Nume: _____ **Data:** _____ **Punctaj:** _____

Analiza software-ului rău intenționat și limitarea amenințărilor Ghid

Troieni, ransomware, spyware, rootkit-uri, sandbox-uri de virtualizare, izolare

PREZENTARE GENERALĂ A ÎNVĂȚĂRII: ANALIZA SOFTWARE-ULUI RĂU INTENȚIONAT

SECURIZAT
CRIPTAREA DATELOR
Standardul AES pe 256 de biți

CONFORM
STANDARDE GLOBALE
Cadrele GDPR și CCPA

ZERO-TRUST
POLITICĂ DE ACCES
Autentificare multifactor

Bun venit! Acest pachet de activități te ghidează prin analiza și prevenirea malware-ului. Vei explora spyware-ul, troienii, sarcinile utile ale ransomware-ului, instrumentele de inginerie inversă, comportamentul rootkit-urilor și strategiile de izolare.

PUNCTE DE CONTROL ALE FIȘEI DE LUCRU

- [ ] **Partea 1-4: Stăpânește securitatea cibernetică și prevenirea amenințărilor.**
- [ ] **Partea 5-7: Rezolvă puzzle-uri de tip cuvinte încrucișate și căutare de cuvinte.**
- [ ] **Partea 8-9: Rezolvă studii de caz și provocarea cu codul cifrat.**
- [ ] **Partea 10: Parcurge paginile de întrebări frecvente de bază și avansate.**
- [ ] **Partea 11: Explorează 10 fapte interesante din lumea reală.**
- [ ] **Bonus: provocarea Gândește repede.**

Deschide Ghidul VPN.com de securitate cibernetică

URL: https://www.vpn.com/ro/securitate-cibernetica/malware/

Harta ta de învățare despre reducerea riscurilor software-ului rău intenționat

- Diferențiază tipurile de software rău intenționat: troian, vierme și rootkit.
- Implementează execuția în medii virtualizate de tip sandbox pentru analiza codului.
- Proiectează planuri de izolare și de curățare pentru payload-urile active de ransomware.

INSTRUCȚIUNI PENTRU GHIDUL DE ANALIZĂ A SOFTWARE-ULUI RĂU INTENȚIONAT

Răspunde la întrebările cu alegere multiplă și adevărat/fals, completează propozițiile cu spații libere folosind banca de cuvinte, asociază definițiile și rezolvă cuvintele încrucișate și puzzle-ul de căutare a cuvintelor. Aplică ce ai învățat despre atenuarea efectelor software-ului rău intenționat. Încheie cu activitatea bonus Gândește repede.

ANALIZA SOFTWARE-ULUI RĂU INTENȚIONAT ȘI LIMITAREA AMENINȚĂRILOR (INTRODUCERE)

Codul rău intenționat, precum troienii, viermii și ransomware-ul, reprezintă amenințări cu impact ridicat pentru stațiile de lucru și servere. Echipele de securitate analizează software-ul rău intenționat în sandbox-uri virtuale și aplică rapid măsuri de izolare a rețelei pentru a limita propagarea încărcăturii malițioase.

CITEȘTE ATENT FIECARE PUNCT DE CONTROL ȘI ALEGE SAU SCRIE RĂSPUNSUL CORECT.

Punct de control 1: Provocare cu alegere multiplă

1. Care este caracteristica definitorie a unui cal troian?

- A. Se dă drept software legitim pentru a păcăli utilizatorii să îl ruleze
- B. Se replică automat prin liniile rețelei locale
- C. Infectează fișiere din interiorul unor sandbox-uri virtuale izolate
- D. Interceptează traficul furnizorului de servicii de internet

2. Ce tip de malware criptează fișierele și cere plata unei sume?

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

3. Ce reprezintă spyware-ul?

- A. Malware conceput să monitorizeze în secret tastările utilizatorului și activitățile din browser
- B. Cod de program care rulează într-un container virtual izolat (sandbox)
- C. Actualizări anti-malware descărcate din registrele bazelor de date
- D. Ajustarea automată a luminozității ecranului

