Emri: _____ Data: _____ Pikët: _____

Analiza e malware-it dhe zbutja e kërcënimeve Udhëzues

Trojanë, ransomware, spyware, rootkit-e, sandbox-e virtualizimi, përmbajtje

PËRMBLEDHJE MËSIMORE PËR ANALIZËN E MALWARE-IT

I SIGURUAR
ENKRIPTIMI I TË DHËNAVE
Standardi AES 256-bit

I PËRPUTHSHËM
STANDARDET GLOBALE
Kornizat GDPR dhe CCPA

ZERO-TRUST
POLITIKA E QASJES
Autentikim me shumë faktorë

Mirë se vjen! Kjo paketë aktivitetesh të udhëheq përmes analizës dhe parandalimit të malware-it. Do të eksplorosh spyware-in, trojanët, ngarkesat e ransomware-it, mjetet e inxhinierisë së kundërt, sjelljen e rootkit-it dhe strategjitë e përmbajtjes.

PIKAT E KONTROLLIT TË FLETËS SË PUNËS

- [ ] **Pjesët 1-4: Zotëro sigurinë kibernetike dhe parandalimin e kërcënimeve.**
- [ ] **Pjesët 5-7: Zgjidh fjalëkryqe dhe enigma me kërkim fjalësh.**
- [ ] **Pjesët 8-9: Zgjidh studime rasti dhe sfidën e kodit.**
- [ ] **Pjesa 10: Shqyrto faqet e pyetjeve të shpeshta bazë dhe të avancuara.**
- [ ] **Pjesa 11: Eksploro 10 fakte interesante nga bota reale.**
- [ ] **Bonus: sfida Mendo shpejt.**

Hap Udhëzuesin VPN.com për sigurinë kibernetike

URL: https://www.vpn.com/sq/siguria-kibernetike/malware/

Udhërrëfyesi yt mësimor për zbutjen e malware-it

- Dallo mes llojeve të malware-it Trojan, worm dhe rootkit.
- Zbato ekzekutim në virtualizim sandbox për analizën e kodit.
- Harto plane izolimi dhe pastrimi për ngarkesat aktive të ransomware-it.

UDHËZIME PËR UDHËZUESIN E ANALIZËS SË MALWARE-IT

Përgjigju pyetjeve me zgjedhje të shumëfishtë dhe pyetjeve E vërtetë/E gabuar, plotëso fjalitë me vende bosh duke përdorur bankën e fjalëve, përputh përkufizimet dhe zgjidh fjalëkryqin dhe enigmën e kërkimit të fjalëve. Zbato njohuritë e tua për zbutjen e malware-it. Përfundo me aktivitetin bonus Mendo shpejt.

ANALIZA E MALWARE-IT DHE PËRMBAJTJA E KËRCËNIMEVE (HYRJE)

Kodi keqdashës si Trojanët, krimbat (worms) dhe ransomware përbën kërcënime me ndikim të lartë për pikat fundore dhe serverët. Ekipet e sigurisë e analizojnë malware-in brenda sandbox-eve virtuale dhe zbatojnë kontrolle të shpejta të izolimit të rrjetit për të frenuar përhapjen e ngarkesës.

LEXO ÇDO PIKË KONTROLLI ME KUJDES DHE ZGJIDH OSE SHKRUAJ PËRGJIGJEN E SAKTË.

Pika e kontrollit 1: Sfida me zgjedhje të shumëfishtë

1 **1. Cila është karakteristika përcaktuese e një Trojan horse?**

- A. Maskohet si softuer legjitim për t'i mashtruar përdoruesit ta ekzekutojnë
- B. Përhapet automatikisht nëpër linjat e rrjetit lokal
- C. Infekton skedarët brenda sandbox-eve virtuale të izoluara
- D. Përgjon trafikun e ofruesit të shërbimit të internetit

2 **2. Cili lloj malware-i enkripton skedarët dhe kërkon pagesë?**

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

3 **3. Çfarë përfaqëson spyware-i?**

- A. Malware i dizajnuar për të monitoruar fshehurazi shtypjet e tastierës dhe aktivitetet e shfletuesit të përdoruesit
- B. Kodi i programit që ekzekutohet brenda një kontejneri virtual sandbox
- C. Përditësimet anti-malware të shkarkuara nga regjistrat e bazave të të dhënave
- D. Rregullim automatik i ndriçimit të ekranit

