Namn: _____ Datum: _____ Poäng: _____

Analys av skadlig kod och hotbegränsning Guide

Trojaner, ransomware, spionprogram, rootkits, virtualiseringssandlådor, inneslutning

INLÄRNINGSÖVERSIKT: ANALYS AV SKADLIG KOD

SÄKRAD
DATAKRYPTERING
256-bitars AES-standard

EFTERLEVANDE
GLOBALA STANDARDER
Ramverken GDPR och CCPA

ZERO TRUST
ÅTKOMSTPOLICY
Multifaktorautentisering

Välkommen! Det här aktivitetshäftet guidar dig genom analys och förebyggande av skadlig kod. Du utforskar spionprogram, trojaner, ransomware-nyttolaster, verktyg för reverse engineering, rootkit-beteende och inneslutningsstrategier.

KONTROLLPUNKTER I ARBETSBLADET

- [ ] **Del 1-4: Behärska cybersäkerhet och hothantering.**
- [ ] **Del 5-7: Lös korsord och ordsökare.**
- [ ] **Del 8-9: Lös fallstudier och chifferutmaning.**
- [ ] **Del 10: Gå igenom sidorna med grundläggande och avancerade vanliga frågor.**
- [ ] **Del 11: Utforska 10 intressanta fakta från verkligheten.**
- [ ] **Bonus: utmaningen Tänk snabbt.**

Öppna VPN.com:s guide om cybersäkerhet

URL: https://www.vpn.com/sv/cybersakerhet/skadlig-programvara/

Din inlärningsplan för att begränsa skadlig kod

- Skilj mellan skadlig kod av typen trojan, mask och rootkit.
- Inför körning i virtualiserad sandlåda för kodanalys.
- Utforma planer för inneslutning och sanering av aktiva utpressningsprogram.

INSTRUKTIONER: GUIDE TILL ANALYS AV SKADLIG KOD

Besvara flervalsfrågorna och sant/falskt-frågorna, fyll i luckorna med hjälp av ordbanken, matcha definitioner och lös korsordet och ordletarpusslet. Tillämpa dina kunskaper om begränsning av skadlig kod. Avsluta med bonusaktiviteten Tänk snabbt.

SKADEPROGRAMSANALYS OCH HOTBEGRÄNSNING (INTRODUKTION)

Skadlig kod som trojaner, maskar och ransomware utgör hot med stor påverkan mot slutpunkter och servrar. Säkerhetsteam analyserar skadlig kod i virtuella sandlådor och vidtar snabba nätverksisoleringsåtgärder för att begränsa spridningen av nyttolasten.

LÄS VARJE KONTROLLPUNKT NOGGRANT OCH VÄLJ ELLER SKRIV DET RÄTTA SVARET.

Kontrollpunkt 1: Utmaning med flerval

1. Vad är det avgörande kännetecknet för en trojansk häst?

- A. Den utger sig för att vara legitim programvara för att lura användare att köra den
- B. Den sprider sig automatiskt över lokala nätverkslinjer
- C. Den infekterar filer i isolerade virtuella sandlådor
- D. Den fångar upp trafik från internetleverantören

2. Vilken typ av skadlig kod krypterar filer och kräver betalning?

- A. Ransomware
- B. Spionprogram
- C. Rootkit
- D. Adware

3. Vad representerar spionprogram?

- A. Skadlig kod som är utformad för att i hemlighet övervaka användarens tangenttryckningar och webbläsaraktivitet
- B. Programkod som körs i en virtuell sandlådecontainer
- C. Uppdateringar mot skadlig kod som laddas ned från databasregister
- D. Automatisk justering av skärmens ljusstyrka

4. Varför använder utvecklare av skadlig kod rootkits?

- A. Att dölja aktiva processer och skadliga filer för operativsystemet
- B. För att öka CPU-hastigheten på slutpunkter
- C. Att säkerhetskopiera databasfiler till säkra molnvalv
- D. För att förbättra batteritiden på bärbara datorer

