שם: _____ תאריך: _____ ציון: _____

ניתוח נוזקות והפחתת איומים מדריך

סוסים טרויאניים, כופרה, תוכנות ריגול, רוטקיטים, ארגזי חול של וירטואליזציה, בלימה

סקירת למידה: ניתוח נוזקות

אובטח

הצפנת נתונים

תקן AES של 256 סיביות

תואם

תקנים עולמיים

מסגרות GDPR ו-CCPA

אפס אמון

מדיניות גישה

אימות רב-גורמי

ברוכים הבאים! חוברת הפעילויות הזו תדריך אתכם דרך ניתוח נוזקות ומניעתן. תחקרו תוכנות ריגול, סוסים טרויאניים, מטעני תוכנות כופר, כלי הנדסה הפוכה, התנהגות רוטקיט ואסטרטגיות הכלה.

נקודות הביקורת בדף העבודה

- [ ] **חלק 1-4: שלטו באבטחת סייבר ובמניעת איומים.**
- [ ] **חלק 5-7: פתרו תשבצים ופאזלי חיפוש מילים.**
- [ ] **חלק 8-9: פתרו מקרי בוחן ואתגר צופן.**
- [ ] **חלק 10: סקרו את דפי השאלות הנפוצות הבסיסיים והמתקדמים.**
- [ ] **חלק 11: חקרו 10 עובדות מעניינות מהעולם האמיתי.**
- [ ] **בונוס: אתגר חשבו מהר**

פתחו את מדריך אבטחת הסייבר של VPN.com

URL: https://www.vpn.com/cybersecurity/malware/

מפת הלמידה שלכם: צמצום נוזקות

- הבחינו בין סוגי נוזקות: סוס טרויאני, תולעת ורוטקיט.
- יישמו הרצה בסביבה וירטואלית מבודדת (sandbox) לניתוח קוד.
- תכננו תוכניות בלימה וטיהור עבור מטענים פעילים של כופרה.

הוראות למדריך ניתוח נוזקות

ענו על שאלות אמריקאיות ועל שאלות נכון/לא נכון, השלימו את המשפטים החסרים בעזרת בנק המילים, התאימו הגדרות ופתרו את התשבץ ואת תפזורת המילים. יישמו את הידע שלכם בנושא צמצום נוזקות. ולסיום, פעילות הבונוס "חשבו מהר".

ניתוח נוזקות ובלימת איומים (מבוא)

קוד זדוני כמו סוסים טרויאניים, תולעים ותוכנות כופר מהווה איום בעל השפעה גבוהה על נקודות קצה ושרתים. צוותי אבטחה מנתחים נוזקות בארגזי חול וירטואליים ומפעילים בקרות בידוד רשת מהירות כדי לבלום את התפשטות המטען.

קראו כל נקודת ביקורת בעיון ובחרו או כתבו את התגובה הנכונה.

נקודת ביקורת 1: אתגר שאלות אמריקאיות

1. מהו המאפיין המגדיר של סוס טרויאני?

- A. הוא מתחזה לתוכנה לגיטימית כדי להערים על משתמשים להריץ אותו
- B. הוא משתכפל אוטומטית לאורך קווי הרשת המקומית
- C. הוא מדביק קבצים בתוך סביבות בדיקה וירטואליות מבודדות
- D. הוא מיירט תעבורה של ספק שירותי האינטרנט

2. איזה סוג של נוזקה מצפין קבצים ודורש תשלום?

- A. תוכנת כופר
- B. תוכנת ריגול
- C. Rootkit
- D. Adware

3. מה מייצג תוכנת ריגול?

- A. נוזקה שנועדה לנטר בחשאי הקשות מקלדת ופעילות דפדפן של משתמשים
- B. קוד תוכנה הרץ בתוך קונטיינר וירטואלי מבודד (ארגז חול)
- C. עדכוני אנטי-נוזקות שהורדו ממאגרי מסדי נתונים
- D. התאמה אוטומטית של בהירות המסך

4. מדוע מפתחי נוזקות משתמשים ברוטקיטים?

- A. כדי להסתיר תהליכים פעילים וקבצים זדוניים ממערכת ההפעלה
- B. כדי להגביר את מהירות העיבוד של המעבד בנקודות קצה
- C. כדי לגבות קבצי מסד נתונים לכספות ענן מאובטחות
- D. כדי לשפר את חיי הסוללה במחשבים ניידים

5. מה משמעות ארגז חול (sandboxing) בניתוח נוזקות?

