Naam: _____ Datum: _____ Score: _____

Malwareanalyse en bestrijding van dreigingen Gids

Trojans, ransomware, spyware, rootkits, virtualisatiesandboxen, insluiting

LEEROVERZICHT MALWAREANALYSE

BEVEILIGD
GEGEVENSVERSLEUTELING
256-bits AES-standaard

COMPLIANT
WERELDWIJDE NORMEN
AVG- en CCPA-kaders

ZERO-TRUST
TOEGANGSBELEID
Multifactorauthenticatie

Welkom! Dit activiteitenpakket leidt je door malware-analyse en -preventie. Je verkent spyware, trojans, ransomware-payloads, reverse-engineeringtools, rootkitgedrag en beheersingsstrategieën.

CONTROLEPUNTEN VAN HET WERKBLAD

- [ ] **Deel 1-4: Beheers cyberbeveiliging en dreigingspreventie.**
- [ ] **Deel 5-7: Los kruiswoord- en woordzoekpuzzels op.**
- [ ] **Deel 8-9: Los casestudy's en de codeopdracht op.**
- [ ] **Deel 10: Bekijk de pagina's met veelgestelde vragen (basis en gevorderd).**
- [ ] **Deel 11: Ontdek 10 interessante feiten uit de praktijk.**
- [ ] **Bonus: Snel denken-uitdaging.**

Open de VPN.com-gids over cyberbeveiliging

URL: https://www.vpn.com/nl/cyberbeveiliging/malware/

Jouw leertraject: malware beperken

- Maak onderscheid tussen trojan-, worm- en rootkit-malwaretypen.
- Voer code-analyse uit in een gevirtualiseerde sandbox.
- Ontwerp inperkings- en saneringsplannen voor actieve ransomware-payloads.

INSTRUCTIES VOOR DE GIDS MALWAREANALYSE

Beantwoord de meerkeuzevragen en de vragen waar/onwaar, vul de zinnen aan met behulp van de woordenbank, koppel de definities en los de kruiswoordpuzzel en de woordzoeker op. Pas je kennis toe op het beperken van malware. Sluit af met de bonusopdracht Snel denken.

MALWAREANALYSE EN DREIGINGSBEHEERSING (INLEIDING)

Kwaadaardige code zoals trojans, wormen en ransomware vormt een bedreiging met grote impact voor endpoints en servers. Beveiligingsteams analyseren malware in virtuele sandboxes en voeren snelle netwerkisolatie uit om de verspreiding van de payload te beperken.

LEES ELK CONTROLEPUNT ZORGVULDIG EN KIES OF SCHRIJF HET JUISTE ANTWOORD.

Controlepunt 1: Meerkeuzeopdracht

1. Wat is het kenmerkende van een Trojaans paard?

- A. Het doet zich voor als legitieme software om gebruikers te misleiden het uit te voeren
- B. Het verspreidt zich automatisch via lokale netwerkverbindingen
- C. Het infecteert bestanden in geïsoleerde virtuele sandboxes
- D. Het onderschept het verkeer van de internetprovider

2. Welk type malware versleutelt bestanden en eist betaling?

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

3. Wat staat voor spyware?

- A. Malware die is ontworpen om toetsaanslagen en browseractiviteiten van gebruikers heimelijk te bewaken
- B. Programmacode die binnen een gesandboxte virtuele container wordt uitgevoerd
- C. Anti-malwareupdates die van databaseregisters worden gedownload
- D. Automatische aanpassing van de schermhelderheid

4. Waarom gebruiken malwareontwikkelaars rootkits?

- A. Om actieve processen en schadelijke bestanden voor het besturingssysteem te verbergen
- B. Om de verwerkingssnelheid van de cpu op endpoints te verhogen
- C. Databasebestanden back-uppen naar beveiligde cloudkluizen
- D. Om de accuduur van laptops te verbeteren

5. Wat betekent sandboxing bij malware-analyse?

- A. Verdachte bestanden uitvoeren in een geïsoleerde virtuele kluis om het gedrag veilig te observeren
- B. Bestandshashes scannen op basis van databases met bekende bedreigingen
- C. Databaseback-ups herstellen na een inbraak
- D. Lokale netwerkrouters loskoppelen van openbare lijnen

Controlepunt 2: Waar-of-onwaar-opdracht

6 Vraag 6

6. Computerwormen hebben menselijke interactie van de gebruiker nodig om zich over lokale netwerken te verspreiden.

- ◯ Waar
- ◯ Onwaar

7 Vraag 7

7. Adware is altijd onschadelijk en volgt het gedrag of de browsegeschiedenis van gebruikers niet.

- ◯ Waar
- ◯ Onwaar

8 Vraag 8

8. Het herstellen van schone offline back-ups stelt slachtoffers in staat versleutelde bestanden terug te krijgen zonder het losgeld te betalen.