5. Vad innebär sandboxing vid analys av skadlig kod?

- A. Att köra misstänkta filer i ett isolerat virtuellt valv för att observera beteendet säkert
- B. Att skanna filers hashvärden mot kända hotdatabaser
- C. Att återställa databassäkerhetskopior efter ett intrång
- D. Att koppla bort lokala nätverksroutrar från offentliga linjer

Kontrollpunkt 2: Utmaning med sant eller falskt

6 Fråga 6

6. Datormaskar kräver att en användare agerar för att spridas över lokala nätverk.

- ○ Sant
- ○ Falskt

7 Fråga 7

7. Adware är alltid ofarligt och spårar inte användarbeteende eller webbhistorik.

- ○ Sant
- ○ Falskt

8 Fråga 8

8. Att återställa rena offlinebackuper gör att offren kan få tillbaka krypterade filer utan att betala lösensumman.

- ○ Sant
- ○ Falskt

9 Fråga 9

9. Signaturbaserade antivirusprogram stoppar pålitligt zero-day-skadlig kod innan det finns någon signatur för den.

- ○ Sant
- ○ Falskt

10 Fråga 10

10. Fillös skadlig kod kör skadliga skript i systemminnet och undviker att skriva filer till disken.

- ○ Sant
- ○ Falskt

Kontrollpunkt 3: Infoga nyckelbegrepp

Läs varje mening nedan och fyll i luckan med rätt term från ordbanken.

1. Skadlig kod som utger sig för att vara ett säkert verktyg är en _____ .
2. Skadliga nyttolaster som låser databassystem för att få pengar utgör _____ .
3. Tangentbordsloggare som i hemlighet registrerar lösenord utgör _____ .
4. Att gömma sig djupt i operativsystemets kärna kräver en _____ .
5. Att analysera misstänkta filer i ett isolerat valv sker i en virtuell _____ .
6. Att stoppa spridningen av aktiv skadlig kod kräver omedelbar _____ i nätverket.

ORDBANK

DATORMASK FILLÖS INDÄMNING RANSOMWARE ROOTKIT SANDLÅDA SPIONPROGRAM TROJAN

Skriv dina svar här:

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

Kontrollpunkt 4: Matchning av säkerhetsbegrepp

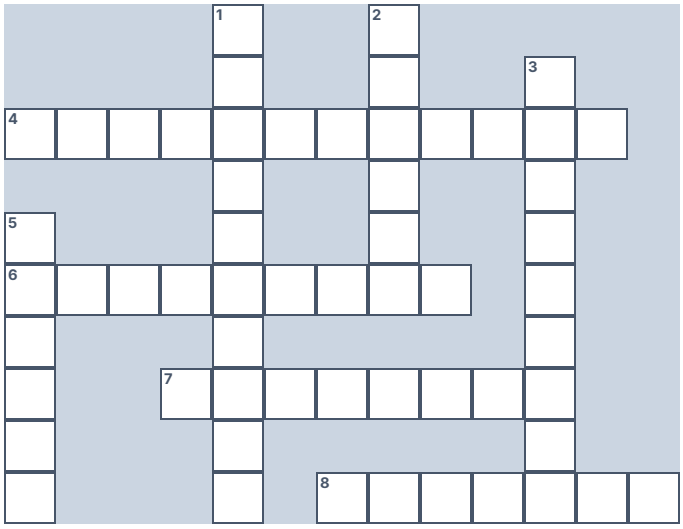
MATCHNING AV DEFINITIONER

Para ihop varje begrepp till vänster med rätt definition till höger genom att skriva motsvarande bokstav (A–H) i det ifyllbara fältet.