- A. הרצת קבצים חשודים בכספת וירטואלית מבודדת כדי לצפות בהתנהגותם בבטחה
- B. סריקת האשים של קבצים מול מסדי נתונים של איומים מוכרים
- C. שחזור גיבויי מסדי נתונים לאחר חדירה
- D. ניתוק נתבי רשת מקומית מהקווים הציבוריים

נקודת ביקורת 2: אתגר נכון או לא נכון

שאלה 6

6. תולעים מחשביות דורשות אינטראקציה של משתמש אנושי כדי להתפשט ברשתות מקומיות.

נכון ○ לא נכון ○

שאלה 7

7. אדוור הוא תמיד בלתי מזיק ואינו עוקב אחר התנהגות המשתמש או היסטוריית הגלישה.

נכון ○ לא נכון ○

שאלה 8

8. שחזור גיבויים נקיים לא מקוונים מאפשר לקורבנות להתאושש מקבצים מוצפנים בלי לשלם את הכופר.

נכון ○ לא נכון ○

שאלה 9

9. אנטי-וירוס מבוסס חתימות עוצר באופן אמין נוזקות zero-day לפני שקיימת עבורן חתימה כלשהי.

נכון ○ לא נכון ○

שאלה 10

10. נוזקה ללא קבצים מריצה סקריפטים זדוניים בזיכרון המערכת ונמנעת מכתיבת קבצים לדיסק.

נכון ○ לא נכון ○

נקודת ביקורת 3: השלמת מונחי מפתח

קראו כל משפט שלהלן והשלימו את החסר במונח הנכון מבנק המילים.

1. נוזקה המוסווית כתוכנית שירות בטוחה היא _____ .
2. מטענים זדוניים הנועלים מערכות מסדי נתונים תמורת כסף מייצגים _____ .
3. תוכנות המתעדות סיסמאות בחשאי (keyloggers) מייצגות _____ .
4. הסתתרות עמוק בגרעיני מערכות ההפעלה מחייבת _____ .
5. ניתוח קבצים חשודים בכספת מבודדת נעשה באמצעות _____ וירטואלי.
6. עצירת התפשטותם של מטעני נוזקה פעילים מחייבת _____ מיידית של הרשת.

בנק מילים

ארגז חול | הכלה | נטול קבצים | סוס טרויאני | רוטקיט | תוכנת כופר | תוכנת ריגול | תולעת

כתבו את תשובותיכם כאן:

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

נקודת ביקורת 4: התאמת מושגים באבטחה

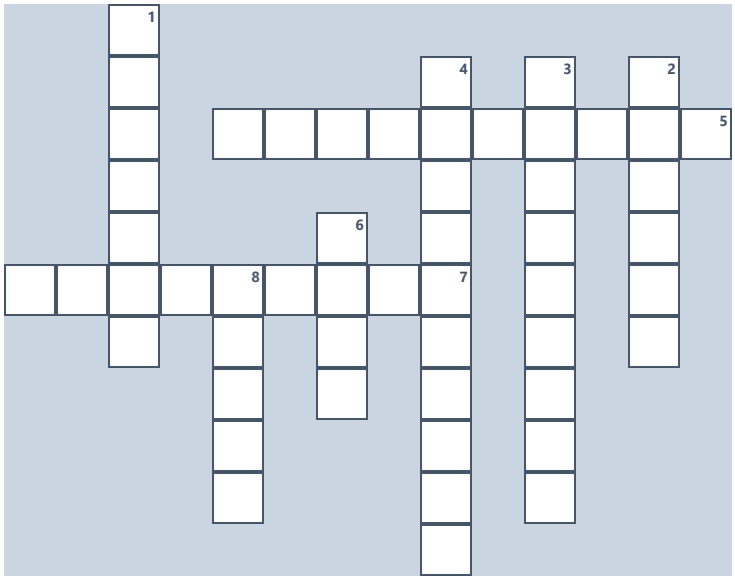
התאמת הגדרות

התאימו כל מונח אוצר מילים בצד ימין להגדרה הנכונה שלו בצד שמאל על ידי כתיבת האות המתאימה (A-H) בתיבת הקלט הניתנת למילוי.

1. סוס טרויאני	A	תוכנה שנועדה לפקח בסתר ולתעד את פעילות המשתמש ואת הקלט שלו.
2. תוכנת כופר	B	נוזקה הפועלת ישירות ב-RAM כדי להימנע מזיהוי בידי סורקי דיסק.
3. תוכנת ריגול	C	בידוד נקודות קצה נגועות כדי למנוע התפשטות מטעני איום.
4. רוטקיט	D	תוכנה זדונית המחופשת לתוכנית שירות תמימה או שימושית.
5. ארגז חול	E	נוזקה המתפשטת מעצמה ברחבי רשתות ללא פעולה אנושית.
6. בלימה	F	נוזקה המצפינה את אחסון המערכת ודורשת תשלום תמורת מסירת המפתח.
7. תולעת	G	סביבה וירטואלית מבודדת המשמשת לניתוח בטוח של קבצים זדוניים.
8. ללא קבצים	H	נוזקה חמקנית המסתתרת עמוק בליבות מערכת כדי לשמור על שליטה ניהולית.