- ◯ Waar
- ◯ Onwaar

9 Vraag 9

9. Antivirus op basis van handtekeningen stopt zero-day-malware betrouwbaar voordat er een handtekening voor bestaat.

- ◯ Waar
- ◯ Onwaar

10 Vraag 10

10. Fileless malware voert schadelijke scripts uit in het systeemgeheugen en vermijdt het schrijven van bestanden naar schijf.

- ◯ Waar
- ◯ Onwaar

Controlepunt 3: Kernbegrippen invullen

Lees elke zin hieronder en vul de open plek in met de juiste term uit de woordenbank.

1. Malware die zich voordoet als een veilig hulpprogramma is een _____ .
2. Schadelijke payloads die databasesystemen tegen betaling vergrendelen, zijn _____ .
3. Keyloggers die heimelijk wachtwoorden vastleggen, zijn _____ .
4. Zich diep in de kernels van besturingssystemen verbergen vereist een _____ .
5. Het analyseren van verdachte bestanden in een geïsoleerde kluis gebeurt in een virtuele _____ .
6. Het stoppen van de verspreiding van actieve malwarepayloads vereist onmiddellijke _____ van het netwerk.

WOORDENBANK

FIREWALL | INDAMMING | PHISHING | RANSOMWARE | ROOTKIT | SANDBOX | SPYWARE | TROJAN

Schrijf hier je antwoorden:

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

Controlepunt 4: Beveiligingsbegrippen koppelen

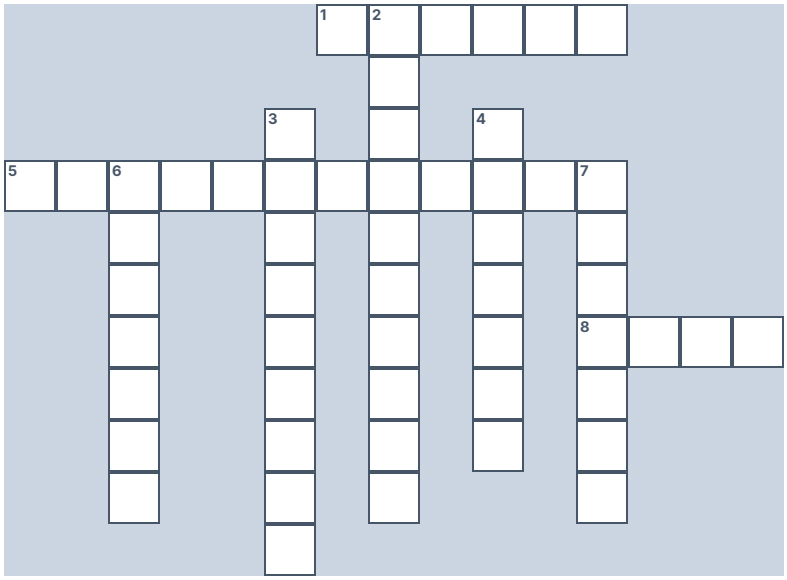
DEFINITIES KOPPELEN

Koppel elke term aan de linkerkant aan de juiste definitie aan de rechterkant door de bijbehorende letter (A-H) in het invulvak te schrijven.

☐	1. TROJAN	A	Programma dat is ontworpen om heimelijk de activiteit en invoer van gebruikers te bewaken en vast te leggen.
☐	2. RANSOMWARE	B	Malware die rechtstreeks in het RAM draait om detectie door schijfscanners te vermijden.
☐	3. SPYWARE	C	Geïnfecteerde eindpunten beperken om de verspreiding van dreigingspayloads te voorkomen.
☐	4. ROOTKIT	D	Kwaadaardige software die zich voordoet als een onschuldig of nuttig hulpprogramma.
☐	5. SANDBOX	E	Zichzelf vermenigvuldigende malware die zich zonder menselijk handelen over netwerken verspreidt.
☐	6. INDAMMING	F	Malware die systeemopslag versleutelt en betaling eist voor het leveren van de sleutel.
☐	7. WORM	G	Geïsoleerde virtuele omgeving om kwaadaardige bestanden veilig te analyseren.
☐	8. BESTANDSLOOS	H	Verborgen malware die diep in systeemkernels verstopt zit om beheerderscontrole te behouden.