4 **4. Pse përdorin zhvilluesit e malware-it rootkit-e?**

- A. Për të fshehur proceset aktive dhe skedarët keqdashës nga sistemi operativ
- B. Për të rritur shpejtësinë e përpunimit të CPU-së në pikat fundore
- C. Për të bërë kopje rezervë të skedarëve të bazës së të dhënave në kasaforta të sigurta cloud
- D. Për të përmirësuar jetëgjatësinë e baterisë në laptopë

5 **5. Çfarë do të thotë sandboxing në analizën e malware-it?**

- A. Ekzekutimi i skedarëve të dyshimtë në një kasafortë virtuale të izoluar për të vëzhguar sjelljen në mënyrë të sigurt
- B. Skanimi i hash-eve të skedarëve me bazat e të dhënave të kërcënimeve të njohura
- C. Rikthimi i kopjeve rezervë të bazës së të dhënave pas një ndërhyrjeje
- D. Shkëputja e router-ave të rrjetit lokal nga linjat publike

Pika e kontrollit 2: Sfida: E vërtetë ose e gabuar

6 Pyetja 6

6. Krimbat kompjuterikë kërkojnë ndërveprim të përdoruesit njeri për t'u përhapur nëpër rrjetet lokale.

- ○ E vërtetë
- ○ E gabuar

7 Pyetja 7

7. Adware është gjithmonë i padëmshëm dhe nuk gjurmon sjelljen e përdoruesit ose historikun e shfletuesit.

- ○ E vërtetë
- ○ E gabuar

8 Pyetja 8

8. Rikthimi i kopjeve rezervë offline të pastra u lejon viktimave t'i rikuperojnë skedarët e enkriptuar pa paguar shpërblimin.

- ○ E vërtetë
- ○ E gabuar

9 Pyetja 9

9. Antivirusi i bazuar në nënshkrime i ndalon me besueshmëri malware-et zero-day para se të ekzistojë ndonjë nënshkrim për to.

- ○ E vërtetë
- ○ E gabuar

10 Pyetja 10

10. Malware-i pa skedarë ekzekuton skripte keqdashëse në memorien e sistemit, duke shmangur shkrimin e skedarëve në disk.

- ○ E vërtetë
- ○ E gabuar

Pika e kontrollit 3: Futja e termave kryesorë

Lexo secilën fjali më poshtë dhe plotëso vendin bosh me termin e saktë nga Banka e Fjalëve.

1. Malware i maskuar si program i sigurt shërbimi është një _____ .

2. Ngarkesat keqdashëse që bllokojnë sistemet e bazave të të dhënave për para përfaqësojnë _____ .

3. Keylogger-ët që regjistrojnë fshehurazi fjalëkalimet përfaqësojnë _____ .

4. Fshehja thellë brenda berthamave të sistemeve operative kërkon një _____ .

5. Analizimi i skedarëve të dyshimtë në një kasafortë të izoluar përdor një _____ virtual.

6. Ndalimi i përhapjes së ngarkesave aktive të malware-it kërkon _____ të menjëhershëm të rrjetit.

BANKA E FJALËVE TË LEKSIKUT

FIREWALL IZOLIM PHISHING RANSOMWARE ROOTKIT SANDBOX SPYWARE TROJAN

Shkruaj përgjigjet e tua këtu:

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

Pika e kontrollit 4: Përputhja e koncepteve të sigurisë

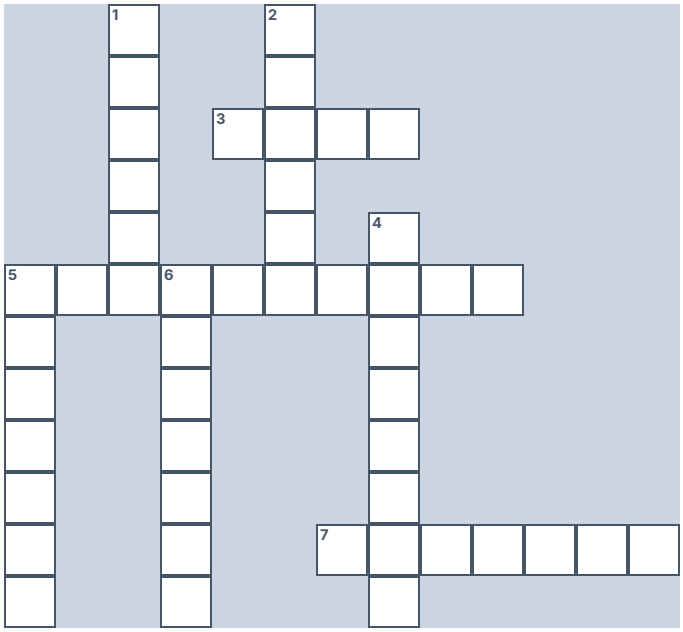
PËRPUTHJA E PËRKUFIZIMEVE

Përputh çdo term fjalori në të majtë me përkufizimin e tij të saktë në të djathtë, duke shkruar shkronjën përkatëse (A-H) në kutinë e plotësueshme.