☐	1. TROJAN	A	Program som är utformat för att i hemlighet övervaka och registrera användaraktivitet och inmatning.
☐	2. RANSOMWARE	B	Skadlig kod som körs direkt i RAM för att undvika upptäckt av diskskannrar.
☐	3. SPIONPROGRAM	C	Att isolera infekterade slutpunkter för att förhindra att hotinnehåll sprids.
☐	4. ROOTKIT	D	Skadlig programvara som utger sig för att vara ett ofarligt eller användbart verktyg.
☐	5. SANDLÅDA	E	Självspridande skadlig kod som sprider sig över nätverk utan mänsklig handling.
☐	6. BEGRÄNSNING	F	Skadlig kod som krypterar systemets lagring och kräver betalning för att lämna ut nyckeln.
☐	7. MASK	G	Isolerad virtuell miljö som används för att analysera skadliga filer på ett säkert sätt.
☐	8. FILLÖS	H	Dold skadlig kod som gömmer sig djupt i systemkärnor för att behålla administrativ kontroll.

Kontrollpunkt 5: Korsord

Lös korsordet genom att skriva bokstäver i de aktiva vita rutorna. Siffrorna motsvarar ledtrådarna nedan.



VÅGRÄTT

4. Program som är utformat för att i hemlighet övervaka och registrera användarens aktivitet och inmatning. (12)

6. Isolering av infekterade slutpunkter för att förhindra att hotets nyttolast sprids. (9)

7. Isolerad virtuell miljö som används för att analysera skadliga filer på ett säkert sätt. (8)

8. Dold skadlig kod som gömmer sig djupt i systemkärnan för att behålla administrativ kontroll. (7)

LODRÄTT

1. Skadlig kod som krypterar systemets lagring och kräver betalning för att lämna ut nyckeln. (10)

2. Skadlig programvara som utger sig för att vara ett ofarligt eller användbart verktyg. (6)

3. Självreplikerande skadlig kod som sprids över nätverk utan mänsklig inblandning. (9)

5. Skadlig kod som körs direkt i RAM för att undgå upptäckt av diskskannrar. (6)

Kontrollpunkt 5, alternativ: Tillgängliga korsordsledtrådar

Användare av skärmläsare och tangentbord kan skriva korsordssvaren direkt i textfälten nedan.

VÅGRÄTT

4 vågrätt: Program som är utformat för att i hemlighet övervaka och registrera användarens aktivitet och inmatning. (12 bokstäver):

6 vågrätt: Isolering av infekterade slutpunkter för att förhindra att hotets nyttolast sprids. (9 bokstäver):

7 vågrätt: Isolerad virtuell miljö som används för att analysera skadliga filer på ett säkert sätt. (8 bokstäver):

8 vågrätt: Dold skadlig kod som gömmer sig djupt i systemkärnan för att behålla administrativ kontroll. (7 bokstäver):

LODRÄTT

1 lodrätt: Skadlig kod som krypterar systemets lagring och kräver betalning för att lämna ut nyckeln. (10 bokstäver):

2 lodrätt: Skadlig programvara som utger sig för att vara ett ofarligt eller användbart verktyg. (6 bokstäver):

3 lodrätt: Självreplikerande skadlig kod som sprids över nätverk utan mänsklig inblandning. (9 bokstäver):

5 lodrätt: Skadlig kod som körs direkt i RAM för att undgå upptäckt av diskskannrar. (6 bokstäver):

Kontrollpunkt 6: Dolt ordsök

Hitta de 8 viktiga ordförrådstermerna som är gömda i rutnätet nedan. Orden kan vara vågräta, lodräta eller diagonala.

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

ORDLISTA

TROJAN, RANSOMWARE, SPIONPROGRAM, ROOTKIT, SANDLÅDA, INDÄMNING, DATORMASK, FILLÖS

Kontrollpunkt 6, alternativ: Tillgänglig matchning av ordförråd

Para ihop var och en av de 8 begreppen från ordsökningen med rätt definition genom att skriva bokstaven (A–H) på den tomma raden.