Controlepunt 5: Kruiswoordpuzzel

Los de kruiswoordpuzzel op door letters in de actieve witte vakjes te typen. De nummers komen overeen met de aanwijzingen hieronder.



HORIZONTAAL

1. Kwaadaardige software die zich voordoet als een onschuldig of nuttig hulpprogramma. (6)

5. Malware die rechtstreeks in het RAM wordt uitgevoerd om detectie door schijfscanners te ontlopen. (12)

8. Zichzelf kopiërende malware die zich zonder menselijk handelen over netwerken verspreidt. (4)

VERTICAAL

2. Malware die systeemopslag versleutelt en betaling eist voor het verstrekken van de sleutel. (10)

3. Het beperken van geïnfecteerde endpoints om de verspreiding van bedreigingspayloads te voorkomen. (9)

4. Stealth-malware die zich diep in systeemkernels verbergt om beheerderscontrole te behouden. (7)

6. Geïsoleerde virtuele omgeving waarin kwaadaardige bestanden veilig worden geanalyseerd. (7)

7. Programma dat is ontworpen om heimelijk gebruikersactiviteit en invoer te volgen en vast te leggen. (7)

Controlepunt 5, alternatief: Toegankelijke kruiswoordaanwijzingen

Gebruikers van schermlezers en toetsenborden kunnen de antwoorden van de kruiswoordpuzzel rechtstreeks typen in de tekstvelden hieronder.

HORIZONTAAL

1 horizontaal: Kwaadaardige software die zich voordoet als een onschuldig of nuttig hulpprogramma. (6 letters):

5 horizontaal: Malware die rechtstreeks in het RAM wordt uitgevoerd om detectie door schijfscanners te ontlopen. (12 letters):

8 horizontaal: Zichzelf kopiërende malware die zich zonder menselijk handelen over netwerken verspreidt. (4 letters):

VERTICAAL

2 verticaal: Malware die systeemopslag versleutelt en betaling eist voor het verstrekken van de sleutel. (10 letters):

3 verticaal: Het beperken van geïnfecteerde endpoints om de verspreiding van bedreigingspayloads te voorkomen. (9 letters):

4 verticaal: Stealth-malware die zich diep in systeemkernels verbergt om beheerderscontrole te behouden. (7 letters):

6 verticaal: Geïsoleerde virtuele omgeving waarin kwaadaardige bestanden veilig worden geanalyseerd. (7 letters):

7 verticaal: Programma dat is ontworpen om heimelijk gebruikersactiviteit en invoer te volgen en vast te leggen. (7 letters):

Controlepunt 6: Verborgen woorden zoeken

Zoek de 8 belangrijkste vakwoorden die in het onderstaande rooster verborgen zijn. Woorden kunnen horizontaal, verticaal of diagonaal staan.

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

WOORDENLIJST

TROJAN RANSOMWARE SPYWARE ROOTKIT SANDBOX INDAMMING
WORM BESTANDSLOOS

Controlepunt 6, alternatief: Toegankelijk woordenschat koppelen

Koppel elk van de 8 vaktermen uit de woordzoeker aan de juiste definitie door de letter (A-H) in de lege ruimte te schrijven.

BEGRIPPEN

- **A. TROJAN**
- **B. RANSOMWARE**
- **C. SPYWARE**
- **D. ROOTKIT**
- **E. SANDBOX**
- **F. INDAMMING**
- **G. WORM**
- **H. BESTANDSLOOS**

DEFINITIES EN KOPPELVELDEN

1. Stealth-malware die zich diep in systeemkernels verbergt om beheerderscontrole te behouden.
2. Het beperken van geïnfecteerde endpoints om de verspreiding van bedreigingspayloads te voorkomen.
3. Malware die rechtstreeks in het RAM wordt uitgevoerd om detectie door schijfscanners te ontlopen.
4. Zichzelf kopiërende malware die zich zonder menselijk handelen over netwerken verspreidt.
5. Malware die systeemopslag versleutelt en betaling eist voor het verstrekken van de sleutel.
6. Programma dat is ontworpen om heimelijk gebruikersactiviteit en invoer te volgen en vast te leggen.
7. Kwaadaardige software die zich voordoet als een onschuldig of nuttig hulpprogramma.
8. Geïsoleerde virtuele omgeving waarin kwaadaardige bestanden veilig worden geanalyseerd.