☐	1. KALI I TROJËS	A	Program i projektuar për të monitoruar dhe regjistruar fshehurazi aktivitetin dhe të dhënat e futura të përdoruesit.
☐	2. RANSOMWARE	B	Malware që ekzekutohet drejtpërdrejt në RAM për të shmangur zbulimin nga skanerët e diskut.
☐	3. SPYWARE	C	Kufizimi i pikave fundore të infektuara për të parandaluar përhapjen e ngarkesave kërcënuese.
☐	4. ROOTKIT	D	Softuer keqdashës i maskuar si një program shërbimi i padëmshëm ose i dobishëm.
☐	5. SANDBOX	E	Malware vetëkopjues që përhapet nëpër rrjete pa veprim njerëzor.
☐	6. PËRMBAJTJE	F	Malware që enkripton ruajtjen e sistemit dhe kërkon pagesë për dërgimin e çelësit.
☐	7. KRIMB	G	Mjedis virtual i izoluar që përdoret për të analizuar skedarët keqdashës në mënyrë të sigurt.
☐	8. PA SKEDARË	H	Malware stealth që fshihet thellë në kernelet e sistemit për të ruajtur kontrollin administrativ.

Pika e kontrollit 5: Fjalëkryq

Zgjidhe fjalëkryqin duke shkruar shkronja në kutitë e bardha aktive. Numrat korrespondojnë me indiciet më poshtë.



HORIZONTALISHT

3. Malware vetëkopjues që përhapet nëpër rrjete pa veprim njerëzor. (4)

5. Malware që enkripton ruajtjen e sistemit dhe kërkon pagesë për dorëzimin e çelësit. (10)

7. Mjedis virtual i izoluar që përdoret për të analizuar skedarë keqdashës në mënyrë të sigurt. (7)

VERTIKALISHT

1. Softuer keqdashës i maskuar si program i padëmshëm ose i dobishëm. (6)

2. Kufizimi i pikave fundore të infektuara për të parandaluar përhapjen e ngarkesave të kërcënimit. (6)

4. Malware që ekzekutohet drejtpërdrejt në RAM për të shmangur zbulimin nga skanerët e diskut. (8)

5. Malware i fshehtë i ngjitur thellë në kernelet e sistemit për të ruajtur kontrollin administrativ. (7)

6. Program i projektuar për të monitoruar dhe regjistruar fshehurazi aktivitetin dhe të dhënat e futura të përdoruesit. (7)

Pika e kontrollit 5, alternativa: Çelësa të aksesueshëm të fjalëkryqit

Përdoruesit e lexuesve të ekranit dhe të tastierës mund t'i shkruajnë përgjigjet e fjalëkryqit drejtpërdrejt në fushat e tekstit më poshtë.

HORIZONTALISHT

3 horizontalisht: Malware vetëkopjues që përhapet nëpër rrjete pa veprim njerëzor. (4 shkronja):

5 horizontalisht: Malware që enkripton ruajtjen e sistemit dhe kërkon pagesë për dorëzimin e çelësit. (10 shkronja):

7 horizontalisht: Mjedis virtual i izoluar që përdoret për të analizuar skedarë keqdashës në mënyrë të sigurt. (7 shkronja):

VERTIKALISHT

1 vertikalisht: Softuer keqdashës i maskuar si program i padëmshëm ose i dobishëm. (6 shkronja):

2 vertikalisht: Kufizimi i pikave fundore të infektuara për të parandaluar përhapjen e ngarkesave të kërcënimit. (6 shkronja):

4 vertikalisht: Malware që ekzekutohet drejtpërdrejt në RAM për të shmangur zbulimin nga skanerët e diskut. (8 shkronja):

5 vertikalisht: Malware i fshehtë i ngjitur thellë në kernelet e sistemit për të ruajtur kontrollin administrativ. (7 shkronja):

6 vertikalisht: Program i projektuar për të monitoruar dhe regjistruar fshehurazi aktivitetin dhe të dhënat e futura të përdoruesit. (7 shkronja):

Pika e kontrollit 6: Kërkimi i fjalës së fshehur

Gjej 8 termat kyç të fjalorit të fshehur në rrjetën më poshtë. Fjalët mund të jenë horizontale, vertikale ose diagonale.