ORDLISTA

- **A. TROJAN**
- **B. RANSOMWARE**
- **C. SPIONPROGRAM**
- **D. ROOTKIT**
- **E. SANDLÅDA**
- **F. INDÄMNING**
- **G. DATORMASK**
- **H. FILLÖS**

DEFINITIONER OCH MATCHNINGSFÄLT

1. Dold skadlig kod som gömmer sig djupt i systemkärnan för att behålla administrativ kontroll.
2. Isolering av infekterade slutpunkter för att förhindra att hotets nyttolast sprids.
3. Skadlig kod som körs direkt i RAM för att undgå upptäckt av diskskannrar.
4. Självreplikerande skadlig kod som sprids över nätverk utan mänsklig inblandning.
5. Skadlig kod som krypterar systemets lagring och kräver betalning för att lämna ut nyckeln.
6. Program som är utformat för att i hemlighet övervaka och registrera användarens aktivitet och inmatning.
7. Skadlig programvara som utger sig för att vara ett ofarligt eller användbart verktyg.
8. Isolerad virtuell miljö som används för att analysera skadliga filer på ett säkert sätt.

Kontrollpunkt 7: Utmaning med blandade ord

Avkoda bokstäverna nedan för att avslöja viktiga begrepp och termer inom cybersäkerhet. Skriv dina svar i rutorna.

1. **OTJANR**
2. **MPNPSRAIOG RO**
3. **DASLÅADN**
4. **RKSOAMDAT**
5. **AMEASWORR N**
6. **IOKRTTO**
7. **NINGIÄNMD**
8. **LSFÖLI**

Bonusaktivitet: Tänk snabbt

3 SVAR PER KATEGORI. DEN SOM FÖRST FYLLER I LISTAN VINNER.

1	Platser där du kan ladda ner säkra appar			
2	Enheter som kan hackas			
3	Saker du säkerhetskopierar			
4	Varningstecken i ett e-postmeddelande			
5	Tecken på att en telefon har skadlig kod			
6	Typer av skadlig kod du känner till			
7	Filtyper du ska vara försiktig med			
8	Sätt som skadlig kod tar sig in på en dator			
9	Säkra vanor du kan börja med i dag			
10	Ord som hör ihop med cybersäkerhet			
11	Saker att göra efter en dataläcka			
12	Skäl till att uppdatera programvara			
13	Djur eller figurer med namn som liknar skadlig kod			
14	Saker som skadlig kod kan stjäla			
15	Saker att göra om du har klickat på fel länk			

Kontrollpunkt 8: Fallstudier om cybersäkerhet

Tillämpa de begrepp du har lärt dig för att lösa de verkliga scenarierna nedan.

FALLSTUDIE 1: BEGRÄNSA RANSOMWARE-NYTTOLAST I FÖRETAG



Scenario: Ett lokalt nätverk (LAN) på ett företag har drabbats av pågående ransomware. Viktiga filservrar har börjat visa filändelser med .locked. Upprätta policyer för inneslutning.

Diskussionsfråga: Beskriv i detalj stegen för isolering och redogör för protokollet för dataåterställning.

FALLSTUDIE 2: FILLÖS SKADLIG KOD MED MINNESINJEKTION



Scenario: En analytiker upptäcker misstänkta skriptmönster som körs direkt i systemets flyktiga RAM med vanliga administrativa verktyg, men det finns inga skadliga filer på disken.

Diskussionsfråga: Förklara strategin för minnesanalys och ange verktyg för att blockera filfri exekvering.

Kontrollpunkt 9: Knäck chiffret

En cybersäkerhetsexpert skyddar nätverkstillgångar mot hotaktörer online. Använd bokstav-till-siffra-nyckeln nedan för att avkoda meddelandet genom att skriva de matchande bokstäverna på de tomma raderna.