Controlepunt 7: Opdracht met door elkaar gehaalde woorden

Ontcijfer de letters hieronder om kernbegrippen van cyberbeveiliging te onthullen. Schrijf je antwoorden in de invulvelden.

1. OTJANR
2. SYERAWP
3. DSBXNOA
4. MRWO
5. AMEASWORRN
6. IOKRTTO
7. MINGIANMD
8. SSAODSBNEOLT

Bonusopdracht: Snel denken

3 ANTWOORDEN PER CATEGORIE. WIE DE LIJST ALS EERSTE INVULT, WINT.

1	Plekken om veilige apps te downloaden			
2	Apparaten die gehackt kunnen worden			
3	Dingen waarvan je een back-up maakt			
4	Waarschuwingssignalen in een e-mail			
5	Tekenen dat een telefoon malware heeft			
6	Soorten malware die je kent			
7	Bestandstypen waar je voorzichtig mee moet zijn			
8	Manieren waarop malware op een pc komt			
9	Veilige gewoonten die je vandaag kunt beginnen			
10	Woorden die met cyberbeveiliging te maken hebben			
11	Dingen die je doet na een datalek			
12	Redenen om software bij te werken			
13	Dieren of personages met namen die op malware lijken			
14	Dingen die malware kan stelen			
15	Dingen die je doet als je op de verkeerde link hebt geklikt			

Controlepunt 8: Casestudy's cyberbeveiliging

Pas de concepten die je hebt geleerd toe om de onderstaande praktijkscenario's op te lossen.

CASESTUDY 1: INDAMMEN VAN EEN RANSOMWARE-PAYLOAD IN EEN ENTERPRISE-OMGEVING

👨‍💻

Scenario: Een lokaal bedrijfsnetwerk is aangetast door actieve ransomware. Belangrijke bestandsservers zijn begonnen bestandsextensies met .locked te tonen. Stel beleid voor indamming op.

Discussievraag: Beschrijf in detail de stappen voor indamming en schets het protocol voor gegevensherstel.

CASESTUDY 2: BESTANDSLOZE MALWARE MET GEHEUGENINJECTIE

👨‍💻

Scenario: Een analist detecteert verdachte scriptpatronen die rechtstreeks in het vluchtige systeemgeheugen (RAM) draaien met standaard beheerdershulpmiddelen, maar er staan geen schadelijke bestanden op de schijf.

Discussievraag: Leg de strategie voor geheugenanalyse uit en geef tools aan om fileless uitvoering te blokkeren.

Controlepunt 9: De code ontcijferen

Een cyberbeveiligingsprofessional beschermt netwerkmiddelen tegen online bedreigers. Gebruik de onderstaande letter-naar-cijfersleutel om het bericht te ontcijferen door de bijbehorende letters in de lege vakjes te schrijven.

LETTER-NAAR-CIJFER-VERSLEUTELINGSSLEUTEL

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

4	5	20	5	3	20	5	5	18

5	14	4	16	15	9	14	20	16	1	25	12	15	1	4	19	13	5	20

7	5	4	18	1	7	19	13	15	14	9	20	15	18	19				

Ontcijferd bericht:

TIP: ELK GETAL STAAT VOOR DE POSITIE VAN DIE LETTER IN HET ALFABET (BIJV. 1 = A, 2 = B, 26 = Z).

Controlepunt 10: Veelgestelde vragen over cyberbeveiliging – basis (Deel A)

Bekijk veelgestelde vragen en antwoorden over het beperken van online dreigingen.

Q1: Wat is malware?

Kwaadaardige software die door aanvallers is ontworpen om apparaten en netwerken te beschadigen, over te nemen of gegevens te stelen.

