Nome: _____ **Data:** _____ **Punteggio:** _____

Analisi del malware e mitigazione delle minacce Guida

Trojan, ransomware, spyware, rootkit, sandbox di virtualizzazione, contenimento

PANORAMICA DIDATTICA SULL'ANALISI DEL MALWARE

PROTETTO
CRITTOGRAFIA DEI DATI
Standard AES a 256 bit

CONFORME
STANDARD GLOBALI
Framework GDPR e CCPA

ZERO-TRUST
POLITICA DI ACCESSO
Autenticazione a più fattori

Benvenuto! Questo pacchetto di attività ti guida attraverso l'analisi e la prevenzione dei malware. Esplorerai spyware, trojan, payload di ransomware, strumenti di reverse engineering, il comportamento dei rootkit e le strategie di contenimento.

PUNTI DI CONTROLLO DELLA SCHEDA DI LAVORO

- [ ] **Parti 1-4: Padroneggia la sicurezza informatica e la prevenzione delle minacce.**
- [ ] **Parti 5-7: Risolvi cruciverba e parole nascoste.**
- [ ] **Parti 8-9: Risolvi casi di studio e la sfida del codice.**
- [ ] **Parte 10: Consulta le pagine delle domande frequenti di base e avanzate.**
- [ ] **Parte 11: Esplora 10 fatti interessanti dal mondo reale.**
- [ ] **Bonus: sfida Pensa veloce.**

Apri la guida alla sicurezza informatica di VPN.com

URL: https://www.vpn.com/it/sicurezza-informatica/malware/

Il tuo percorso di apprendimento sulla mitigazione del malware

- Distingui tra i tipi di malware trojan, worm e rootkit.
- Implementa l'esecuzione in virtualizzazione sandbox per l'analisi del codice.
- Progetta piani di contenimento e bonifica per i payload ransomware attivi.

ISTRUZIONI DELLA GUIDA ALL'ANALISI DEL MALWARE

Rispondi alle domande a scelta multipla e vero/falso, completa le frasi con gli spazi vuoti usando l'elenco di parole, abbina le definizioni e risolvi il cruciverba e la ricerca di parole. Applica le tue conoscenze alla mitigazione del malware. Concludi con l'attività bonus Pensa veloce.

ANALISI DEL MALWARE E CONTENIMENTO DELLE MINACCE (INTRODUZIONE)

Il codice dannoso come trojan, worm e ransomware rappresenta una minaccia ad alto impatto per endpoint e server. I team di sicurezza analizzano il malware in sandbox virtuali ed eseguono rapidi controlli di isolamento della rete per contenere la propagazione del payload.

LEGGI CON ATTENZIONE OGNI PUNTO DI CONTROLLO E SELEZIONA O SCRIVI LA RISPOSTA CORRETTA.

Punto di controllo 1: Sfida a scelta multipla

1. Qual è la caratteristica distintiva di un cavallo di Troia?

- A. Si spaccia per software legittimo per indurre gli utenti a eseguirlo
- B. Si replica automaticamente lungo le linee della rete locale
- C. Infetta i file all'interno di sandbox virtuali isolate
- D. Intercetta il traffico del provider di servizi internet

2. Quale tipo di malware cifra i file e richiede un pagamento?

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

3. Che cosa rappresenta lo spyware?

- A. Malware progettato per monitorare di nascosto la digitazione e le attività del browser dell'utente
- B. Codice di programma eseguito all'interno di un container virtuale isolato in sandbox
- C. Aggiornamenti antimalware scaricati dai registri dei database
- D. Regolazione automatica della luminosità dello schermo

4. Perché gli sviluppatori di malware usano i rootkit?

- A. Nascondere al sistema operativo i processi attivi e i file dannosi
- B. Aumentare la velocità di elaborazione della CPU sugli endpoint
- C. Per eseguire il backup dei file del database in caveau cloud sicuri
- D. Per migliorare l'autonomia della batteria dei laptop