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

LISTA E FJALËVE TË LEKSIKUT

TROJAN RANSOMWARE SPYWARE ROOTKIT SANDBOX IZOLIM WORM PASKEDAR

Pika e kontrollit 6, alternativa: Përputhja e aksesueshme e fjalorit

Përputh secilin nga 8 termat e fjalorit nga Kërkimi i fjalëve me përkufizimin e saktë të tij, duke shkruar shkronjën (A-H) në vendin bosh.

TERMA LEKSIKORË

A. TROJAN

B. RANSOMWARE

C. SPYWARE

D. ROOTKIT

E. SANDBOX

F. IZOLIM

G. WORM

H. PASKEDAR

PËRKUFIZIME DHE FUSHA PËRPUTHJEJE

1. Malware i fshehtë i ngjitur thellë në kernelet e sistemit për të ruajtur kontrollin administrativ.

2. Kufizimi i pikave fundore të infektuara për të parandaluar përhapjen e ngarkesave të kërcënimit.

3. Malware që ekzekutohet drejtpërdrejt në RAM për të shmangur zbulimin nga skanerët e diskut.

4. Malware vetëkopjues që përhapet nëpër rrjete pa veprim njerëzor.

5. Malware që enkripton ruajtjen e sistemit dhe kërkon pagesë për dorëzimin e çelësit.

6. Program i projektuar për të monitoruar dhe regjistruar fshehurazi aktivitetin dhe të dhënat e futura të përdoruesit.

7. Softuer keqdashës i maskuar si program i padëmshëm ose i dobishëm.

8. Mjedis virtual i izoluar që përdoret për të analizuar skedarë keqdashës në mënyrë të sigurt.

Pika e kontrollit 7: Sfida e fjalëve të përzier

Rirenditi shkronjat më poshtë për të zbuluar konceptet dhe termat kryesorë të sigurisë kibernetike. Shkruaji përgjigjet në kutitë e dhëna.

1. **OTJANR** _____
2. **SYERAWP** _____
3. **DSBXNOA** _____
4. **MRWO** _____
5. **AMEASWORRN** _____
6. **IOKRTTO** _____
7. **IILMOZ** _____
8. **KAERPADS** _____

Aktivitet bonus: Mendo shpejt

3 PËRGJIGJE PËR ÇDO KATEGORI. FITON KUSH E PLOTËSON I PARI LISTËN.

1	Vende ku mund të shkarkosh aplikacione të sigurta			
2	Pajisje që mund të hakohen			
3	Gjëra që ruan si kopje rezervë			
4	Shenja paralajmëruese në një email			
5	Shenja që një telefon ka malware			
6	Lloje malware-i që njeh			
7	Lloje skedarësh me të cilët duhet të jesh i kujdesshëm			
8	Mënyra si hyn malware-i në një kompjuter			
9	Zakone të sigurta që mund t'i fillosh sot			
10	Fjalë që lidhen me sigurinë kibernetike			
11	Gjëra që bëhen pas një rrjedhjeje të dhënash			
12	Arsye për të përditësuar softuerin			
13	Kafshë ose personazhe me emra të ngjashëm me malware-in			
14	Gjëra që mund të vjedhë malware-i			
15	Gjëra që bëhen nëse ke klikuar lidhjen e gabuar			

Pika e kontrollit 8: Studime rasti për sigurinë kibernetike

Zbato konceptet që ke mësuar për të zgjidhur skenarët reale më poshtë.

STUDIMI I RASTIT 1: PËRMBAJTJA E NGARKESËS RANSOMWARE NË NDËRMARRJE

👷

Skenari: Një rrjet lokal korporativ është shkelur nga ransomware aktiv. Serverët kryesorë të skedarëve kanë filluar të shfaqin shtesa skedarësh me .locked. Vendos politika përmbajtjeje.

Pyetje për diskutim: Përshkruaj në detaje hapat e izolimit dhe përshkruaj protokollin e rikuperimit të të dhënave.

STUDIMI I RASTIT 2: INJEKTIMI I MALWARE-IT PA SKEDAR NË MEMORIE

👷

Skenari: Një analist zbulon modele të dyshimta skriptimi që ekzekutohen drejtpërdrejt në RAM-in e paqëndrueshëm të sistemit duke përdorur mjete standarde administrimi, por në disk nuk ekzistojnë skedarë keqdashës.