Q2: Wat is het verschil tussen een virus en een worm?

Een virus heeft menselijk handelen nodig (zoals het openen van een bestand) om zich te verspreiden, terwijl een worm zich automatisch over netwerken verspreidt.

Q3: Hoe besmet een trojaans paard een computer?

Het misleidt gebruikers door zich voor te doen als een onschuldig of veilig programma en verbergt de kwaadaardige payload erin.

Q4: Wat is ransomware?

Een soort malware die bestanden op het doelsysteem versleutelt en een financiële betaling eist in ruil voor de ontsleutelingssleutel. [1]

Q5: Wat is spyware?

Kwaadaardige software die in het geheim toetsaanslagen, wachtwoorden en surfgedrag van gebruikers registreert om die naar aanvallers te sturen.

Controlepunt 10: Veelgestelde vragen over cyberbeveiliging – basis (Deel B)

Bekijk veelgestelde vragen en antwoorden over het beperken van online dreigingen.

Q6: Wat betekent sandboxing?

Verdachte bestanden uitvoeren in een beveiligde, geïsoleerde virtuele omgeving om hun gedrag te observeren zonder risico voor productiesystemen.

Q7: Wat is fileless malware?

Malware die rechtstreeks in het systeemgeheugen (RAM) draait met behulp van legitieme hulpprogramma's en geen bestanden naar de schijf schrijft, om eenvoudige scanners te omzeilen.

Q8: Hoe beschermt een rootkit malware?

Het verbergt kwaadaardige processen en bestanden, vaak door de kernel van het besturingssysteem te ondermijnen, zodat antivirusscanners ze kunnen missen.

Q9: Wat is dynamische gedragsmonitoring?

Antivirusscans die actieve processen in realtime bewaken om handelingen te blokkeren die typisch zijn voor malware, zoals het in bulk versleutelen van bestanden.

Q10: Waarom is indamming urgent bij incidentrespons?

Het isoleren van gecompromitteerde endpoints voorkomt dat actieve malwarepayloads zich naar andere netwerkapparaten verspreiden.

Controlepunt 10: Veelgestelde vragen over beveiliging – gevorderd (Deel C)

Verken geavanceerde technische aspecten van beveiligingsframeworks, malwareanalyse en gegevenscompliance.

Q1: Hoe omzeilen malwareontwikkelaars antivirusscanners die op handtekeningen zijn gebaseerd?

Ze gebruiken polymorfisme: bij elke infectie veranderen ze de hash en codestructuur van het bestand, terwijl het kwaadaardige gedrag hetzelfde blijft.

Q2: Wat is het risico van tools voor dubbel gebruik in malwarecampagnes?

Aanvallers gebruiken legitieme beheerprogramma's (zoals PowerShell of Sysinternals) om op te gaan in het normale netwerkverkeer, waardoor detectie lastig wordt.

Q3: Hoe voert process hollowing schadelijke payloads uit?

Het start een legitiem systeemproces in een opgeschorte status, vervangt de geheugencode ervan door malware en hervat de uitvoering.

Q4: Welke rol speelt een Command-and-Control-server (C2)?

Een externe server die door hackers wordt beheerd om instructies en payloads te sturen naar malware die op gecompromitteerde machines draait.

Q5: Waarom is keylogging moeilijk te detecteren?

Eenvoudige keyloggers gebruiken minimale cpu-capaciteit en verbergen hun processen in legitieme hulpprogramma's in de gebruikersruimte.

Controlepunt 10: Veelgestelde vragen over beveiliging – gevorderd (Deel D)

Verken geavanceerde technische aspecten van beveiligingsframeworks, malwareanalyse en gegevenscompliance.

Q6: Hoe vertraagt code-obfuscatie malware-analyse?

Het versleutelt of herschikt de broncode, waardoor die onleesbaar wordt voor analysetools en beveiligingsscanners.

Q7: Wat is de functie van een bootkit?

Een rootkit die het opstartproces infecteert (de MBR, de bootsector of UEFI-firmware), zodat hij draait voordat het besturingssysteem wordt geladen.

Q8: Hoe herkent heuristisch scannen zero-day-bedreigingen?

Het scant op verdachte codepatronen en beheeropdrachten in plaats van te zoeken naar een overeenkomende hash in een database.

Q9: Wat is de dreiging van DLL-hijacking?