5. Che cosa significa sandboxing nell'analisi dei malware?

- A. Eseguire file sospetti in una cassaforte virtuale isolata per osservarne il comportamento in sicurezza
- B. Confrontare gli hash dei file con database di minacce note
- C. Ripristinare i backup del database dopo un'intrusione
- D. Scollegare i router della rete locale dalle linee pubbliche

Punto di controllo 2: Sfida Vero o Falso

6 Domanda 6

6. I worm informatici richiedono l'interazione di un utente umano per propagarsi nelle reti locali.

Vero Falso

7 Domanda 7

7. L'adware è sempre innocuo e non traccia il comportamento degli utenti né la cronologia del browser.

Vero Falso

8 Domanda 8

8. Ripristinare backup offline puliti permette alle vittime di recuperare i file cifrati senza pagare il riscatto.

Vero Falso

9 Domanda 9

9. L'antivirus basato sulle firme blocca in modo affidabile il malware zero-day prima che esista una firma per esso.

Vero Falso

10 Domanda 10

10. Il malware fileless esegue script dannosi nella memoria di sistema, evitando di scrivere file sul disco.

Vero Falso

Punto di controllo 3: Inserimento dei termini chiave

Leggi ogni frase qui sotto e completa lo spazio vuoto con il termine corretto dell'elenco di parole.

1. Un malware camuffato da programma di utilità sicuro è un _____ .
2. I payload dannosi che bloccano i sistemi di database in cambio di denaro rappresentano un _____ .
3. I keylogger che registrano di nascosto le password sono _____ .
4. Nascondersi in profondità nei kernel dei sistemi operativi richiede un _____ .
5. Analizzare file sospetti in una cassaforte isolata richiede una _____ virtuale.
6. Fermare la diffusione dei payload di malware attivi richiede l'immediato _____ della rete.

BANCA DELLE PAROLE DEL VOCABOLARIO

CONTENIMENTO FILELESS RANSOMWARE ROOTKIT SANDBOX SPYWARE TROJAN WORM

Scrivi qui le tue risposte:

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

Punto di controllo 4: Abbinamento di concetti sulla sicurezza

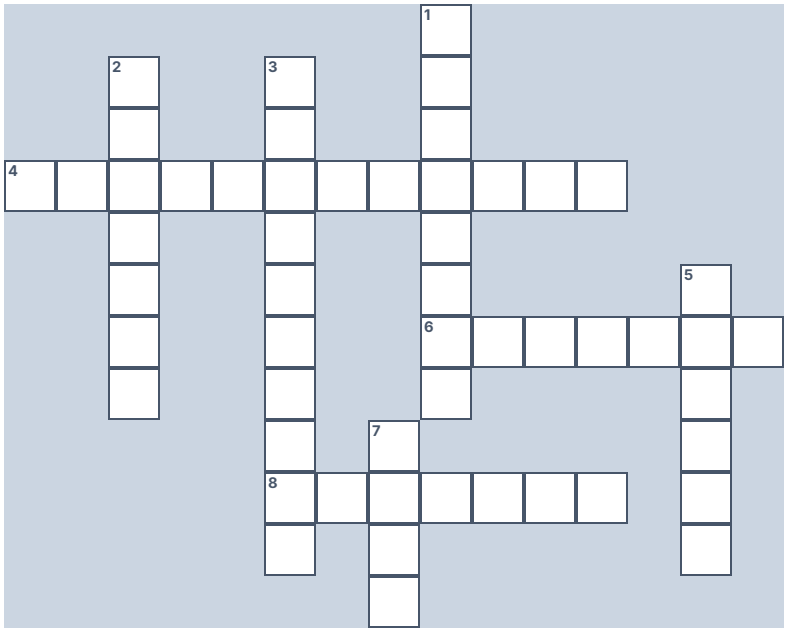
ABBINAMENTO DELLE DEFINIZIONI

Abbina ogni termine del vocabolario a sinistra alla sua definizione corretta a destra scrivendo la lettera corrispondente (A-H) nella casella compilabile.