Pyetje për diskutim: Shpjego strategjinë e analizës së memories dhe specifiko mjetet për të bllokuar ekzekutimin pa skedarë (fileless).

Pika e kontrollit 9: Deshifrimi i kodit

Një profesionist i sigurisë kibernetike mbron asetet e rrjetit nga aktorët e kërcënimeve online. Përdor çelësin shkronjë-numër më poshtë për të deshifruar mesazhin duke shkruar shkronjat përkatëse në hapësirat e zbrazëta.

ÇELËSI I ENKRIPTIMIT SHKRONJË-NË-NUMËR

A=1 B=2 C=3 Ç=4 D=5 E=6 Ë=7 F=8 G=9

H=10 I=11 J=12 K=13 L=14 M=15 N=16 O=17 P=18

Q=19 R=20 S=21 T=22 U=23 V=24 X=25 Y=26 Z=27

27	2	23	14	17		16	9	1	20	13	6	21	1	22	15	6

15	17	16	11	22	17	20	11	15		21	12	6	14	14	12	6	12	6

Mesazhi i deshifruar:

KËSHILLË: ÇDO NUMËR PËRFAQËSON POZICIONIN E ASAJ SHKRONJE NË ALFABET (P.SH. 1 = A, 2 = B, 27 = Z).

Pika e kontrollit 10: Pyetje të shpeshta bazë për sigurinë kibernetike (Pjesa A)

Rishiko pyetje dhe përgjigje të zakonshme për zbutjen e kërcënimeve në internet.

Q1: Çfarë është malware-i?

Softuer keqdashës i projektuar nga aktorë kërcënimi për të dëmtuar, rrëmbyer ose vjedhur të dhëna nga pajisjet dhe rrjetet.

Q2: Cili është ndryshimi midis një virusi dhe një krimbi?

Një virus kërkon veprim njerëzor (si hapja e një skedari) për t'u përhapur, ndërsa një worm përhapet automatikisht nëpër rrjete.

Q3: Si e infekton një kompjuter një kalë Trojan?

I mashtron përdoruesit duke u maskuar si një program i padëmshëm ose i sigurt, duke fshehur brenda tij payload-in keqdashës.

Q4: Çfarë është ransomware?

Një lloj malware-i që enkripton skedarët në sistemin e synuar, duke kërkuar pagesë financiare në këmbim të çelësit të deshifrimit. [1]

Q5: Çfarë është spyware?

Softuer keqdashës që regjistron fshehurazi shtypjet e tastierës, fjalëkalimet dhe zakonet e shfletimit të përdoruesit për t'ua dërguar sulmuesve.

Pika e kontrollit 10: Pyetje të shpeshta bazë për sigurinë kibernetike (Pjesa B)

Rishiko pyetje dhe përgjigje të zakonshme për zbutjen e kërcënimeve në internet.

Q6: Çfarë do të thotë sandboxing?

Ekzekutimi i skedarëve të dyshimtë në një mjedis virtual të sigurt e të izoluar për të vëzhguar sjelljen e tyre pa rrezik për sistemet e prodhimit.

Q7: Çfarë është malware pa skedar (fileless malware)?

Malware që ekzekutohet drejtpërdrejt në memorien e sistemit (RAM) duke përdorur mjete legjitime, duke shmangur shkrimin e skedarëve në disk për të anashkaluar skanerët bazë.

Q8: Si e mbron një rootkit malware-in?

Fsheh procese dhe skedarë keqdashës, shpesh duke nënshtruar kernelin e sistemit operativ, ndaj skanerët antivirus mund t'i humbasin.

Q9: Çfarë është monitorimi dinamik i sjelljes?

Skanim antivirus që monitoron proceset aktive në kohë reale për të bllokuar veprimet tipike të malware-it, si enkriptimi masiv i skedarëve.

Q10: Pse është urgjente përmbajtja gjatë përgjigjes ndaj incidentit?

Izolimi i pikave fundore të kompromentuara parandalon përhapjen e payload-eve aktive të malware-it te pajisjet e tjera të rrjetit.

Pika e kontrollit 10: Pyetje të shpeshta të avancuara për sigurinë (Pjesa C)

Eksploro aspektet e avancuara teknike të kornizave të sigurisë, analizës së malware-it dhe pajtueshmërisë me të dhënat.

Q1: Si i kapërcejnë zhvilluesit e malware-it skanerët antivirus të bazuar në nënshkrime?

Përdorin polimorfizëm, duke ndryshuar hash-in dhe strukturën e kodit të skedarit me çdo infektim, ndërsa sjellja e dëmshme mbetet e njëjtë.