Een legitieme applicatie dwingen om een kwaadaardige dynamic link library (DLL) te laden door die in het mappad van de applicatie te plaatsen.

Q10: Hoe gebruiken geautomatiseerde pijplijnen voor malwareanalyse virtualisatie?

Ze voeren verdachte bestanden uit in meerdere vm's met verschillende besturingssystemen en genereren automatisch gedragslogs en PCAP-netwerkbestanden.

Deel 11: 10 cyberbeveiligingsfeiten en inzichten uit de praktijk

Bekijk feiten uit de praktijk over beveiligingsincidenten, verdedigingsmechanismen en compliancenormen.

1. BEVEILIGINGSINZICHT

Trojaanse paarden blijven een veelgebruikte besmettingsmethode, omdat ze schadelijke code verbergen in programma's die er onschuldig uitzien.

2. BEVEILIGINGSINZICHT

De IC3 van de FBI ontving in 2025 meer dan 3.600 meldingen van ransomware, met gemelde verliezen van meer dan $32 miljoen. [3]

3. BEVEILIGINGSINZICHT

Wormen kunnen zich snel over netwerken verspreiden door onbeveiligde protocolkwetsbaarheden uit te buiten, zoals EternalBlue in SMB.

4. BEVEILIGINGSINZICHT

Fileless malware is moeilijk te detecteren omdat ze via legitieme tools in het geheugen draait en weinig sporen op schijf achterlaat.

5. BEVEILIGINGSINZICHT

Analysesandboxes keren doorgaans na elke run terug naar een schone momentopname, zodat elke test vanuit een bekende toestand begint.

6. BEVEILIGINGSINZICHT

Rootkits kunnen systeemaanroepen van de kernel wijzigen en zo valse diagnoseresultaten melden aan antimalwarescanners.

7. BEVEILIGINGSINZICHT

Code-obfuscatie gebruikt packertools om de werkelijke binaire payloadstructuur van malware te comprimeren en te verbergen.

8. BEVEILIGINGSINZICHT

Polymorfe malware verandert bij elke nieuwe kopie zijn code, en dus ook zijn bestandshash, om handtekeningcontroles te ontwijken.

9. BEVEILIGINGSINZICHT

DLL-hijacking maakt misbruik van de zoekvolgorde-instellingen in standaardbesturingssystemen zoals Windows.

10. BEVEILIGINGSINZICHT

Beveiligingsleveranciers vinden dagelijks enorme aantallen nieuwe malwaresamples, dus handtekeningen moeten voortdurend worden bijgewerkt.

Technische referenties en bronnen

De studiegids en de interactieve puzzels zijn samengesteld uit wereldwijde NIST- en OWASP-standaarden en standaarden voor naleving van gegevensprivacy.

WETENSCHAPPELIJKE EN BRANCHEREFERENTIES

[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

Antwoordsleutel: Controlepunt 1 - Meerkeuze

1 Vraag 1

Juist antwoord: A

DOCENTENNOTITIE

Wat is het kenmerkende van een Trojaans paard? → Het doet zich voor als legitieme software om gebruikers te misleiden het uit te voeren

2 Vraag 2

Juist antwoord: A

DOCENTENNOTITIE

Welk type malware versleutelt bestanden en eist betaling? → Ransomware

3 Vraag 3

Juist antwoord: A

DOCENTENNOTITIE

Wat staat voor spyware? → Malware die is ontworpen om toetsaanslagen en browseractiviteiten van gebruikers heimelijk te bewaken

4 Vraag 4

Juist antwoord: A

DOCENTENNOTITIE

Waarom gebruiken malwareontwikkelaars rootkits? → Om actieve processen en schadelijke bestanden voor het besturingssysteem te verbergen

5 Vraag 5

Juist antwoord: A

DOCENTENNOTITIE

Wat betekent sandboxing bij malware-analyse? → Verdachte bestanden uitvoeren in een geïsoleerde virtuele kluis om het gedrag veilig te observeren

Antwoordsleutel: Controlepunt 2 - Waar of onwaar

6 Vraag 6

Juist antwoord: Onwaar

DOCENTENNOTITIE

Onwaar: wormen repliceren zichzelf en verspreiden zich over netwerken zonder enige handeling van de gebruiker.