4. De ce folosesc dezvoltatorii de malware rootkit-uri?

- A. Pentru a ascunde procesele active și fișierele rău intenționate față de sistemul de operare
- B. Pentru a crește viteza de procesare a procesorului pe stațiile terminale
- C. Pentru a face copii de rezervă ale fișierelor bazei de date în seifuri cloud securizate
- D. Pentru a îmbunătăți autonomia bateriei laptopurilor

5. Ce înseamnă sandboxing în analiza malware?

- A. Executarea fișierelor suspecte într-un seif virtual izolat pentru a observa în siguranță comportamentul
- B. Scanarea hash-urilor fișierelor în baze de date cu amenințări cunoscute
- C. Restaurarea copiilor de rezervă ale bazei de date după o intruziune
- D. Deconectarea routerelor din rețeaua locală de la liniile publice

Punct de control 2: Provocare Adevărat sau Fals

6 Întrebare 6

6. Viermii informatici necesită interacțiunea unui utilizator uman pentru a se propaga în rețelele locale.

- ◯ Adevărat
- ◯ Fals

7 Întrebare 7

7. Adware-ul este întotdeauna inofensiv și nu urmărește comportamentul utilizatorului sau istoricul browserului.

- ◯ Adevărat
- ◯ Fals

8 Întrebare 8

8. Restaurarea copiilor de rezervă offline curate le permite victimelor să recupereze fișierele criptate fără a plăti răscumpărarea.

- ◯ Adevărat
- ◯ Fals

9 Întrebare 9

9. Antivirusul bazat pe semnături oprește în mod fiabil malware-ul zero-day înainte să existe vreo semnătură pentru el.

- ◯ Adevărat
- ◯ Fals

10 Întrebare 10

10. Software-ul rău intenționat fără fișiere (fileless) execută scripturi malițioase în memoria sistemului, evitând scrierea fișierelor pe disc.

- ◯ Adevărat
- ◯ Fals

Punct de control 3: Inserarea termenilor-cheie

Citește fiecare propoziție de mai jos și completează spațiul liber cu termenul corect din Banca de cuvinte.

1. Un software rău intenționat deghizat într-un utilitar sigur este un _____ .

2. Sarcinile utile rău intenționate care blochează sistemele de baze de date pentru bani reprezintă _____ .

3. Keyloggerele care înregistrează în secret parolele reprezintă _____ .

4. Ascunderea adâncă în nucleele sistemelor de operare necesită un _____ .

5. Analizarea fișierelor suspecte într-un seif izolat folosește un _____ virtual.

6. Oprirea răspândirii sarcinilor active de malware necesită o _____ imediată a rețelei.

BANCĂ DE CUVINTE DIN VOCABULAR

FĂRĂ FIȘIERE IZOLARE RANSOMWARE ROOTKIT SANDBOX SPYWARE TROJAN VIERME

Scrie răspunsurile aici:

1. **2.**

3. **4.**

5. **6.**

Punct de control 4: Asocierea conceptelor despre securitate

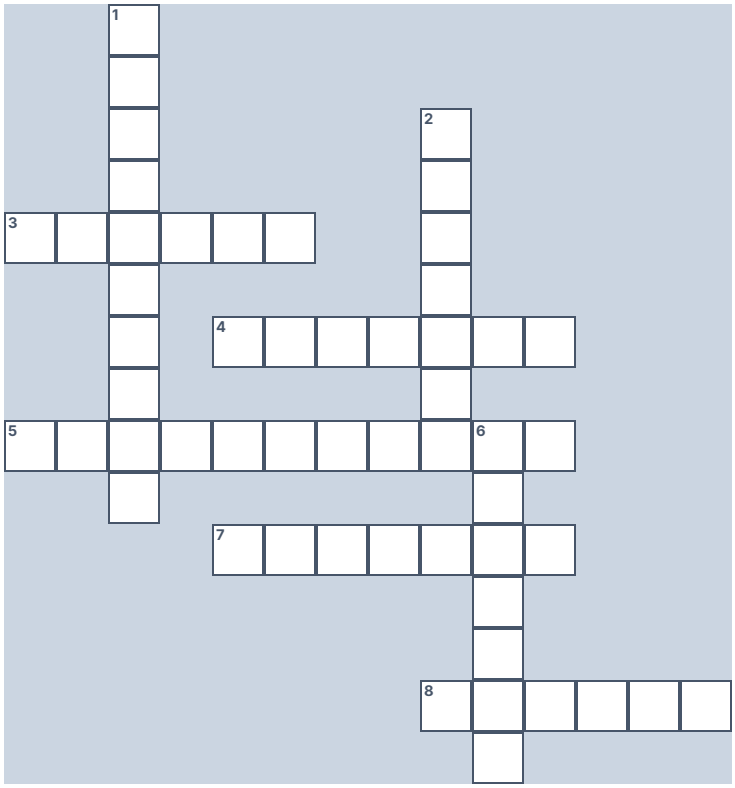
ASOCIEREA DEFINIȚIILOR

Asociază fiecare termen de vocabular din stânga cu definiția corectă din dreapta, scriind litera corespunzătoare (A-H) în câmpul de completare.

☐	1. TROIAN	A	Program conceput să monitorizeze și să înregistreze în secret activitatea și datele introduse de utilizator.
☐	2. RANSOMWARE	B	Software rău intenționat care se execută direct în RAM pentru a evita detectarea de către scanerele de disc.
☐	3. SPYWARE	C	Restricționarea punctelor finale infectate pentru a preveni răspândirea payload-urilor amenințării.
☐	4. ROOTKIT	D	Software rău intenționat deghizat într-un program utilitar inofensiv sau util.
☐	5. SANDBOX	E	Malware care se autoreplică și se propagă prin rețele fără acțiune umană.
☐	6. LIMITARE	F	Software rău intenționat care criptează spațiul de stocare al sistemului și cere o plată pentru livrarea cheii.
☐	7. WORM	G	Mediu virtual izolat folosit pentru analiza în siguranță a fișierelor rău intenționate.
☐	8. FĂRĂ FIȘIERE	H	Malware discret ascuns adânc în kernelul sistemului pentru a menține controlul administrativ.

Punct de control 5: Careu de cuvinte încrucișate

Rezolvă careul de cuvinte încrucișate tastând litere în căsuțele albe active. Numerele corespund indiciilor de mai jos.



ORIZONTAL

3. Software rău intenționat deghizat într-un program utilitar inofensiv sau util. (6)

4. Restricționarea endpoint-urilor infectate pentru a opri răspândirea sarcinilor utile ale amenințării. (7)

5. Malware care se execută direct în RAM pentru a evita detectarea de către scanerele de disc. (11)

7. Mediu virtual izolat folosit pentru analiza în siguranță a fișierelor rău intenționate. (7)

8. Malware care se autoreplică și se propagă prin rețele fără intervenție umană. (6)

VERTICAL

1. Malware care criptează stocarea sistemului și cere plată pentru livrarea cheii. (10)

2. Program conceput să monitorizeze și să înregistreze în secret activitatea și datele introduse de utilizator. (7)

6. Malware furiș, ascuns adânc în nucleul sistemului, pentru a păstra controlul administrativ. (7)

Punct de control 5, variantă alternativă: Indicii accesibile pentru cuvinte încrucișate

Utilizatorii de cititoare de ecran și de tastatură pot introduce răspunsurile la cuvintele încrucișate direct în câmpurile de text de mai jos.

ORIZONTAL

3 orizontal: Software rău intenționat deghizat într-un program utilitar inofensiv sau util. (6 litere):

4 orizontal: Restricționarea endpoint-urilor infectate pentru a opri răspândirea sarcinilor utile ale amenințării. (7 litere):

5 orizontal: Malware care se execută direct în RAM pentru a evita detectarea de către scanerele de disc. (11 litere):

7 orizontal: Mediu virtual izolat folosit pentru analiza în siguranță a fișierelor rău intenționate. (7 litere):

8 orizontal: Malware care se autoreplică și se propagă prin rețele fără intervenție umană. (6 litere):

VERTICAL

1 vertical: Malware care criptează stocarea sistemului și cere plată pentru livrarea cheii. (10 litere):

2 vertical: Program conceput să monitorizeze și să înregistreze în secret activitatea și datele introduse de utilizator. (7 litere):

6 vertical: Malware furiș, ascuns adânc în nucleul sistemului, pentru a păstra controlul administrativ. (7 litere):

Punct de control 6: Căutarea cuvintelor ascunse

Găsește în grila de mai jos cei 8 termeni cheie de vocabular ascunși. Cuvintele pot fi orizontale, verticale sau diagonale.