Q2: Cili është rreziku i mjeteve me dy përdorime në fushatat e malware-it?

Sulmuesit përdorin mjete administrative të ligjshme (si PowerShell ose Sysinternals) për t'u përzier me trafikun normal të rrjetit, duke e bërë zbulimin të vështirë.

Q3: Si i ekzekuton process hollowing ngarkesat keqdashëse?

Nis një proces legjitim të sistemit në gjendje të pezulluar, e zëvendëson kodin e tij në memorie me malware dhe e rinis ekzekutimin.

Q4: Cili është roli i një serveri Command and Control (C2)?

Një server i largët i operuar nga hakerat për të dërguar udhëzime dhe ngarkesa te malware-i që funksionon në makina të kompromet uara.

Q5: Pse është e vështirë të zbulohet keylogging?

Keylogger-ët bazë konsumojnë burime minimale të CPU-së dhe i fshehin proceset e tyre brenda mjeteve të ligjshme të hapësirës së përdoruesit.

Pika e kontrollit 10: Pyetje të shpeshta të avancuara për sigurinë (Pjesa D)

Eksploro aspektet e avancuara teknike të kornizave të sigurisë, analizës së malware-it dhe pajtueshmërisë me të dhënat.

Q6: Si e vonon errësimi i kodit analizën e malware-it?

Enkripton ose riorganizon kodin burimor, duke e bërë të palexueshëm për mjetet e analistëve dhe skanerët e sigurisë.

Q7: Cili është funksioni i një bootkit-i?

Një rootkit që infekton procesin e nisjes (MBR, sektorin e nisjes ose firmware-in UEFI), ndaj ekzekutohet para se të ngarkohet sistemi operativ.

Q8: Si i identifikon skanimi heuristik kërcënimet zero-day?

Skanon për modele të dyshimta kodi dhe komanda administrative në vend që të kërkojë një hash përputhës në bazën e të dhënave.

Q9: Cili është kërcënimi i rrëmbimit të DLL-ve (DLL hijacking)?

Detyrimi i një aplikacioni legjitim që të ngarkojë një bibliotekë keqdashëse me lidhje dinamike (DLL) duke e vendosur në shtegun e direktorisë së aplikacionit.

Q10: Si e përdorin virtualizimin linjat e automatizuara të analizës së malware-it?

Ekzekutojnë skedarë të dyshimtë nëpër VM të shumta të sistemeve operative, duke gjeneruar automatikisht regjistra sjelljeje dhe skedarë PCAP të rrjetit.

Pjesa 11: 10 fakte dhe njohuri nga bota reale për sigurinë kibernetike

Rishiko fakte reale për shkeljet e sigurisë, mekanizmat e mbrojtjes dhe standardet e pajtueshmërisë.

1. PERSPEKTIVË PËR SIGURINË

Kali i Trojës mbetet metodë e zakonshme infektimi sepse fsheh kodin e dëmshëm brenda programeve që duken të padëmshme.

2. PERSPEKTIVË PËR SIGURINË

IC3 i FBI-së mori mbi 3,600 ankesa për ransomware në 2025, me humbje të raportuara mbi 32 milionë dollarë. [3]

3. PERSPEKTIVË PËR SIGURINË

Krimbat (worms) mund të përhapen shpejt nëpër rrjete duke shfrytëzuar cenueshmëri të paarnuara të protokolleve, si EternalBlue në SMB.

4. PERSPEKTIVË PËR SIGURINË

Malware-i pa skedarë është i vështirë për t'u zbuluar sepse funksionon në memorie përmes mjeteve legjitime dhe lë pak gjurmë në disk.

5. PERSPEKTIVË PËR SIGURINË

Sandbox-et e analizës zakonisht kthehen te një snapshot i pastër pas çdo ekzekutimi, që çdo test të nisë nga një gjendje e njohur.

6. PERSPEKTIVË PËR SIGURINË

Rootkit-et mund të ndryshojnë thirrjet e sistemit të kernelit, duke raportuar rezultate të rreme diagnostikimi te skanerët kundër malware-it.

7. NJOHURI PËR SIGURINË

Errësimi i kodit përdor programe paketuese për të ngjeshur dhe fshehur strukturën e vërtetë binare të ngarkesës së malware-it.

8. NJOHURI PËR SIGURINË

Malware-i polimorfik e ndryshon kodin e vet, dhe kështu hash-in e skedarit, me çdo kopje të re për të shmangur kontrollet e nënshkrimeve.

