F	U	C	A	M	R	C	Å	N	L	Y
T	W	A	U	Z	K	N	N	H	I	O	I	T	G	M

KRYSSORDLØSNING

						D	A	T	A	M	A	S	K	
								R						
					R	O	O	T	K	I	T			
								J						
F								A		S				
I						I		N		P				
L	Ø	S	E	P	E	N	G	E	V	I	R	U	S	
L						N		R		O			A	
Ø						D				N			N	
S						E				V			D	
						M				A			K	
						M				R			A	
						I				E			S	
						N							S	
						G							E	

LÆRERVEILEDNING FOR KRYSSORDLØSNINGER

VANNRETT

1 vannrett: DATAMASK Selvreplikerende skadevare som sprer seg over nettverk uten menneskelig handling. (8 bokstaver)

3 vannrett: ROOTKIT Skjult skadevare som gjemmer seg dypt i systemkjerner for å beholde administrativ kontroll. (7 bokstaver)

7 vannrett: LØSEPENGEVIRUS Skadevare som krypterer systemlagring og krever betaling for å levere nøkkelen. (14 bokstaver)

LODDRETT

2 loddrett: TROJANER Skadelig programvare forkledd som et harmløst eller nyttig verktøyprogram. (8 bokstaver)

4 loddrett: FILLØS Skadevare som kjører direkte i RAM for å unngå oppdagelse av diskskannere. (6 bokstaver)

5 loddrett: SPIONVARE Program utformet for å i det skjulte overvåke og registrere brukeraktivitet og inndata. (9 bokstaver)

6 loddrett: INNDEMMING Begrensning av infiserte endepunkter for å hindre at trusselnyttelast sprer seg. (10 bokstaver)

8 loddrett: SANDKASSE Isolert virtuelt miljø som brukes til å analysere skadelige filer trygt. (9 bokstaver)

Fasit for kodeord og chiffer

Fasit for vokabularøvelsen med ordstokking og den hemmelige chifferutfordringen.

FASIT: BOKSTAVBLANDING

1. EJATNRRO — **TROJANER**
2. ESROPVANI — **SPIONVARE**
3. SAKASEDSN — **SANDKASSE**
4. ASKAMDAT — **DATAMASK**
5. VSRØGEPSEINLUE — **LØSEPENGEVIRUS**
6. IOKRTTO — **ROOTKIT**
7. NDIMMINGEN — **INNDEMMING**
8. LSFØLI — **FILLØS**

FASIT TIL DEN HEMMELIGE CHIFFERUTFORDRINGEN

"FINN SKADELIG NYTTELAST MED ATFERDSOVERVÅKING"

Fasit til casestudiene

A Casestudie 1: Begrensning av løsepengevirus-nyttelast i bedrifter

Løsning for læreren

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Scenarioanalyse: Et lokalt nettverk i et selskap er brutt gjennom av aktivt løsepengevirus. Viktige filservere har begynt å vise filtypene .locked. Etabler policyer for inneslutning.
- Anbefalt strategi og løsning: Koble alle berørte servere fra det lokale nettverket. Avslutt aktive administrative økter. Gjenopprett uskadde filer fra et sikkert, skrivebeskyttet frakoblet sikkerhetskopisystem.

B Casestudie 2: Minneinjeksjon av filløs skadevare

Løsning for læreren

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Scenarioanalyse: En analytiker oppdager mistenkelige skriptmønstre som kjører direkte i flyktig system-RAM ved hjelp av standard administrasjonsverktøy, men det finnes ingen skadelige filer på disken.
- Anbefalt strategi og løsning: Isoler de berørte endepunktene og ta først et minnebilde. Gå gjennom PowerShell- og WMI-logger, blokker ikke-godkjente skript med AppLocker, og start deretter på nytt for å fjerne nyttelasten.