נקודת ביקורת 5: תשבץ

פתרו את התשבץ על ידי הקלדת אותיות בתיבות הלבנות הפעילות. המספרים מתאימים לרמזים שלהלן.



מאונן

5. תוכנה זדונית המוסווית כתוכנית שירות תמימה או שימושית (10)

7. נוזקה המצפינה את אחסון המערכת ודורשת תשלום תמורת מסירת המפתח (9)

מאונך

1. סביבה וירטואלית מבודדת לניתוח בטוח של קבצים זדוניים (7)

2. נוזקה חמקנית המסתתרת עמוק בגרעין המערכת כדי לשמור על שליטה ניהולית (6)

3. נוזקה הרצה ישירות ב-RAM כדי להימנע מזיהוי על ידי סורקי דיסק (9)

4. תוכנית שנועדה לנטר ולתעד בחשאי את פעילות המשתמש ואת הקלט שלו (10)

6. הגבלת נקודות קצה נגועות כדי למנוע את התפשטות מטעני האיום (4)

8. נוזקה משכפלת את עצמה, המתפשטת ברשתות ללא פעולה אנושית (5)

נקודת ביקורת 5 – פעילות חלופית: רמזים נגישים לתשבץ

משתמשי קורא מסך ומקלדת יכולים להקליד את תשובות התשבץ ישירות בשדות הטקסט שלהלן.

מאוזן

5 מאוזן: תוכנה זדונית המוסווית כתוכנית שירות תמימה או שימושית (10 אותיות):

7 מאוזן: נוזקה המצפינה את אחסון המערכת ודורשת תשלום תמורת מסירת המפתח (9 אותיות):

מאונך

1 מאונך: סביבה וירטואלית מבודדת לניתוח בטוח של קבצים זדוניים (7 אותיות):

2 מאונך: נוזקה חמקנית המסתתרת עמוק בגרעין המערכת כדי לשמור על שליטה ניהולית (6 אותיות):

3 מאונך: נוזקה הרצה ישירות ב-RAM כדי להימנע מזיהוי על ידי סורקי דיסק (9 אותיות):

4 מאונך: תוכנית שנועדה לנטר ולתעד בחשאי את פעילות המשתמש ואת הקלט שלו (10 אותיות):

6 מאונך: הגבלת נקודות קצה נגועות כדי למנוע את התפשטות מטעני האיום (4 אותיות):

8 מאונך: נוזקה משכפלת את עצמה, המתפשטת ברשתות ללא פעולה אנושית (5 אותיות):

נקודת ביקורת 6: חיפוש מילה נסתרת

מצאו את 8 מונחי המפתח בלוח שלהלן. מילים יכולות להופיע אופקית, אנכית או באלכסון.

ג	ע	ח	ו	מ	ע	ל	א	ס	ש	ס	מ	ג	צ	פ
פ	ה	ת	י	ט	ב	א	ר	ב	ג	ר	נ	ת	י	ט
ל	ת	ע	י	ש	צ	י	ג	ד	ס	ו	ל	ט	ד	ח
ו	ל	ל	ל	י	ס	נ	ז	ז	ל	ט	ל	ס	ע	פ
ג	צ	ו	צ	ו	ס	ב	ח	פ	ס	ק	מ	ח	ת	ע
י	ב	ת	ר	ד	ו	פ	ו	ם	ק	י	ג	ם	ו	ר
ר	ו	י	ז	ם	ס	ד	ל	נ	ל	ט	ד	ע	כ	ש
ת	נ	ב	ק	ב	ט	א	ם	ט	מ	ד	י	א	נ	ד
נ	מ	ד	ה	ז	ר	ח	ד	ו	ע	ס	ל	ה	ת	ח
כ	ע	ם	פ	ה	ו	ה	ע	ל	ר	ה	א	א	כ	ע
ו	נ	ל	נ	צ	י	כ	ש	ק	ס	ט	ע	צ	ו	פ
ת	ג	ל	ת	ב	א	ל	ו	ב	ע	ש	ש	ט	פ	א
ע	ם	ת	ת	כ	נ	ה	ו	צ	ח	ל	ע	ט	ר	כ
כ	צ	נ	ז	ס	י	ס	ז	י	ם	א	מ	ק	ו	ק
ב	ת	ע	ת	ב	ז	כ	ם	ם	ו	ט	מ	נ	מ	ש

רשימת מילים

סוסטרויאני תוכנתכופר תוכנתריגול רוטקיט ארגזחול הכלה תולעת נטולקבצים

נקודת ביקורת 6 – פעילות חלופית: התאמת אוצר מילים נגישה

התאימו כל אחד מ-8 מונחי המילון מתפזורת המילים להגדרה הנכונה שלו על ידי כתיבת האות (A-H) במקום הריק.