9. NJOHURI PËR SIGURINË

Rrëmbimi i DLL-ve shfrytëzon konfigurimet e rendit të kërkimit në sisteme operative standarde si Windows.

10. PERSPEKTIVË PËR SIGURINË

Shitësit e sigurisë gjejnë çdo ditë numra të mëdhenj kampionësh të rinj malware, ndaj nënshkrimet kanë nevojë për përditësime të vazhdueshme.

Referenca teknike dhe burime

Udhëzuesi i studimit dhe enigmat interaktive janë përpiluar nga standardet globale të NIST, OWASP dhe të pajtueshmërisë me privatësinë e të dhënave.

REFERENCA AKADEMIKE DHE TË INDUSTRISË

[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

Çelësi i përgjigjeve: Pika e kontrollit 1 - Zgjedhje e shumëfishtë

1 **Pyetja 1** — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Cila është karakteristika përcaktuese e një Trojan horse? → Maskohet si softuer legjitim për t'i mashtruar përdoruesit ta ekzekutojnë

2 **Pyetja 2** — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Cili lloj malware-i enkripton skedarët dhe kërkon pagesë? → Ransomware

3 **Pyetja 3** — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Çfarë përfaqëson spyware-i? → Malware i dizajnuar për të monitoruar fshehurazi shtypjet e tastierës dhe aktivitetet e shfletuesit të përdoruesit

4 **Pyetja 4** — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Pse përdorin zhvilluesit e malware-it rootkit-e? → Për të fshehur proceset aktive dhe skedarët keqdashës nga sistemi operativ

5 **Pyetja 5** — **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Çfarë do të thotë sandboxing në analizën e malware-it? → Ekzekutimi i skedarëve të dyshimtë në një kasafortë virtuale të izoluar për të vëzhguar sjelljen në mënyrë të sigurt

Çelësi i përgjigjeve: Pika e kontrollit 2 - E vërtetë ose e gabuar

6 **Pyetja 6** — **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

E gabuar: krimbat vetë-replikohen dhe përhapen nëpër rrjete pa asnjë veprim të përdoruesit.

7 **Pyetja 7** — **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

E gabuar: adware nuk është gjithmonë i padëmshëm; një pjesë e madhe e gjurmon shfletimin për të targetuar reklama.

8 **Pyetja 8** — **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

E vërtetë: kopjet rezervë offline të pastra i rikthejnë skedarët e enkriptuar pa pagesë, megjithëse të dhënat e vjedhura mund të rrjedhin prapë.

9 **Pyetja 9** — **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

E gabuar: skanerët me nënshkrime kanë nevojë për një mostër të njohur, ndaj malware-i i ri zero-day mund t'u shpëtojë.

10 **Pyetja 10** — **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

Malware-i pa skedarë ekzekuton skripte keqdashëse në memorien e sistemit, duke shmangur shkrimin e skedarëve në disk.

Çelësat e fjalorit dhe rubrika e vlerësimit

Rubrika e vlerësimit për mësuesin: Jep 1 pikë për çdo përputhje të saktë (8 pikë gjithsej) dhe term konteksti (6 pikë gjithsej).

PIKA E KONTROLLIT 4: ÇELËSI – PËRPUTHJA E KONCEPTEVE

D 1. KALI I TROJËS	F 2. RANSOMWARE	A 3. SPYWARE	H 4. ROOTKIT
G 5. SANDBOX	C 6. PËRMBAJTJE	E 7. KRIMB	B 8. PA SKEDARË

PIKA E KONTROLLIT 3: ÇELËSI – TERMAT KRYESORË

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

PIKA E KONTROLLIT 6, ALTERNATIVA: ÇELËSI – PËRPUTHJA E FJALËVE

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

SHËNIME PËR DISKUTIM PËR MËSUESIT

Termat kryesorë:
Kontrollo nëse nxënësit mund të shpjegojnë KALI I TROJËS, RANSOMWARE dhe SPYWARE me fjalët e tyre dhe të japin një shembull për secilin.

Studimet e rastit:
Kërkoju nxënësve t'i mbështesin rekomandimet me fakte nga fleta, jo me supozime.