☐	1. TROJAN	A	Programma progettato per monitorare e registrare di nascosto l'attività e gli input dell'utente.
☐	2. RANSOMWARE	B	Malware eseguito direttamente nella RAM per evitare di essere rilevato dagli scanner del disco.
☐	3. SPYWARE	C	Limitazione degli endpoint infetti per impedire la diffusione dei payload delle minacce.
☐	4. ROOTKIT	D	Software dannoso camuffato da programma di utilità innocuo o utile.
☐	5. SANDBOX	E	Malware auto-replicante che si propaga attraverso le reti senza intervento umano.
☐	6. CONTENIMENTO	F	Malware che crittografa l'archiviazione del sistema e chiede un pagamento per consegnare la chiave.
☐	7. WORM	G	Ambiente virtuale isolato usato per analizzare in sicurezza i file dannosi.
☐	8. SENZA FILE	H	Malware stealth che si nasconde in profondità nei kernel di sistema per mantenere il controllo amministrativo.

Punto di controllo 5: Cruciverba

Risolvi il cruciverba digitando le lettere nelle caselle bianche attive. I numeri corrispondono alle definizioni qui sotto.



ORIZZONTALI

4. Limitazione degli endpoint infetti per impedire la diffusione dei payload della minaccia. (12)

6. Programma progettato per monitorare e registrare di nascosto l'attività e gli input dell'utente. (7)

8. Malware furtivo nascosto in profondità nei kernel di sistema per mantenere il controllo amministrativo. (7)

VERTICALI

1. Malware che viene eseguito direttamente nella RAM per evitare il rilevamento da parte degli scanner del disco. (8)

2. Ambiente virtuale isolato usato per analizzare in sicurezza file dannosi. (7)

3. Malware che cifra l'archiviazione del sistema e chiede un pagamento per consegnare la chiave. (10)

5. Software dannoso camuffato da programma di utilità innocuo o utile. (6)

7. Malware che si replica da solo e si propaga attraverso le reti senza intervento umano. (4)

Punto di controllo 5, alternativa: Indizi accessibili del cruciverba

Gli utenti di screen reader e di tastiera possono digitare le risposte del cruciverba direttamente nei campi di testo qui sotto.

ORIZZONTALI

4 orizzontale: Limitazione degli endpoint infetti per impedire la diffusione dei payload della minaccia. (12 lettere):

6 orizzontale: Programma progettato per monitorare e registrare di nascosto l'attività e gli input dell'utente. (7 lettere):

8 orizzontale: Malware furtivo nascosto in profondità nei kernel di sistema per mantenere il controllo amministrativo. (7 lettere):

VERTICALI

1 verticale: Malware che viene eseguito direttamente nella RAM per evitare il rilevamento da parte degli scanner del disco. (8 lettere):

2 verticale: Ambiente virtuale isolato usato per analizzare in sicurezza file dannosi. (7 lettere):

3 verticale: Malware che cifra l'archiviazione del sistema e chiede un pagamento per consegnare la chiave. (10 lettere):

5 verticale: Software dannoso camuffato da programma di utilità innocuo o utile. (6 lettere):

7 verticale: Malware che si replica da solo e si propaga attraverso le reti senza intervento umano. (4 lettere):

Punto di controllo 6: Cerca la parola nascosta

Trova gli 8 termini chiave del vocabolario nascosti nella griglia qui sotto. Le parole possono essere orizzontali, verticali o diagonali.