מונחי אוצר מילים
A. סוסטרויאני
B. תוכנתכופר
C. תוכנתריגול
D. רוטקיט
E. ארגזחול
F. הכלה
G. תולעת
H. נטולקבצים

הגדרות ושדות התאמה	
1. נוזקה חמקנית המסתתרת עמוק בגרעין המערכת כדי לשמור על שליטה ניהולית.	
2. הגבלת נקודות קצה נגועות כדי למנוע את התפשטות מטעני האיום.	
3. נוזקה הרצה ישירות ב-RAM כדי להימנע מזיהוי על ידי סורקי דיסק.	
4. נוזקה משכפלת את עצמה, המתפשטת ברשתות ללא פעולה אנושית.	
5. נוזקה המצפינה את אחסון המערכת ודורשת תשלום תמורת מסירת המפתח.	
6. תוכנית שנועדה לנטר ולתעד בחשאי את פעילות המשתמש ואת הקלט שלו.	
7. תוכנה זדונית המוסווית כתוכנית שירות תמימה או שימושית.	
8. סביבה וירטואלית מבודדת לניתוח בטוח של קבצים זדוניים.	

נקודת ביקורת 7: אתגר מילים מבולבלות

סדרו מחדש את האותיות שלהלן כדי לחשוף מושגים ומונחים מרכזיים באבטחת סייבר. כתבו את תשובותיכם בתיבות הקלט המסופקות.

1. ניורוסאיטס
2. ונתותליגרכ
3. זאחלגור
4. לתעתו
5. ותורכנתפכ
6. יקרטטו
7. להכ
8. סקינלטבצו

פעילות בונוס: חשבו מהר

כתבו 3 תשובות לכל קטגוריה. מי שמסיים ראשון את הרשימה מנצח.

1	מקומות להורדת אפליקציות בטוחות		
2	מכשירים שאפשר לפרוץ אליהם		
3	דברים שמגבים		
4	סימני אזהרה באימייל		
5	סימנים לכך שבטלפון יש נוזקה		
6	סוגי נוזקות שאתם מכירים		
7	סוגי קבצים שצריך להיזהר מהם		
8	דרכים שבהן נוזקה מגיעה למחשב		
9	הרגלים בטוחים שאפשר להתחיל כבר היום		
10	מילים הקשורות לאבטחת סייבר		
11	דברים שעושים אחרי דליפת נתונים		
12	סיבות לעדכן תוכנה		
13	חיות או דמויות עם שמות שנשמעים כמו נוזקות		
14	דברים שנוזקה יכולה לגנוב		
15	דברים שעושים אם לחצתם על הקישור הלא נכון		

נקודת ביקורת 8: מקרי בוחן באבטחת סייבר

יישמו את המושגים שלמדתם כדי לפתור את התרחישים מהעולם האמיתי שלהלן.

מקרה בוחן 1: בלימת מטען כופרה ארגוני

👨‍💻

תרחיש: רשת מקומית ארגונית נפרצה על ידי כופרה פעילה. בשרתי קבצים מרכזיים החלו להופיע קבצים עם הסיומת .locked. קבעו מדיניות בלימה.

שאלה לדיון: פרטו את צעדי הבלימה, ותארו בקצרה את פרוטוקול שחזור הנתונים.

מקרה בוחן 2: הזרקת זיכרון של נוזקה חסרת קבצים

👨‍💻

תרחיש: אנליסט מזהה דפוסי סקריפטים חשודים שמופעלים ישירות בזיכרון ה-RAM הנדיף של המערכת באמצעות כלי ניהול סטנדרטיים, אך אין קבצים זדוניים בדיסק.

שאלה לדיון: הסבירו את אסטרטגיית ניתוח הזיכרון, וציינו כלים לחסימת הרצה ללא קבצים (fileless).

נקודת ביקורת 9: פענוח הצופן

איש מקצוע באבטחת סייבר מגן על נכסי רשת מפני גורמי איום מקוונים. השתמשו במפתח האותיות-למספרים שלהלן כדי לפענח את ההודעה, וכתבו את האותיות המתאימות במקומות הריקים.