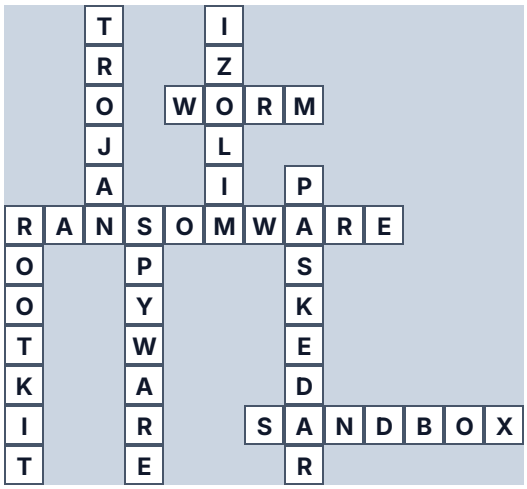
Vlerësimi i burimeve:
Kërkoju nxënësve të verifikojnë të paktën një pohim në burimet e fletës dhe diskutoni pse numrat, çmimet dhe rregullat mund të ndryshojnë me kalimin e kohës.

Çelësat e enigmave dhe shënimet për mësuesin

ZGJIDHJA E LOJËS ME FJALË

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

ZGJIDHJA E FJALËKRYQIT



UDHËZUES PËR MËSUESIN PËR ZGJIDHJET E KRYQËZËS

HORIZONTALISHT

3 horizontalisht: WORM Malware vetëkopjues që përhapet nëpër rrjete pa veprim njerëzor. (4 shkronja)

5 horizontalisht: RANSOMWARE Malware që enkripton ruajtjen e sistemit dhe kërkon pagesë për dorëzimin e çelësit. (10 shkronja)

7 horizontalisht: SANDBOX Mjedis virtual i izoluar që përdoret për të analizuar skedarë keqdashës në mënyrë të sigurt. (7 shkronja)

VERTIKALISHT

1 vertikalisht: TROJAN Softuer keqdashës i maskuar si program i padëmshëm ose i dobishëm. (6 shkronja)

2 vertikalisht: IZOLIM Kufizimi i pikave fundore të infektuara për të parandaluar përhapjen e ngarkesave të kërcënimit. (6 shkronja)

4 vertikalisht: PASKEDAR Malware që ekzekutohet drejtpërdrejt në RAM për të shmangur zbulimin nga skanerët e diskut. (8 shkronja)

5 vertikalisht: ROOTKIT Malware i fshehtë i ngjitur thellë në kernelet e sistemit për të ruajtur kontrollin administrativ. (7 shkronja)

6 vertikalisht: SPYWARE Program i projektuar për të monitoruar dhe regjistruar fshehurazi aktivitetin dhe të dhënat e futura të përdoruesit. (7 shkronja)

Çelësi i fjalëve të përzierura dhe i zgjidhjes së kodit

Çelësi i vlerësimit për aktivitetin e rirenditjes së fjalorit dhe për Sfidën e Kodit të Fshehtë.

ÇELËSI I RIRENDITJES SË FJALËVE

1. OTJANR	TROJAN	5. AMEASWORRN	RANSOMWARE
2. SYERAWP	SPYWARE	6. IOKRTTO	ROOTKIT
3. DSBXNOA	SANDBOX	7. IILMOZ	IZOLIM
4. MRWO	WORM	8. KAERPADS	PASKEDAR

ÇELËSI I SFIDËS SË KODIT TË FSHEHTË

"ZBULO NGARKESAT ME MONITORIM SJELLJEJE"

Çelësi i studimeve të rastit

A Studimi i rastit 1: Përmbajtja e ngarkesës ransomware në ndërmarrje

Zgjidhja për mësuesin

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Analiza e skenarit: Një rrjet lokal korporativ është shkelur nga ransomware aktiv. Serverët kyç të skedarëve kanë nisur të shfaqin shtesa skedarësh me .locked. Vendos politika izolimi.
- Strategjia dhe zgjidhja e rekomanduar: Shkëput të gjithë serverët e prekur nga rrjeti lokal. Mbyll seancat aktive administrative. Rikthe skedarët e pakompromentuar nga një sistem i sigurt kopjeruajtjeje offline, i mbyllur për shkrim.

B Studimi i rastit 2: Injektimi i malware-it pa skedar në memorie

Zgjidhja për mësuesin

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Analiza e skenarit: Një analist zbulon modele të dyshimta skriptimi që ekzekutohen drejtpërdrejt në RAM-in e paqëndrueshëm të sistemit duke përdorur mjete standarde administrative, por nuk ekzistojnë skedarë keqdashës në disk.
- Strategjia dhe zgjidhja e rekomanduar: Izolo pikat fundore të prekura dhe merr fillimisht një imazh të memories. Rishiko regjistrat e PowerShell dhe WMI, blloko skriptet e paaprovuara me AppLocker, pastaj rinise për të pastruar ngarkesën.