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

LISTĂ DE CUVINTE DIN VOCABULAR

TROJAN RANSOMWARE SPYWARE ROOTKIT SANDBOX IZOLARE VIERME FĂRĂFIȘIERE

Punct de control 6, variantă alternativă: Asocierea accesibilă a vocabularului

Asociază fiecare dintre cei 8 termeni de vocabular din Căutarea de cuvinte cu definiția corectă, scriind litera (A-H) în spațiul liber.

TERMENI DE VOCABULAR

- **A. TROJAN**
- **B. RANSOMWARE**
- **C. SPYWARE**
- **D. ROOTKIT**
- **E. SANDBOX**
- **F. IZOLARE**
- **G. VIERME**
- **H. FĂRĂFIȘIERE**

DEFINIȚII ȘI CÂMPURI DE ASOCIERE

1. Malware furiș, ascuns adânc în nucleul sistemului, pentru a păstra controlul administrativ.
2. Restricționarea endpoint-urilor infectate pentru a opri răspândirea sarcinilor utile ale amenințării.
3. Malware care se execută direct în RAM pentru a evita detectarea de către scanerele de disc.
4. Malware care se autoreplică și se propagă prin rețele fără intervenție umană.
5. Malware care criptează stocarea sistemului și cere plată pentru livrarea cheii.
6. Program conceput să monitorizeze și să înregistreze în secret activitatea și datele introduse de utilizator.
7. Software rău intenționat deghizat într-un program utilitar inofensiv sau util.
8. Mediu virtual izolat folosit pentru analiza în siguranță a fișierelor rău intenționate.

Punct de control 7: Provocare cu cuvinte amestecate

Descifrează literele de mai jos pentru a dezvălui conceptele și termenii-cheie de securitate cibernetică. Scrie răspunsurile în casetele de introducere furnizate.

1. **OTJANR**
2. **SYERAWP**
3. **DSBXNOA**
4. **EREMVI**
5. **AMEASWORRN**
6. **IOKRTTO**
7. **IRAEZLO**
8. **EȘEIRFFĂRIĂ**

Activitate bonus: Gândește repede

3 RĂSPUNSURI PE CATEGORIE. CÂȘTIGĂ CINE COMPLETEAZĂ PRIMUL LISTA.

1	Locuri de unde poți descărca aplicații sigure			
2	Dispozitive care pot fi sparte			
3	Lucruri pe care le salvezi într-o copie de rezervă			
4	Semnale de avertizare într-un e-mail			
5	Semne că un telefon are malware			
6	Tipuri de malware pe care le cunoști			
7	Tipuri de fișiere cu care trebuie să fii atent			
8	Moduri în care malware-ul ajunge pe un PC			
9	Obiceiuri sigure pe care le poți începe de azi			
10	Cuvinte legate de securitatea cibernetică			
11	Lucruri de făcut după o scurgere de date			
12	Motive pentru care ar trebui să actualizezi software-ul			
13	Animale sau personaje cu nume asemănătoare malware-ului			
14	Lucruri pe care le poate fura malware-ul			
15	Lucruri de făcut dacă ai dat clic pe link-ul greșit			

Punct de control 8: Studii de caz despre securitatea cibernetică

Aplică conceptele pe care le-ai învățat pentru a rezolva scenariile reale de mai jos.

STUDIU DE CAZ 1: LIMITAREA ÎNCĂRCĂTURII UNUI RANSOMWARE ÎNTR-O ORGANIZAȚIE

👷

Scenariu: O rețea locală corporativă a fost compromisă de un ransomware activ. Serverele de fișiere cheie au început să afișeze fișiere cu extensia .locked. Stabilește politici de izolare.

Întrebare de discuție: Detaliază pașii de izolare și descrie pe scurt protocolul de recuperare a datelor.

STUDIU DE CAZ 2: INJECTAREA ÎN MEMORIE A MALWARE-ULUI FĂRĂ FIȘIERE

👷

Scenariu: Un analist detectează tipare suspecte de scripting care se execută direct în memoria RAM volatilă a sistemului, folosind instrumente administrative standard, dar pe disc nu există fișiere rău intenționate.

Întrebare de discuție: Explică strategia de analiză a memoriei și specifică instrumente pentru blocarea execuției fără fișiere (fileless).