KRYPTERINGSNYCKEL FÖR BOKSTAV TILL SIFFRA

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 Å=27 Ä=28 Ö=29

21	16	16	20	28	3	11		8	15	20	16	27
19	12	21	20	16	21	14	11	20	5	18	13	5	4
2	5	20	5	5	14	4	5	1	14	1	12	25	19

Avkodat meddelande:

TIPS: VARJE SIFFRA MOTSVARAR BOKSTAVENS PLATS I ALFABETET (T.EX. 1 = A, 2 = B, 29 = Ö).

Kontrollpunkt 10: Grundläggande vanliga frågor om cybersäkerhet (Del A)

Gå igenom vanliga frågor och svar om att begränsa hot på nätet.

Q1: Vad är skadlig kod?

Skadlig programvara som hotaktörer har utformat för att skada, kapa eller stjäla data från enheter och nätverk.

Q2: Vad är skillnaden mellan ett virus och en mask?

Ett virus kräver mänsklig handling (som att öppna en fil) för att spridas, medan en mask sprids automatiskt över nätverk.

Q3: Hur infekterar en trojan en dator?

Den lurar användare genom att maskera sig som ett ofarligt eller säkert program och gömmer sin skadliga nyttolast inuti.

Q4: Vad är ransomware?

En typ av skadlig kod som krypterar filer på målsystemet och kräver betalning i utbyte mot dekrypteringsnyckeln. [1]

Q5: Vad är spionprogram?

Skadlig programvara som i hemlighet registrerar användares tangenttryckningar, lösenord och surfvanor för att skicka dem till angripare.

Kontrollpunkt 10: Grundläggande vanliga frågor om cybersäkerhet (Del B)

Gå igenom vanliga frågor och svar om att begränsa hot på nätet.

Q6: Vad betyder sandboxing?

Att köra misstänkta filer i en säker, isolerad virtuell miljö för att observera deras beteende utan risk för produktionssystem.

Q7: Vad är filfri skadlig kod?

Skadlig kod som körs direkt i systemminnet (RAM) med hjälp av legitima verktyg och undviker att skriva filer till disken för att kringgå enkla skannrar.

Q8: Hur skyddar en rootkit skadlig kod?

Den döljer skadliga processer och filer, ofta genom att undergräva operativsystemets kärna, så att antivirusskannrar kan missa dem.

Q9: Vad är dynamisk beteendeövervakning?

Antivirusskanning som övervakar aktiva processer i realtid för att blockera beteenden som är typiska för skadlig kod, till exempel masskryptering av filer.

Q10: Varför är inneslutning brådskande vid incidenthantering?

Att isolera komprometterade slutpunkter förhindrar att aktiv skadlig kod sprids till andra nätverksenheter.

Kontrollpunkt 10: Avancerade vanliga frågor om säkerhet (Del C)

Utforska avancerade tekniska aspekter av säkerhetsramverk, analys av skadlig kod och dataefterlevnad.

Q1: Hur kringgår utvecklare av skadlig kod antivirusskannrar som bygger på signaturer?

De använder polymorfism, vilket ändrar filens hashvärde och kodstruktur vid varje infektion medan det skadliga beteendet förblir detsamma.

Q2: Vilken risk innebär verktyg med dubbla användningsområden i kampanjer med skadlig kod?

Angripare använder legitima administrationsverktyg (som PowerShell eller Sysinternals) för att smälta in i den vanliga nätverkstrafiken, vilket gör upptäckt svår.

Q3: Hur kör process hollowing skadlig kod?

Den startar en legitim systemprocess i vilande läge, ersätter dess minneskod med skadlig kod och återupptar körningen.

Q4: Vilken roll har en kommando- och kontrollserver (C2)?

En fjärrserver som drivs av hackare för att skicka instruktioner och nyttolaster till skadlig kod som körs på komprometterade maskiner.

Q5: Varför är det svårt att upptäcka tangentbordsloggning (keylogging)?

Enkla keyloggers förbrukar minimalt med CPU-resurser och döljer sina processer i legitima verktyg i användarutrymmet.