מפתח הצפנה של אות למספר

א=1 ב=2 ג=3 ד=4 ה=5 ו=6 ז=7 ח=8 ט=9

י=10 כ=11 ל=12 מ=13 נ=14 ס=15 ע=16 פ=17 צ=18

ק=19 ר=20 ש=21 ת=22 ך=23 ם=24 ן=25 ף=26 ץ=27

22	20	7	16	2		5	18	19		10	14	16	9	13		6	5	7	
24	10	10	22	6	3	5	14	22	5		24	10	20	9	14	13			

ההודעה המפוענחת:

טיפ: כל מספר מייצג אות עברית אחת מהמפתח שלמעלה.

נקודת ביקורת 10: שאלות נפוצות על אבטחת סייבר – בסיסי (חלק A)

עיינו בשאלות ותשובות נפוצות בנושא צמצום איומים ברשת.

Q1: מהי נוזקה?

תוכנה זדונית שתוכננה בידי גורמי איום כדי לפגוע במכשירים וברשתות, לחטוף אותם או לגנוב מהם נתונים.

Q2: מה ההבדל בין וירוס לתולעת?

וירוס דורש פעולה אנושית (כמו פתיחת קובץ) כדי להתפשט, ואילו תולעת מתפשטת אוטומטית ברשתות.

Q3: כיצד סוס טרויאני מדביק מחשב?

הוא מטעה משתמשים בכך שהוא מתחזה לתוכנית תמימה או בטוחה ומסתיר בתוכה מטען זדוני.

Q4: מהי תוכנת כופר?

סוג של נוזקה שמצפינה קבצים במערכת היעד ודורשת תשלום כספי תמורת מפתח הפענוח. [1]

Q5: מהן תוכנות ריגול?

תוכנה זדונית המקליטה בסתר הקשות מקלדת, סיסמאות והרגלי גלישה של משתמשים כדי לשלוח אותם לתוקפים.

נקודת ביקורת 10: שאלות נפוצות על אבטחת סייבר – בסיסי (חלק B)

עיינו בשאלות ותשובות נפוצות בנושא צמצום איומים ברשת.

Q6: מה משמעות ארגז חול (sandboxing)?

הרצת קבצים חשודים בסביבה וירטואלית מאובטחת ומבודדת כדי לצפות בהתנהגותם בלי סיכון למערכות הייצור.

Q7: מהי נוזקה ללא קבצים (fileless malware)?

נוזקה הפועלת ישירות בזיכרון המערכת (RAM) באמצעות כלים לגיטימיים, ונמנעת מכתיבת קבצים לדיסק כדי לעקוף סורקים בסיסיים.

Q8: כיצד rootkit מגן על נוזקה?

הוא מסתיר תהליכים וקבצים זדוניים, לרוב על ידי חתירה תחת גרעין מערכת ההפעלה, ולכן סורקי אנטי-וירוס עלולים לפספס אותם.

Q9: מהו ניטור התנהגות דינמי?

סריקת אנטי-וירוס המנטרת תהליכים פעילים בזמן אמת כדי לחסום פעולות האופייניות לנוזקות, כגון הצפנה המונית של קבצים.

Q10: מדוע בלימה דחופה במהלך תגובה לאירוע?

בידוד נקודות קצה שנפרצו מונע ממטענים פעילים של נוזקות להתפשט למכשירי רשת אחרים.

נקודת ביקורת 10: שאלות נפוצות על אבטחה – מתקדם (חלק C)

חקרו היבטים טכניים מתקדמים של מסגרות אבטחה, ניתוח נוזקות ועמידה בדרישות נתונים.

Q1: כיצד מפתחי נוזקות עוקפים סורקי אנטי-וירוס מבוססי חתימות?

הם משתמשים בפולימורפיזם, משנים את הגיבוב ואת מבנה הקוד של הקובץ בכל הדבקה תוך שמירה על אותה התנהגות זדונית.

Q2: מהו הסיכון של כלים דו-שימושיים בקמפייני נוזקות?

תוקפים משתמשים בכלי ניהול לגיטימיים (כמו PowerShell או Sysinternals) כדי להשתלב בתעבורת הרשת הרגילה, מה שמקשה על הזיהוי.

Q3: כיצד process hollowing מריץ מטענים זדוניים?

הוא מפעיל תהליך מערכת לגיטימי במצב מושהה, מחליף את קוד הזיכרון שלו בנוזקה וממשיך בהרצה.

Q4: מה תפקידו של שרת פיקוד ובקרה (C2)?

שרת מרוחק המופעל על ידי האקרים כדי לשלוח הוראות ותוכן לנוזקות שרצות על מכונות שנפרצו.