Punct de control 9: Descifrează codul

Un profesionist în securitate cibernetică protejează activele rețelei de actorii amenințărilor online. Folosește cheia literă–număr de mai jos pentru a descifra mesajul, scriind literele corespunzătoare în spațiile libere.

CHEIE DE CRIPTARE LITERĂ-NUMĂR

A=1 Ă=2 Â=3 B=4 C=5 D=6 E=7 F=8 G=9 H=10 I=11

Î=12 J=13 K=14 L=15 M=16 N=17 O=18 P=19 Q=20 R=21 S=22

Ș=23 T=24 Ț=25 U=26 V=27 W=28 X=29 Y=30 Z=31

6	7	24	7	5	24	7	1	31	2

1	16	7	17	11	17	25	2	21	11	15	7	19	21	11	17

5	18	16	19	18	21	24	1	16	7	17	24

Mesaj descifrat:

SFAT: FIECARE NUMĂR REPREZINTĂ POZIȚIA ACELEI LITERE ÎN ALFABET (DE EX. 1 = A, 2 = B, 31 = Z).

Punct de control 10: Întrebări frecvente de bază despre securitatea cibernetică (Partea A)

Parcurge întrebările și răspunsurile frecvente despre atenuarea amenințărilor online.

Q1: Ce este software-ul rău intenționat (malware)?

Software rău intenționat creat de actori ai amenințărilor pentru a deteriora, deturna sau fura date de pe dispozitive și din rețele.

Q2: Care este diferența dintre un virus și un vierme?

Un virus necesită o acțiune umană (precum deschiderea unui fișier) pentru a se răspândi, în timp ce un vierme se răspândește automat prin rețele.

Q3: Cum infectează un cal troian un computer?

Păcălește utilizatorii deghizându-se într-un program inofensiv sau sigur, ascunzând în interior sarcina sa rău intenționată.

Q4: Ce este ransomware-ul?

Un tip de malware care criptează fișierele de pe sistemul țintă și cere o plată financiară în schimbul cheii de decriptare. [1]

Q5: Ce este spyware-ul?

Software rău intenționat care înregistrează în secret tastele apăsate de utilizator, parolele și obiceiurile de navigare pentru a le trimite atacatorilor.

Punct de control 10: Întrebări frecvente de bază despre securitatea cibernetică (Partea B)

Parcurge întrebările și răspunsurile frecvente despre atenuarea amenințărilor online.

Q6: Ce înseamnă sandboxing?

Rularea fișierelor suspecte într-un mediu virtual securizat și izolat pentru a observa comportamentul lor fără risc pentru sistemele de producție.

Q7: Ce este software-ul rău intenționat fără fișiere (fileless malware)?

Software rău intenționat care rulează direct în memoria sistemului (RAM) folosind utilitare legitime, evitând scrierea de fișiere pe disc pentru a ocoli scanerele de bază.

Q8: Cum protejează un rootkit software-ul rău intenționat?

Ascunde procese și fișiere rău intenționate, adesea prin subminarea nucleului sistemului de operare, astfel încât scanerele antivirus pot să nu le detecteze.

Q9: Ce este monitorizarea dinamică a comportamentului?

Scanare antivirus care monitorizează procesele active în timp real pentru a bloca acțiunile tipice software-ului rău intenționat, precum criptarea în masă a fișierelor.

Q10: De ce este urgentă izolarea în timpul răspunsului la incidente?

Izolarea punctelor terminale compromise împiedică propagarea sarcinilor malware active către alte dispozitive din rețea.

Punct de control 10: Întrebări frecvente avansate despre securitate (Partea C)

Explorează aspecte tehnice avansate ale cadrelor de securitate, ale analizei software-ului rău intenționat și ale conformității datelor.

Q1: Cum ocolesc dezvoltatorii de software rău intenționat scanerele antivirus bazate pe semnături?

Folosesc polimorfismul, schimbând hash-ul și structura codului fișierului la fiecare infectare, păstrând același comportament rău intenționat.

Q2: Care este riscul instrumentelor cu dublă utilizare în campaniile de software rău intenționat?

Atacatorii folosesc instrumente administrative legitime (precum PowerShell sau Sysinternals) pentru a se camufla în traficul normal de rețea, ceea ce îngreunează detectarea.