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

ELENCO DELLE PAROLE DEL VOCABOLARIO

TROJAN RANSOMWARE SPYWARE WORM ROOTKIT FILELESS SANDBOX CONTENIMENTO

Punto di controllo 6, alternativa: Abbinamento accessibile del vocabolario

Abbina ciascuno degli 8 termini del vocabolario della Ricerca di parole alla sua definizione corretta scrivendo la lettera (A-H) nello spazio vuoto.

TERMINI DEL VOCABOLARIO
A. TROJAN
B. RANSOMWARE
C. SPYWARE
D. ROOTKIT
E. SANDBOX
F. CONTENIMENTO
G. WORM
H. FILELESS

DEFINIZIONI E CAMPI DI ABBINAMENTO

1. Malware furtivo nascosto in profondità nei kernel di sistema per mantenere il controllo amministrativo.
2. Limitazione degli endpoint infetti per impedire la diffusione dei payload della minaccia.
3. Malware che viene eseguito direttamente nella RAM per evitare il rilevamento da parte degli scanner del disco.
4. Malware che si replica da solo e si propaga attraverso le reti senza intervento umano.
5. Malware che cifra l'archiviazione del sistema e chiede un pagamento per consegnare la chiave.
6. Programma progettato per monitorare e registrare di nascosto l'attività e gli input dell'utente.
7. Software dannoso camuffato da programma di utilità innocuo o utile.
8. Ambiente virtuale isolato usato per analizzare in sicurezza file dannosi.

Punto di controllo 7: Sfida delle parole mescolate

Riordina le lettere qui sotto per scoprire concetti e termini chiave della sicurezza informatica. Scrivi le tue risposte nelle caselle fornite.

1. OTJANR
2. SYERAWP
3. DSBXNOA
4. MRWO
5. AMEASWORRN
6. IOKRTTO
7. MEECOIONTNNT
8. EILSFSEL

Attività bonus: Pensa veloce

3 RISPOSTE PER CATEGORIA. VINCE CHI COMPLETA PER PRIMO LA LISTA.

1	Luoghi in cui scaricare app sicure			
2	Dispositivi che possono essere hackerati			
3	Cose di cui fai il backup			
4	Segnali di allarme in un'email			
5	Segnali che indicano che un telefono ha un malware			
6	Tipi di malware che conosci			
7	Tipi di file con cui stare attenti			
8	Modi in cui il malware arriva su un PC			
9	Buone abitudini sicure che puoi iniziare oggi			
10	Parole legate alla sicurezza informatica			
11	Cose da fare dopo una fuga di dati			
12	Motivi per aggiornare il software			
13	Animali o personaggi con nomi simili a quelli dei malware			
14	Cose che il malware può rubare			
15	Cose da fare se hai cliccato sul link sbagliato			

Punto di controllo 8: Casi di studio sulla sicurezza informatica

Applica i concetti che hai imparato per risolvere gli scenari reali qui sotto.

CASO DI STUDIO 1: CONTENIMENTO DEL PAYLOAD DI UN RANSOMWARE AZIENDALE

👷

Scenario: La rete locale (LAN) di un'azienda è stata violata da un ransomware attivo. I file server principali hanno iniziato a mostrare file con estensione .locked. Stabilisci policy di contenimento.

Domanda di discussione: Descrivi nel dettaglio i passaggi di contenimento e illustra il protocollo di recupero dei dati.

CASO DI STUDIO 2: INIEZIONE IN MEMORIA DI MALWARE FILELESS

👷

Scenario: Un analista rileva schemi di script sospetti eseguiti direttamente nella RAM volatile del sistema tramite normali strumenti di amministrazione, ma sul disco non esiste alcun file dannoso.

Domanda di discussione: Spiega la strategia di analisi della memoria e indica gli strumenti per bloccare l'esecuzione fileless.

Punto di controllo 9: Decifrare il codice

Un professionista della sicurezza informatica protegge le risorse di rete dagli attori delle minacce online. Usa la chiave lettera-numero qui sotto per decifrare il messaggio scrivendo le lettere corrispondenti negli spazi vuoti.