Kontrollpunkt 10: Avancerade vanliga frågor om säkerhet (Del D)

Utforska avancerade tekniska aspekter av säkerhetsramverk, analys av skadlig kod och dataefterlevnad.

Q6: Hur fördröjer kodobfuskering analys av skadlig kod?

Den krypterar eller ordnar om källkoden så att den blir oläslig för analytikers verktyg och säkerhetsskannrar.

Q7: Vilken funktion har en bootkit?

En rootkit som infekterar startprocessen (MBR, startsektorn eller UEFI-firmware), så att den körs innan operativsystemet laddas.

Q8: Hur identifierar heuristisk skanning zero-day-hot?

Den skannar efter misstänkta kodmönster och administrativa kommandon i stället för att leta efter en matchande databashash.

Q9: Vad är hotet med DLL-kapning?

Att tvinga ett legitimt program att läsa in ett skadligt dynamiskt länkbibliotek (DLL) genom att placera det i programmets katalogsökväg.

Q10: Hur använder automatiserade analyskedjor för skadlig kod virtualisering?

De kör misstänkta filer över flera virtuella maskiner med olika operativsystem och genererar automatiskt beteendeloggar och PCAP-filer för nätverket.

Del 11: 10 verkliga fakta och insikter om cybersäkerhet

Gå igenom verkliga fakta om säkerhetsintrång, försvarsmekanismer och efterlevnadsstandarder.

1. SÄKERHETSINSIKT

Trojanska hästar är fortfarande en vanlig infektionsmetod eftersom de gömmer skadlig kod i program som ser ofarliga ut.

2. SÄKERHETSINSIKT

FBI:s IC3 tog emot över 3 600 klagomål om ransomware under 2025, med rapporterade förluster på över 32 miljoner dollar. [3]

3. SÄKERHETSINSIKT

Maskar kan spridas snabbt över nätverk genom att utnyttja ej korrigerade protokollsårbarheter, till exempel EternalBlue i SMB.

4. SÄKERHETSINSIKT

Fillös skadlig kod är svår att upptäcka eftersom den körs i minnet via legitima verktyg och lämnar få spår på disken.

5. SÄKERHETSINSIKT

Analyssandlådor återgår vanligtvis till en ren ögonblicksbild efter varje körning så att varje test startar från ett känt tillstånd.

6. SÄKERHETSINSIKT

Rootkits kan ändra systemanrop i kärnan och rapportera falska diagnosresultat till skannrar för skadlig kod.

7. SÄKERHETSINSIKT

Kodobfuskering använder packningsverktyg för att komprimera och dölja den verkliga binära nyttolastens struktur i skadlig kod.

8. SÄKERHETSINSIKT

Polymorf skadlig kod ändrar sin kod, och därmed sin filhash, för varje ny kopia för att undgå signaturkontroller.

9. SÄKERHETSINSIKT

DLL-kapning utnyttjar konfigurationer av sökordning i vanliga operativsystem som Windows.

10. SÄKERHETSINSIKT

Säkerhetsleverantörer hittar enorma mängder nya prover av skadlig kod varje dag, så signaturer måste uppdateras hela tiden.

Tekniska referenser och källor

Studieguiden och de interaktiva pusslen är sammanställda utifrån globala standarder från NIST och OWASP samt standarder för efterlevnad av dataskydd.