Q3: Cum execută process hollowing sarcini utile rău intenționate?

Lansează un proces legitim de sistem în stare suspendată, îi înlocuiește codul din memorie cu malware și reia execuția.

Q4: Care este rolul unui server Command and Control (C2)?

Un server la distanță operat de hackeri pentru a trimite instrucțiuni și sarcini utile către malware-ul care rulează pe mașinile compromise.

Q5: De ce este dificil de detectat keylogging-ul?

Keyloggerele simple consumă resurse minime ale procesorului și își ascund procesele în utilitare legitime din spațiul utilizatorului.

Punct de control 10: Întrebări frecvente avansate despre securitate (Partea D)

Explorează aspecte tehnice avansate ale cadrelor de securitate, ale analizei software-ului rău intenționat și ale conformității datelor.

Q6: Cum întârzie ofuscarea codului analiza software-ului rău intenționat?

Criptează sau rearanjează codul sursă, făcându-l ilizibil pentru instrumentele analiștilor și scanerele de securitate.

Q7: Care este funcția unui bootkit?

Un rootkit care infectează procesul de pornire (MBR, sectorul de boot sau firmware-ul UEFI), astfel încât rulează înainte de încărcarea sistemului de operare.

Q8: Cum identifică scanarea euristică amenințările zero-day?

Scanează tiparele de cod suspecte și comenzile administrative, în loc să caute un hash potrivit din baza de date.

Q9: Care este amenințarea deturnării DLL?

Forțarea unei aplicații legitime să încarce o bibliotecă de legături dinamice (DLL) rău intenționată, prin plasarea acesteia în calea directorului aplicației.

Q10: Cum folosesc conductele automate de analiză a software-ului rău intenționat virtualizarea?

Rulează fișiere suspecte pe mai multe mașini virtuale cu diferite sisteme de operare, generând automat jurnale de comportament și fișiere PCAP de rețea.

Partea 11: 10 fapte și perspective din lumea reală despre securitatea cibernetică

Parcurge fapte din lumea reală despre breșele de securitate, mecanismele de apărare și standardele de conformitate.

1. INFORMAȚII DESPRE SECURITATE

Caii troieni rămân o metodă frecventă de infectare, deoarece ascund cod rău intenționat în programe care par inofensive.

2. INFORMAȚII DESPRE SECURITATE

IC3 al FBI a primit peste 3.600 de plângeri privind ransomware în 2025, cu pierderi raportate de peste 32 de milioane de dolari. [3]

3. INFORMAȚII DESPRE SECURITATE

Viermii se pot răspândi rapid prin rețele exploatând vulnerabilități de protocol nepetecite, precum EternalBlue în SMB.

4. INFORMAȚII DESPRE SECURITATE

Software-ul rău intenționat fără fișiere (fileless) este greu de detectat, deoarece rulează în memorie prin instrumente legitime și lasă puține urme pe disc.

5. INFORMAȚII DESPRE SECURITATE

Sandbox-urile de analiză revin de obicei la un snapshot curat după fiecare rulare, astfel încât fiecare test să înceapă dintr-o stare cunoscută.

6. INFORMAȚII DESPRE SECURITATE

Rootkiturile pot modifica apelurile de sistem ale kernelului, raportând rezultate de diagnostic false către scanerele anti-malware.

7. PERSPECTIVĂ ASUPRA SECURITĂȚII

Ofuscarea codului folosește utilitare de tip packer pentru a comprima și a ascunde structura reală a încărcăturii binare a malware-ului.

8. PERSPECTIVĂ ASUPRA SECURITĂȚII

Software-ul rău intenționat polimorfic își schimbă codul, și implicit hash-ul fișierului, la fiecare copie nouă pentru a evita verificările de semnături.

9. PERSPECTIVĂ ASUPRA SECURITĂȚII

Deturnarea DLL exploatează configurările ordinii de căutare din sistemele de operare obișnuite, precum Windows.

10. INFORMAȚII DESPRE SECURITATE

Furnizorii de securitate descoperă zilnic un număr uriaș de noi mostre de malware, așa că semnăturile trebuie actualizate constant.

Referințe tehnice și surse

Ghidul de studiu și puzzle-urile interactive sunt alcătuite pe baza standardelor globale NIST, OWASP și de conformitate privind confidențialitatea datelor.