7 Vraag 7

Juist antwoord: Onwaar

DOCENTENNOTITIE

Onwaar: adware is niet altijd onschuldig; veel ervan volgt het browsen om advertenties te richten.

8 Vraag 8

Juist antwoord: Waar

DOCENTENNOTITIE

Waar: schone offline back-ups herstellen versleutelde bestanden zonder te betalen, al kunnen gestolen gegevens nog steeds uitlekken.

9 Vraag 9

Juist antwoord: Onwaar

DOCENTENNOTITIE

Onwaar: handtekeningscanners hebben een bekend voorbeeld nodig, dus gloednieuwe zero-day-malware kan er doorheen glippen.

10 Vraag 10

Juist antwoord: Waar

DOCENTENNOTITIE

Fileless malware voert schadelijke scripts uit in het systeemgeheugen en vermijdt het schrijven van bestanden naar schijf.

Woordenlijstsleutels en beoordelingsrubriek

Beoordelingsrubriek voor docenten: Geef 1 punt voor elke juiste koppeling (totaal 8 punten) en elk juist contextbegrip (totaal 6 punten).

CONTROLEPUNT 4: ANTWOORDEN BEGRIPPEN KOPPELEN

D 1. TROJAN	F 2. RANSOMWARE	A 3. SPYWARE	H 4. ROOTKIT
G 5. SANDBOX	C 6. INDAMMING	E 7. WORM	B 8. BESTANDSLOOS

CONTROLEPUNT 3: ANTWOORDEN KERNBEGRIPPEN

1 TROJAN	2 RANSOMWARE	3 SPYWARE	4 ROOTKIT
5 SANDBOX	6 INDAMMING		

CONTROLEPUNT 6, ALTERNATIEF: ANTWOORDEN WOORDEN KOPPELEN

1 D – ROOTKIT	2 F – INDAMMING	3 H – BESTANDSLOOS	4 G – WORM
5 B – RANSOMWARE	6 C – SPYWARE	7 A – TROJAN	8 E – SANDBOX

DISCUSSIENOTITIES VOOR DOCENTEN

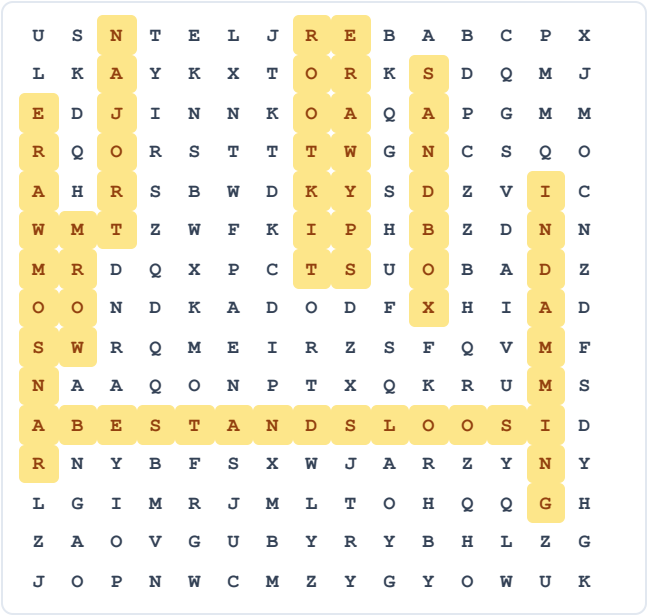
Kernbegrippen:
Controleer of leerlingen TROJAN, RANSOMWARE en SPYWARE in eigen woorden kunnen uitleggen en van elk een voorbeeld kunnen geven.

Casestudy's:
Laat leerlingen hun aanbevelingen onderbouwen met feiten uit het werkblad in plaats van met aannames.

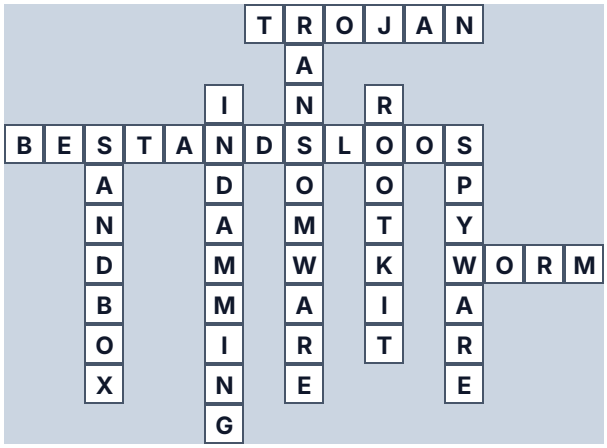
Bronnen beoordelen:
Laat leerlingen ten minste één bewering controleren aan de hand van de bronnen in het werkblad en bespreek waarom cijfers, prijzen en regels kunnen veranderen.