VETENSKAPLIGA OCH BRANSCHRELATERADE REFERENSER

[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

Facit: Kontrollpunkt 1 – Flerval

1 Fråga 1

Rätt svar: A

ANTECKNING FÖR LÄRAREN

Vad är det avgörande kännetecknet för en trojansk häst? → Den utger sig för att vara legitim programvara för att lura användare att köra den

2 Fråga 2

Rätt svar: A

ANTECKNING FÖR LÄRAREN

Vilken typ av skadlig kod krypterar filer och kräver betalning? → Ransomware

3 Fråga 3

Rätt svar: A

ANTECKNING FÖR LÄRAREN

Vad representerar spionprogram? → Skadlig kod som är utformad för att i hemlighet övervaka användarens tangenttryckningar och webbläsaraktivitet

4 Fråga 4

Rätt svar: A

ANTECKNING FÖR LÄRAREN

Varför använder utvecklare av skadlig kod rootkits? → Att dölja aktiva processer och skadliga filer för operativsystemet

5 Fråga 5

Rätt svar: A

ANTECKNING FÖR LÄRAREN

Vad innebär sandboxing vid analys av skadlig kod? → Att köra misstänkta filer i ett isolerat virtuellt valv för att observera beteendet säkert

Facit: Kontrollpunkt 2 – Sant eller falskt

6 Fråga 6

Rätt svar: Falskt

ANTECKNING FÖR LÄRAREN

Falskt: maskar replikerar sig själva och sprids över nätverk utan någon åtgärd från användaren.

7 Fråga 7

Rätt svar: Falskt

ANTECKNING FÖR LÄRAREN

Falskt: adware är inte alltid ofarlig; mycket av den spårar surfning för att rikta annonser.

8 Fråga 8

Rätt svar: Sant

ANTECKNING FÖR LÄRAREN

Sant: rena offlinebackuper återställer krypterade filer utan betalning, även om stulna data fortfarande kan läcka.

9 Fråga 9

Rätt svar: Falskt

ANTECKNING FÖR LÄRAREN

Falskt: signaturskannrar behöver ett känt prov, så helt ny zero-day-skadlig kod kan slinka förbi dem.

10 Fråga 10

Rätt svar: Sant

ANTECKNING FÖR LÄRAREN

Fillös skadlig kod kör skadliga skript i systemminnet och undviker att skriva filer till disken.

Facit för ordförråd och bedömningsmall

Bedömningsmatris för läraren: Ge 1 poäng för varje korrekt matchning (totalt 8 poäng) och kontextbegrepp (totalt 6 poäng).

KONTROLLPUNKT 4: FACIT – MATCHNING AV BEGREPP

D 1. TROJAN	F 2. RANSOMWARE	A 3. SPIONPROGRAM	H 4. ROOTKIT
G 5. SANDLÅDA	C 6. BEGRÄNSNING	E 7. MASK	B 8. FILLÖS

KONTROLLPUNKT 3: FACIT – NYCKELBEGREPP

1 TROJAN	2 RANSOMWARE	3 SPIONPROGRAM	4 ROOTKIT
5 SANDLÅDA	6 INDÄMNING		

KONTROLLPUNKT 6, ALTERNATIV: FACIT – MATCHNING AV ORD

1 D – ROOTKIT	2 F – INDÄMNING	3 H – FILLÖS	4 G – DATORMASK
5 B – RANSOMWARE	6 C – SPIONPROGRAM	7 A – TROJAN	8 E – SANDLÅDA

DISKUSSIONSANTECKNINGAR FÖR LÄRAREN

Nyckelbegrepp:
Kontrollera att eleverna kan förklara TROJAN, RANSOMWARE och SPIONPROGRAM med egna ord och ge ett exempel på varje.

Fallstudier:
Be eleverna att stödja sina rekommendationer med fakta från arbetsbladet, inte med antaganden.

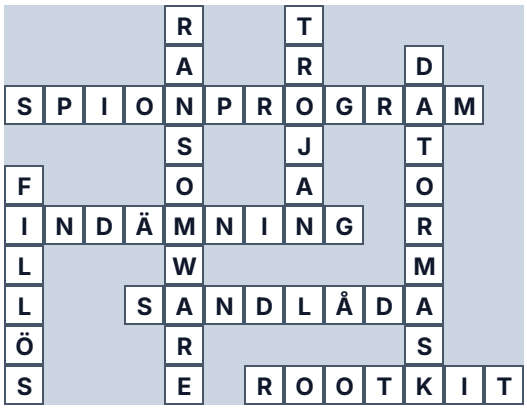
Källkritik:
Be eleverna att kontrollera minst ett påstående i arbetsbladets källor och diskutera varför siffror, priser och regler kan ändras över tid.