REFERINȚE ACADEMICE ȘI DIN INDUSTRIE

[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

Barem: Punct de control 1 – Alegere multiplă

1 Întrebarea 1 — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Care este caracteristica definitorie a unui cal troian? → Se dă drept software legitim pentru a păcăli utilizatorii să îl ruleze

2 Întrebarea 2 — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Ce tip de malware criptează fișierele și cere plata unei sume? → Ransomware

3 Întrebarea 3 — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Ce reprezintă spyware-ul? → Malware conceput să monitorizeze în secret tastările utilizatorului și activitățile din browser

4 Întrebarea 4 — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

De ce folosesc dezvoltatorii de malware rootkit-uri? → Pentru a ascunde procesele active și fișierele rău intenționate față de sistemul de operare

5 Întrebarea 5 — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Ce înseamnă sandboxing în analiza malware? → Executarea fișierelor suspecte într-un seif virtual izolat pentru a observa în siguranță comportamentul

Barem: Punct de control 2 – Adevărat sau fals

6 Întrebarea 6

Răspuns corect: Fals

NOTĂ PENTRU PROFESOR

Fals: viermii se auto-replică și se răspândesc prin rețele fără nicio acțiune a utilizatorului.

7 Întrebarea 7

Răspuns corect: Fals

NOTĂ PENTRU PROFESOR

Fals: adware-ul nu este întotdeauna inofensiv; o mare parte din el urmărește navigarea pentru a ținti reclamele.

8 Întrebarea 8

Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

Adevărat: copiile de rezervă offline curate restaurează fișierele criptate fără plată, deși datele furate pot totuși să fie scurse.

9 Întrebarea 9

Răspuns corect: Fals

NOTĂ PENTRU PROFESOR

Fals: scanerele bazate pe semnături au nevoie de o mostră cunoscută, deci malware-ul zero-day nou-nouț poate trece de ele.

10 Întrebarea 10

Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

Software-ul rău intenționat fără fișiere (fileless) execută scripturi malițioase în memoria sistemului, evitând scrierea fișierelor pe disc.

Chei de vocabular și grilă de notare

Barem de notare pentru profesor: Acordă 1 punct pentru fiecare asociere corectă (8 puncte în total) și pentru fiecare termen din context (6 puncte în total).

PUNCT DE CONTROL 4: BAREM – ASOCIEREA CONCEPTELOR

D 1. TROIAN	F 2. RANSOMWARE	A 3. SPYWARE	H 4. ROOTKIT
G 5. SANDBOX	C 6. LIMITARE	E 7. WORM	B 8. FĂRĂ FIȘIERE

PUNCT DE CONTROL 3: BAREM – TERMENI-CHEIE

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

PUNCT DE CONTROL 6, VARIANTĂ ALTERNATIVĂ: BAREM – ASOCIEREA CUVINTELOR

1 D – ROOTKIT	2 F – IZOLARE	3 H – FĂRĂFIȘIERE	4 G – VIERME
5 B – RANSOMWARE	6 C – SPYWARE	7 A – TROJAN	8 E – SANDBOX

NOTE DE DISCUȚIE PENTRU PROFESORI

Termeni-cheie:
Verifică dacă elevii pot explica TROIAN, RANSOMWARE și SPYWARE cu propriile cuvinte și pot da câte un exemplu pentru fiecare.

Studii de caz:
Cere elevilor să își susțină recomandările cu fapte din fișă, nu cu presupuneri.

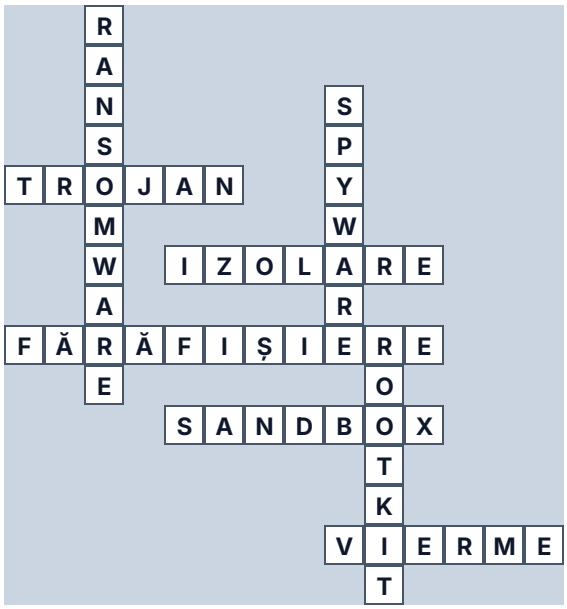
Evaluarea surselor:
Cere elevilor să verifice cel puțin o afirmație în sursele fișei și discutați de ce cifrele, prețurile și regulile se pot schimba în timp.