Q5: מדוע קשה לזהות keylogging?

קיילוגרים בסיסיים צורכים משאבי מעבד מינימליים ומסתירים את התהליכים שלהם בתוך כלי עזר לגיטימיים של מרחב המשתמש.

נקודת ביקורת 10: שאלות נפוצות על אבטחה – מתקדם (חלק D)

חקרו היבטים טכניים מתקדמים של מסגרות אבטחה, ניתוח נוזקות ועמידה בדרישות נתונים.

Q6: כיצד ערפול קוד מעכב ניתוח נוזקות?

הוא מצפין או מסדר מחדש את קוד המקור, כך שאינו קריא לכלי אנליסטים ולסורקי אבטחה.

Q7: מה תפקידו של bootkit?

רוטקיט שמדביק את תהליך האתחול (MBR, מגזר האתחול או קושחת UEFI), ולכן הוא רץ לפני טעינת מערכת ההפעלה.

Q8: כיצד סריקה היוריסטית מזהה איומי zero-day?

הוא סורק דפוסי קוד חשודים ופקודות ניהול במקום לחפש גיבוב תואם במסד נתונים.

Q9: מהו האיום של DLL hijacking?

אילוץ אפליקציה לגיטימית לטעון ספריית קישור דינמית (DLL) זדונית על ידי הנחתה בנתיב התיקייה של האפליקציה.

Q10: כיצד צינורות אוטומטיים לניתוח נוזקות משתמשים בווירטואליזציה?

הם מריצים קבצים חשודים על פני מכונות וירטואליות של כמה מערכות הפעלה, ויוצרים אוטומטית יומני התנהגות וקובצי PCAP של רשת.

חלק 11: 10 עובדות ותובנות מהעולם האמיתי על אבטחת סייבר

עיינו בעובדות מהעולם האמיתי על פריצות אבטחה, מנגנוני הגנה ותקני ציות.

1. תובנות על אבטחה

סוסים טרויאניים נותרים שיטת הדבקה נפוצה משום שהם מסתירים קוד זדוני בתוך תוכנות שנראות תמימות.

2. תובנות על אבטחה

מרכז IC3 של ה-FBI קיבל למעלה מ-3,600 תלונות על כופרה ב-2025, עם הפסדים מדווחים של יותר מ-32 מיליון דולר. [3]

3. תובנות על אבטחה

תולעים יכולות להתפשט במהירות ברשתות על ידי ניצול פגיעויות לא מתוקנות בפרוטוקולים, כמו EternalBlue ב-SMB.

4. תובנות על אבטחה

נוזקה ללא קבצים קשה לזיהוי כי היא רצה בזיכרון באמצעות כלים לגיטימיים ומשאירה מעט עקבות בדיסק.

5. תובנות על אבטחה

ארגזי חול לניתוח חוזרים בדרך כלל לצילום מצב נקי לאחר כל הרצה, כך שכל בדיקה מתחילה ממצב ידוע.

6. תובנות על אבטחה

רוטקיטים יכולים לשנות קריאות מערכת של הקרנל ולדווח על תוצאות אבחון שגויות לסורקי נוזקות.

7. תובנה על אבטחה

טשטוש קוד משתמש בכלי אריזה כדי לדחוס ולהסתיר את מבנה המטען הבינארי האמיתי של נוזקה.

8. תובנה על אבטחה

נוזקה פולימורפית משנה את הקוד שלה, ולכן גם את גיבוב הקובץ, בכל עותק חדש כדי להתחמק מבדיקות חתימה.

9. תובנה על אבטחה

חטיפת DLL מנצלת תצורות של סדר חיפוש במערכות הפעלה רגילות כמו Windows.

10. תובנות על אבטחה

ספקי אבטחה מוצאים מספרים עצומים של דגימות נוזקה חדשות מדי יום, ולכן יש לעדכן את החתימות באופן מתמיד.

מקורות והפניות טכניים

מדריך הלימוד והפאזלים האינטראקטיביים נערכו על סמך תקנים גלובליים של NIST, OWASP ותאימות לפרטיות נתונים.