Facit till pussel och anteckningar för läraren

LÖSNING PÅ ORDSÖKET

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

LÖSNING PÅ KORSORDET



LÄRARHANDLEDNING MED LÖSNINGAR TILL KORSORDET

VÅGRÄTT

4 vågrätt: SPIONPROGRAM Program som är utformat för att i hemlighet övervaka och registrera användarens aktivitet och inmatning. (12 bokstäver)

6 vågrätt: INDÄMNING Isolering av infekterade slutpunkter för att förhindra att hotets nyttolast sprids. (9 bokstäver)

7 vågrätt: SANDLÅDA Isolerad virtuell miljö som används för att analysera skadliga filer på ett säkert sätt. (8 bokstäver)

8 vågrätt: ROOTKIT Dold skadlig kod som gömmer sig djupt i systemkärnan för att behålla administrativ kontroll. (7 bokstäver)

LODRÄTT

1 lodrätt: RANSOMWARE Skadlig kod som krypterar systemets lagring och kräver betalning för att lämna ut nyckeln. (10 bokstäver)

2 lodrätt: TROJAN Skadlig programvara som utger sig för att vara ett ofarligt eller användbart verktyg. (6 bokstäver)

3 lodrätt: DATORMASK Självreplikerande skadlig kod som sprids över nätverk utan mänsklig inblandning. (9 bokstäver)

5 lodrätt: FILLÖS Skadlig kod som körs direkt i RAM för att undgå upptäckt av diskskannrar. (6 bokstäver)

Facit för blandade ord och chiffer

Facit för övningen med ordvärlden och utmaningen Hemliga chiffret.

FACIT FÖR ORDBLANDNING

1. OTJANR — **TROJAN**
2. MPNPSRAIOGRO — **SPIONPROGRAM**
3. DASLÅADN — **SANDLÅDA**
4. RKSOAMDAT — **DATORMASK**
5. AMEASWORRN — **RANSOMWARE**
6. IOKRTTO — **ROOTKIT**
7. NINGIÄNMD — **INDÄMNING**
8. LSFÖLI — **FILLÖS**

NYCKEL TILL UTMANINGEN MED HEMLIGT CHIFFER

"UPPTÄCK HOT PÅ SLUTPUNKTER MED BETEENDEANALYS"

Facit till fallstudierna

A Fallstudie 1: Begränsa ransomware-nyttolast i företag

Lärarens lösning

BEDÖMNINGSRIKTLINJE

Elevernas svar bör täcka följande punkter:

- Scenarioanalys: Ett lokalt företagsnätverk har drabbats av ett aktivt ransomware-angrepp. Viktiga filservrar har börjat visa filändelsen .locked. Upprätta policyer för inneslutning.
- Rekommenderad strategi och lösning: Koppla bort alla berörda servrar från det lokala nätverket. Avsluta aktiva administrativa sessioner. Återställ ej komprometterade filer från ett säkert, skrivskyddat säkerhetskopieringssystem offline.

B Fallstudie 2: Fillös skadlig kod med minnesinjektion

Lärarens lösning

BEDÖMNINGSRIKTLINJE

Elevernas svar bör täcka följande punkter:

- Scenarioanalys: En analytiker upptäcker misstänkta skriptmönster som körs direkt i systemets flyktiga RAM med vanliga administrationsverktyg, men inga skadliga filer finns på disken.
- Rekommenderad strategi och lösning: Isolera de påverkade slutpunkterna och ta först en minnesavbild. Granska loggar från PowerShell och WMI, blockera ogodkända skript med AppLocker och starta sedan om för att rensa skadeinnehållet.