Chei de rezolvare ale puzzle-urilor și note pentru profesor

SOLUȚIA JOCULUI DE CĂUTARE DE CUVINTE

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

SOLUȚIA CUVINTELOR ÎNCRUCIȘATE



GHID PENTRU PROFESOR: SOLUȚIILE LA CUVINTELE ÎNCRUCIȘATE

ORIZONTAL

3 orizontal: TROJAN Software rău intenționat deghizat într-un program utilitar inofensiv sau util. (6 litere)

4 orizontal: IZOLARE Restricționarea endpoint-urilor infectate pentru a opri răspândirea sarcinilor utile ale amenințării. (7 litere)

5 orizontal: FĂRĂFIȘIERE Malware care se execută direct în RAM pentru a evita detectarea de către scanerele de disc. (11 litere)

7 orizontal: SANDBOX Mediu virtual izolat folosit pentru analiza în siguranță a fișierelor rău intenționate. (7 litere)

8 orizontal: VIERME Malware care se autoreplică și se propagă prin rețele fără intervenție umană. (6 litere)

VERTICAL

1 vertical: RANSOMWARE Malware care criptează stocarea sistemului și cere plată pentru livrarea cheii. (10 litere)

2 vertical: SPYWARE Program conceput să monitorizeze și să înregistreze în secret activitatea și datele introduse de utilizator. (7 litere)

6 vertical: ROOTKIT Malware furiș, ascuns adânc în nucleul sistemului, pentru a păstra controlul administrativ. (7 litere)

Cuvinte amestecate și barem pentru codul cifrat

Barem pentru activitatea de descifrare a cuvintelor de vocabular și pentru provocarea Codul secret.

BAREMUL PENTRU DESCIFRAREA CUVINTELOR

1. OTJANR — **TROJAN**
2. SYERAWP — **SPYWARE**
3. DSBXNOA — **SANDBOX**
4. EREMVI — **VIERME**
5. AMEASWORRN — **RANSOMWARE**
6. IOKRTTO — **ROOTKIT**
7. IRAEZLO — **IZOLARE**
8. EȘEIRFFĂRIĂ — **FĂRĂFIȘIERE**

BAREMUL PROVOCĂRII CU CODUL SECRET

"DETECTEAZĂ AMENINȚĂRILE PRIN COMPORTAMENT"

Barem pentru studiile de caz

A Studiu de caz 1: Limitarea încărcăturii unui ransomware într-o organizație

Soluția profesorului

GHID DE NOTARE

Răspunsurile elevilor ar trebui să acopere următoarele puncte:

- Analiza scenariului: O rețea locală corporativă a fost compromisă de un ransomware activ. Serverele de fișiere cheie au început să afișeze fișiere cu extensia .locked. Stabilește politicile de izolare.
- Strategie și soluție recomandate: Deconectează toate serverele afectate de la rețeaua locală. Încheie sesiunile administrative active. Restaurează fișierele necompromise dintr-un sistem securizat de copii de siguranță offline, protejat la scriere.

B Studiu de caz 2: Injectarea în memorie a malware-ului fără fișiere

Soluția profesorului

GHID DE NOTARE

Răspunsurile elevilor ar trebui să acopere următoarele puncte:

- Analiza scenariului: Un analist detectează tipare suspecte de scripting executate direct în memoria RAM volatilă a sistemului, folosind instrumente administrative standard, dar pe disc nu există fișiere malițioase.
- Strategie și soluție recomandată: Izolează punctele finale afectate și capturează mai întâi o imagine a memoriei. Examinează jurnalele PowerShell și WMI, blochează scripturile neaprobate cu AppLocker, apoi repornește pentru a elimina payload-ul.