מקורות אקדמיים ותעשייתיים

[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

מפתח תשובות: נקודת ביקורת 1 – שאלות אמריקאיות

1 שאלה 1 — תשובה נכונה: A

הערה למורה

מהו המאפיין המגדיר של סוס טרויאני? → הוא מתחזה לתוכנה לגיטימית כדי להערים על משתמשים להריץ אותו

2 שאלה 2 — תשובה נכונה: A

הערה למורה

איזה סוג של נוזקה מצפין קבצים ודורש תשלום? → תוכנת כופר

3 שאלה 3 — תשובה נכונה: A

הערה למורה

מה מייצג תוכנת ריגול? → נוזקה שנועדה לנטר בחשאי הקשות מקלדת ופעילות דפדפן של משתמשים

4 שאלה 4 — תשובה נכונה: A

הערה למורה

מדוע מפתחי נוזקות משתמשים ברוטקיטים? → כדי להסתיר תהליכים פעילים וקבצים זדוניים ממערכת ההפעלה

5 שאלה 5 — תשובה נכונה: A

הערה למורה

מה משמעות ארגז חול (sandboxing) בניתוח נוזקות? → הרצת קבצים חשודים בכספת וירטואלית מבודדת כדי לצפות בהתנהגותם בבטחה

מפתח תשובות: נקודת ביקורת 2 – נכון או לא נכון

6 שאלה 6

תשובה נכונה: לא נכון

הערה למורה

לא נכון: תולעים משכפלות את עצמן ומתפשטות ברשתות בלי שום פעולת משתמש.

7 שאלה 7

תשובה נכונה: לא נכון

הערה למורה

לא נכון: אדוור (adware) אינו תמיד בלתי מזיק; חלק גדול ממנו עוקב אחר גלישה כדי למקד פרסומות.

8 שאלה 8

תשובה נכונה: נכון

הערה למורה

נכון: גיבויים נקיים לא מקוונים משחזרים קבצים מוצפנים בלי לשלם, אף שנתונים גנובים עדיין עלולים לדלוף.

9 שאלה 9

תשובה נכונה: לא נכון

הערה למורה

לא נכון: סורקי חתימות זקוקים לדגימה מוכרת, ולכן נוזקות zero-day חדשות לגמרי יכולות לחמוק מהם.

10 שאלה 10

תשובה נכונה: נכון

הערה למורה

נוזקה ללא קבצים מריצה סקריפטים זדוניים בזיכרון המערכת ונמנעת מכתיבת קבצים לדיסק.

מפתחות אוצר מילים ומחוון הערכה

מחוון הערכה למורה: תנו 1 נקודה לכל התאמה נכונה (סה"כ 8 נקודות) ולכל מונח הקשר (סה"כ 6 נקודות).

נקודת ביקורת 4: מפתח תשובות – התאמת מושגים

D 1. סוס טרויאני	F 2. תוכנת כופר	A 3. תוכנת ריגול	H 4. רוטקיט
G 5. ארגז חול	C 6. בלימה	E 7. תולעת	B 8. ללא קבצים

נקודת ביקורת 3: מפתח תשובות – מונחי מפתח

1 סוס טרויאני	2 תוכנת כופר	3 תוכנת ריגול	4 רוטקיט
5 ארגז חול	6 הכלה		

נקודת ביקורת 6 – פעילות חלופית: מפתח תשובות – התאמת אוצר מילים

1 D – רוטקיט	2 F – הכלה	3 H – נטולקבצים	4 G – תולעת
5 B – תוכנתכופר	6 C – תוכנתריגול	7 A – סוסטרויאני	8 E – ארגזחול

הערות לדיון עבור מורים

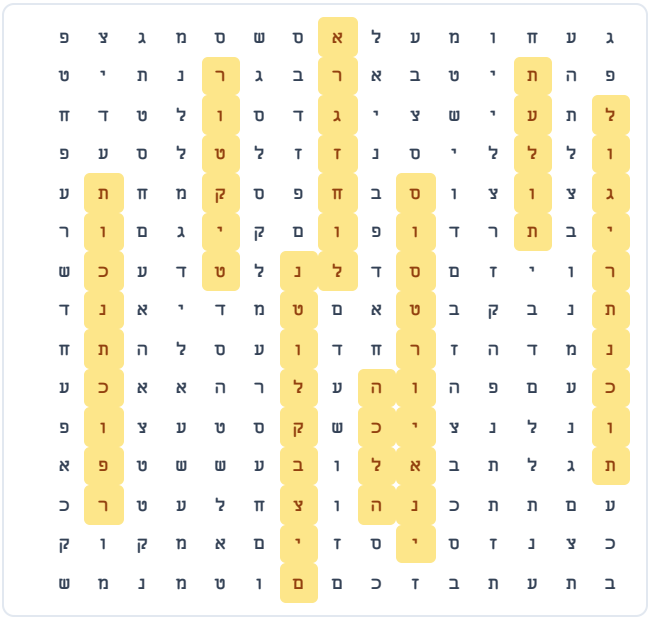
מונחי מפתח:
ודאו שהתלמידים מסבירים במילים שלהם את סוס טרויאני, תוכנת כופר ו-תוכנת ריגול ונותנים דוגמה לכל אחד מהם.