CHIAVE DI CIFRATURA LETTERA-NUMERO

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

18 9 12 5 22 1 9 16 1 25 12 15 1 4 3 15 14

13 15 14 9 20 15 18

3 15 13 16 15 18 20 1 13 5 14 20 1 12 9

Messaggio decifrato:

SUGGERIMENTO: OGNI NUMERO RAPPRESENTA LA POSIZIONE DI QUELLA LETTERA NELL'ALFABETO (AD ES. 1 = A, 2 = B, 26 = Z).

Punto di controllo 10: Domande frequenti di base sulla sicurezza informatica (Parte A)

Rivedi domande e risposte comuni sulla mitigazione delle minacce online.

Q1: Che cos'è il malware?

Software dannoso progettato dagli attori delle minacce per danneggiare, dirottare o rubare dati da dispositivi e reti.

Q2: Qual è la differenza tra un virus e un worm?

Un virus richiede un'azione umana (come aprire un file) per diffondersi, mentre un worm si diffonde automaticamente attraverso le reti.

Q3: Come infetta un computer un trojan?

Inganna gli utenti fingendosi un programma innocuo o sicuro e nascondendo al suo interno il proprio payload dannoso.

Q4: Cos'è il ransomware?

Un tipo di malware che cifra i file del sistema bersaglio, chiedendo un pagamento in cambio della chiave di decifratura. [1]

Q5: Cos'è lo spyware?

Software dannoso che registra di nascosto i tasti premuti dall'utente, le password e le abitudini di navigazione per inviarli agli attaccanti.

Punto di controllo 10: Domande frequenti di base sulla sicurezza informatica (Parte B)

Rivedi domande e risposte comuni sulla mitigazione delle minacce online.

Q6: Cosa significa sandboxing?

Eseguire file sospetti in un ambiente virtuale sicuro e isolato per osservarne il comportamento senza rischi per i sistemi di produzione.

Q7: Cos'è il malware fileless?

Malware che viene eseguito direttamente nella memoria di sistema (RAM) usando utilità legittime, evitando di scrivere file sul disco per aggirare gli scanner di base.

Q8: Come protegge il malware un rootkit?

Nasconde processi e file dannosi, spesso sovvertendo il kernel del sistema operativo, quindi gli scanner antivirus possono non rilevarli.

Q9: Cos'è il monitoraggio dinamico del comportamento?

Scansione antivirus che monitora in tempo reale i processi attivi per bloccare azioni tipiche del malware, come la crittografia di massa dei file.

Q10: Perché il contenimento è urgente durante la risposta agli incidenti?

Isolare gli endpoint compromessi impedisce ai payload di malware attivi di propagarsi ad altri dispositivi di rete.

Punto di controllo 10: Domande frequenti avanzate sulla sicurezza (Parte C)

Esplora gli aspetti tecnici avanzati dei framework di sicurezza, dell'analisi del malware e della conformità dei dati.

Q1: Come aggirano gli sviluppatori di malware gli scanner antivirus basati su firme?

Usano il polimorfismo, cambiando l'hash e la struttura del codice del file a ogni infezione mantenendo invariato il comportamento dannoso.

Q2: Qual è il rischio degli strumenti a duplice uso nelle campagne di malware?

Gli aggressori usano strumenti amministrativi legittimi (come PowerShell o Sysinternals) per mimetizzarsi nel normale traffico di rete, rendendo difficile il rilevamento.

Q3: Come esegue payload dannosi il process hollowing?

Avvia un processo di sistema legittimo in stato sospeso, sostituisce il suo codice in memoria con il malware e riprende l'esecuzione.

Q4: Qual è il ruolo di un server di comando e controllo (C2)?

Un server remoto gestito da hacker per inviare istruzioni e payload al malware in esecuzione su macchine compromesse.

Q5: Perché il keylogging è difficile da individuare?