Puzzelsleutels en docentennotities

OPLOSSING WOORDZOEKER



OPLOSSING VAN DE KRUISWOORDPUZZEL



DOCENTENGIDS VOOR DE OPLOSSINGEN VAN DE KRUISWOORDPUZZEL

HORIZONTAAL

1 horizontaal: TROJAN Kwaadaardige software die zich voordoet als een onschuldig of nuttig hulpprogramma. (6 letters)

5 horizontaal: BESTANDSLOOS Malware die rechtstreeks in het RAM wordt uitgevoerd om detectie door schijfscanners te ontlopen. (12 letters)

8 horizontaal: WORM Zichzelf kopiërende malware die zich zonder menselijk handelen over netwerken verspreidt. (4 letters)

VERTICAAL

2 verticaal: RANSOMWARE Malware die systeemopslag versleutelt en betaling eist voor het verstrekken van de sleutel. (10 letters)

3 verticaal: INDAMMING Het beperken van geïnfecteerde endpoints om de verspreiding van bedreigingspayloads te voorkomen. (9 letters)

4 verticaal: ROOTKIT Stealth-malware die zich diep in systeemkernels verbergt om beheerderscontrole te behouden. (7 letters)

6 verticaal: SANDBOX Geïsoleerde virtuele omgeving waarin kwaadaardige bestanden veilig worden geanalyseerd. (7 letters)

7 verticaal: SPYWARE Programma dat is ontworpen om heimelijk gebruikersactiviteit en invoer te volgen en vast te leggen. (7 letters)

Sleutel voor husselwoorden en coderaadsel

Beoordelingssleutel voor de woordenschatopdracht met door elkaar gehusselde woorden en de Geheime codeopdracht.

SLEUTEL WOORDEN ORDENEN

1.	OTJANR	TROJAN	5.	AMEASWORRN	RANSOMWARE
2.	SYERAWP	SPYWARE	6.	IOKRTTO	ROOTKIT
3.	DSBXNOA	SANDBOX	7.	MINGIANMD	INDAMMING
4.	MRWO	WORM	8.	SSAODSBNEOLT	BESTANDSLOOS

SLEUTEL VOOR DE GEHEIME CODE-OPDRACHT

"DETECTEER ENDPOINTPAYLOADS MET GEDRAGSMONITORS"

Antwoordsleutel casestudy's

A Casestudy 1: Indammen van een ransomware-payload in een enterprise-omgeving

Oplossing voor docenten

BEOORDELINGSRICHTLIJN

De antwoorden van leerlingen moeten de volgende punten behandelen:

- Scenarioanalyse: Een lokaal bedrijfsnetwerk is gehackt door actieve ransomware. Belangrijke bestandsservers tonen bestandsextensies met .locked. Stel beleid op om de schade in te dammen.
- Aanbevolen strategie en oplossing: Koppel alle getroffen servers los van het lokale netwerk. Beëindig actieve beheersessies. Herstel niet-gecompromitteerde bestanden vanuit een beveiligd, tegen schrijven vergrendeld offline back-upsysteem.

B Casestudy 2: Bestandsloze malware met geheugeninjectie

Oplossing voor docenten

BEOORDELINGSRICHTLIJN

De antwoorden van leerlingen moeten de volgende punten behandelen:

- Scenarioanalyse: Een analist detecteert verdachte scriptpatronen die rechtstreeks in het vluchtige systeem-RAM worden uitgevoerd met standaard beheertools, maar er staan geen kwaadaardige bestanden op de schijf.
- Aanbevolen strategie en oplossing: Isoleer de getroffen eindpunten en maak eerst een geheugenkopie. Bekijk de PowerShell- en WMI-logs, blokkeer niet-goedgekeurde scripts met AppLocker en start vervolgens opnieuw op om de payload te wissen.