I keylogger di base consumano pochissime risorse della CPU e nascondono i propri processi dentro utility legittime dello spazio utente.

Punto di controllo 10: Domande frequenti avanzate sulla sicurezza (Parte D)

Esplora gli aspetti tecnici avanzati dei framework di sicurezza, dell'analisi del malware e della conformità dei dati.

Q6: Come ritarda l'analisi del malware l'offuscamento del codice?

Cifra o riorganizza il codice sorgente, rendendolo illeggibile per gli strumenti degli analisti e per gli scanner di sicurezza.

Q7: Qual è la funzione di un bootkit?

Un rootkit che infetta il processo di avvio (MBR, settore di avvio o firmware UEFI), così viene eseguito prima del caricamento del sistema operativo.

Q8: Come individua le minacce zero-day la scansione euristica?

Cerca schemi di codice sospetti e comandi amministrativi anziché cercare un hash corrispondente in un database.

Q9: Qual è la minaccia del DLL hijacking?

Costringere un'applicazione legittima a caricare una libreria a collegamento dinamico (DLL) dannosa collocandola nel percorso della directory dell'applicazione.

Q10: Come usano la virtualizzazione le pipeline di analisi automatica del malware?

Eseguono file sospetti su più VM di sistemi operativi diversi, generando automaticamente log di comportamento e file PCAP di rete.

Parte 11: 10 fatti e spunti reali sulla sicurezza informatica

Rivedi fatti reali su violazioni della sicurezza, meccanismi di difesa e standard di conformità.

1. APPROFONDIMENTO SULLA SICUREZZA

I trojan restano un metodo di infezione diffuso perché nascondono codice dannoso all'interno di programmi che sembrano innocui.

2. APPROFONDIMENTO SULLA SICUREZZA

L'IC3 dell'FBI ha ricevuto oltre 3.600 denunce di ransomware nel 2025, con perdite segnalate superiori a 32 milioni di $. [3]

3. APPROFONDIMENTO SULLA SICUREZZA

I worm possono diffondersi rapidamente attraverso le reti sfruttando vulnerabilità non corrette dei protocolli, come EternalBlue in SMB.

4. APPROFONDIMENTO SULLA SICUREZZA

Il malware fileless è difficile da rilevare perché viene eseguito in memoria tramite strumenti legittimi e lascia poche tracce sul disco.

5. APPROFONDIMENTO SULLA SICUREZZA

Le sandbox di analisi di solito ripristinano uno snapshot pulito dopo ogni esecuzione, così ogni test parte da uno stato noto.

6. APPROFONDIMENTO SULLA SICUREZZA

I rootkit possono modificare le chiamate di sistema del kernel, riportando falsi risultati diagnostici agli scanner anti-malware.

7. APPROFONDIMENTO SULLA SICUREZZA

L'offuscamento del codice usa utilità di packing per comprimere e nascondere la vera struttura del payload binario del malware.

8. APPROFONDIMENTO SULLA SICUREZZA

Il malware polimorfico cambia il proprio codice, e quindi il proprio hash del file, a ogni nuova copia per eludere i controlli basati sulle firme.

9. APPROFONDIMENTO SULLA SICUREZZA

Il DLL hijacking sfrutta le configurazioni dell'ordine di ricerca nei sistemi operativi comuni come Windows.

10. APPROFONDIMENTO SULLA SICUREZZA

I fornitori di sicurezza individuano ogni giorno un numero enorme di nuovi campioni di malware, quindi le firme richiedono aggiornamenti costanti.

Riferimenti tecnici e fonti

La guida di studio e i puzzle interattivi sono compilati a partire dagli standard globali NIST, OWASP e di conformità alla privacy dei dati.

RIFERIMENTI ACCADEMICI E DI SETTORE

[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

Soluzioni: Punto di controllo 1 – Scelta multipla

1 Domanda 1

Risposta corretta: A

NOTA DIDATTICA

Qual è la caratteristica distintiva di un cavallo di Troia? → Si spaccia per software legittimo per indurre gli utenti a eseguirlo

2 Domanda 2

Risposta corretta: A

NOTA DIDATTICA

Quale tipo di malware cifra i file e richiede un pagamento? → Ransomware

3 Domanda 3

Risposta corretta: A

NOTA DIDATTICA

Che cosa rappresenta lo spyware? → Malware progettato per monitorare di nascosto la digitazione e le attività del browser dell'utente

4 Domanda 4

Risposta corretta: A

NOTA DIDATTICA

Perché gli sviluppatori di malware usano i rootkit? → Nascondere al sistema operativo i processi attivi e i file dannosi

5 Domanda 5

Risposta corretta: A

NOTA DIDATTICA

Che cosa significa sandboxing nell'analisi dei malware? → Eseguire file sospetti in una cassaforte virtuale isolata per osservarne il comportamento in sicurezza

Soluzioni: Punto di controllo 2 – Vero o falso

6 **Domanda 6** — **Risposta corretta: Falso**

NOTA DIDATTICA

Falso: i worm si replicano da soli e si diffondono attraverso le reti senza alcuna azione dell'utente.

7 **Domanda 7** — **Risposta corretta: Falso**

NOTA DIDATTICA

Falso: l'adware non è sempre innocuo; molti tracciano la navigazione per mirare gli annunci.

8 **Domanda 8** — **Risposta corretta: Vero**

NOTA DIDATTICA

Vero: i backup offline puliti ripristinano i file cifrati senza pagare, anche se i dati rubati potrebbero comunque essere diffusi.

9 **Domanda 9** — **Risposta corretta: Falso**

NOTA DIDATTICA

Falso: gli scanner basati sulle firme hanno bisogno di un campione noto, quindi il malware zero-day nuovo di zecca può sfuggire loro.

10 **Domanda 10** — **Risposta corretta: Vero**

NOTA DIDATTICA

Il malware fileless esegue script dannosi nella memoria di sistema, evitando di scrivere file sul disco.

Chiavi del vocabolario e griglia di valutazione

Griglia di valutazione per l'insegnante: assegna 1 punto per ogni abbinamento corretto (8 punti in totale) e per ogni termine di contesto (6 punti in totale).

PUNTO DI CONTROLLO 4: SOLUZIONI ABBINAMENTO DI CONCETTI

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

PUNTO DI CONTROLLO 3: SOLUZIONI TERMINI CHIAVE

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

PUNTO DI CONTROLLO 6, ALTERNATIVA: SOLUZIONI ABBINAMENTO DI PAROLE

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

NOTE DI DISCUSSIONE PER GLI INSEGNANTI

Termini chiave:
Verifica che gli studenti sappiano spiegare TROJAN, RANSOMWARE e SPYWARE con parole proprie e fare un esempio per ciascuno.

Casi di studio:
Chiedi agli studenti di motivare le loro raccomandazioni con fatti tratti dalla scheda anziché con supposizioni.

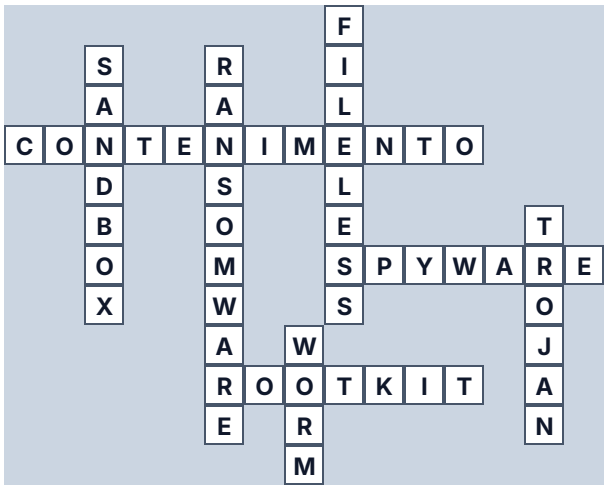
Valutazione delle fonti:
Fai verificare almeno un'affermazione con le fonti della scheda e discuti perché cifre, prezzi e regole possono cambiare nel tempo.

Soluzioni dei rompicapi e note per l'insegnante

SOLUZIONE DELLA RICERCA DELLE PAROLE

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

SOLUZIONE DEL CRUCIVERBA



GUIDA PER L'INSEGNANTE: SOLUZIONI DEL CRUCIVERBA

ORIZZONTALI

4 orizzontale: CONTENIMENTO Limitazione degli endpoint infetti per impedire la diffusione dei payload della minaccia. (12 lettere)

6 orizzontale: SPYWARE Programma progettato per monitorare e registrare di nascosto l'attività e gli input dell'utente. (7 lettere)

8 orizzontale: ROOTKIT Malware furtivo nascosto in profondità nei kernel di sistema per mantenere il controllo amministrativo. (7 lettere)

VERTICALI

1 verticale: FILELESS Malware che viene eseguito direttamente nella RAM per evitare il rilevamento da parte degli scanner del disco. (8 lettere)

2 verticale: SANDBOX Ambiente virtuale isolato usato per analizzare in sicurezza file dannosi. (7 lettere)

3 verticale: RANSOMWARE Malware che cifra l'archiviazione del sistema e chiede un pagamento per consegnare la chiave. (10 lettere)

5 verticale: TROJAN Software dannoso camuffato da programma di utilità innocuo o utile. (6 lettere)

7 verticale: WORM Malware che si replica da solo e si propaga attraverso le reti senza intervento umano. (4 lettere)

Soluzioni delle parole mescolate e del codice cifrato

Chiave di valutazione per l'attività di riordino delle parole del vocabolario e per la sfida del codice segreto.

CHIAVE DELLE PAROLE DA RIORDINARE

1. OTJANR — **TROJAN**
2. SYERAWP — **SPYWARE**
3. DSBXNOA — **SANDBOX**
4. MRWO — **WORM**
5. AMEASWORRN — **RANSOMWARE**
6. IOKRTTO — **ROOTKIT**
7. MEECOIONTNNT — **CONTENIMENTO**
8. EILSFSEL — **FILELESS**

CHIAVE DELLA SFIDA DEL CODICE SEGRETO

"RILEVA I PAYLOAD CON MONITOR COMPORTAMENTALI"

Soluzioni dei casi di studio

A Caso di studio 1: contenimento del payload di un ransomware aziendale

Soluzione per l'insegnante

LINEA GUIDA DI VALUTAZIONE

Le risposte degli studenti dovrebbero coprire i seguenti punti:

- Analisi dello scenario: una rete locale aziendale è stata violata da un ransomware attivo. I file server principali hanno iniziato a mostrare file con estensione .locked. Stabilisci le politiche di contenimento.
- Strategia e soluzione consigliate: scollegare tutti i server interessati dalla rete locale. Terminare le sessioni amministrative attive. Ripristinare i file non compromessi da un sistema di backup offline sicuro con protezione dalla scrittura.

B Caso di studio 2: Iniezione in memoria di malware fileless

Soluzione per l'insegnante

LINEA GUIDA DI VALUTAZIONE

Le risposte degli studenti dovrebbero coprire i seguenti punti:

- Analisi dello scenario: un analista rileva schemi di scripting sospetti eseguiti direttamente nella RAM volatile del sistema tramite strumenti amministrativi standard, ma sul disco non esiste alcun file dannoso.
- Strategia e soluzione consigliate: Isola gli endpoint interessati e acquisisci prima un'immagine della memoria. Esamina i log di PowerShell e WMI, blocca gli script non approvati con AppLocker, quindi riavvia per eliminare il payload.