מקרי בוחן:
בקשו מהתלמידים לבסס את ההמלצות שלהם על עובדות מדף העבודה ולא על דעות.

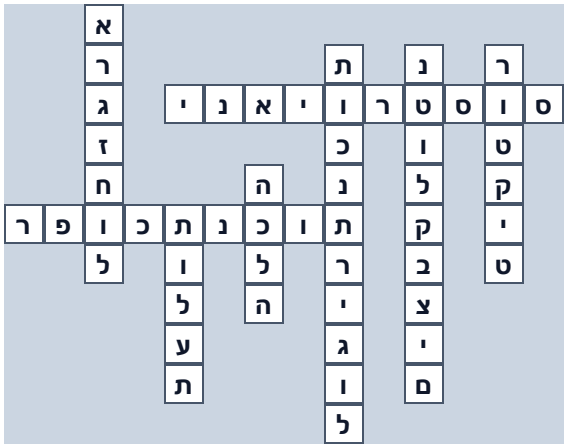
הערכת מקורות:
בקשו מהתלמידים לאמת לפחות טענה אחת במקורות של דף העבודה, ודונו מדוע נתונים, מחירים וכללים עשויים להשתנות עם הזמן.

מפתחות פאזלים והערות למורה

פתרון תפזורת



פתרון תשבץ



מדריך למורה לפתרונות התשבץ

מאוזן

5 מאוזן: סוסטרואיאני תוכנה זדונית המוסווית כתוכנית שירות תמימה או שימושית (10 אותיות)

7 מאוזן: תוכנתכופר נוזקה המצפינה את אחסון המערכת ודורשת תשלום תמורת מסירת המפתח (9 אותיות)

מאונך

1 מאונך: ארגזחול סביבה וירטואלית מבודדת לניתוח בטוח של קבצים זדוניים (7 אותיות)

2 מאונך: רוטקיט נוזקה חמקנית המסתתרת עמוק בגרעין המערכת כדי לשמור על שליטה ניהולית (6 אותיות)

3 מאונך: נטולקבצים נוזקה הרצה ישירות ב-RAM כדי להימנע מזיהוי על ידי סורקי דיסק (9 אותיות)

4 מאונך: תוכנתריגול תוכנית שנועדה לנטר ולתעד בחשאי את פעילות המשתמש ואת הקלט שלו (10 אותיות)

6 מאונך: הכלה הגבלת נקודות קצה נגועות כדי למנוע את התפשטות מטעני האיום (4 אותיות)

8 מאונך: תולעת נוזקה משכפלת את עצמה, המתפשטת ברשתות ללא פעולה אנושית (5 אותיות)

מפתח פתרונות: מילים מבולבלות ופענוח הצופן

מפתח הערכה לפעילות פענוח מילות אוצר המילים ולאתגר הצופן הסודי.

מפתח פענוח מילים מבולבלות

1. ניורוסאיטס — סוסטרויאני
2. ונתותליגרכ — תוכנתריגול
3. זאחלגור — ארגזחול
4. לתעתו — תולעת
5. ותורכנתפכ — תוכנתכופר
6. יקרטטו — רוטקיט
7. לההכ — הכלה
8. סקינלטבצו — נטולקבצים

מפתח אתגר הצופן הסודי

"זהו מטעני קצה בעזרת מנטרים התנהגותיים"

מפתח תשובות למקרי הבוחן

A מקרה בוחן 1: בלימת מטען כופרה ארגוני

פתרון למורה

הנחיות הערכה

תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- ניתוח תרחיש: רשת מקומית ארגונית נפרצה על ידי תוכנת כופר פעילה. שרתי קבצים מרכזיים החלו להציג סיומות קבצים .locked. קבעו מדיניות בלימה.
- אסטרטגיה ופתרון מומלצים: נתקו את כל השרתים שנפגעו מהרשת המקומית. סיימו הפעלות ניהול פעילות. שחזרו קבצים שלא נפגעו ממערכת גיבוי לא מקוונת מאובטחת ונעולה לכתיבה.

B מקרה בוחן 2: הזרקת זיכרון של נוזקה חסרת קבצים

פתרון למורה

הנחיות הערכה

תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- ניתוח תרחיש: אנליסט מזהה דפוסי סקריפטים חשודים שרצים ישירות בזיכרון RAM נדיף של המערכת באמצעות כלי ניהול סטנדרטיים, אך אין קבצים זדוניים בדיסק.
- אסטרטגיה ופתרון מומלצים: בודדו את נקודות הקצה שנפגעו ולכדו תחילה תמונת זיכרון. בדקו יומני PowerShell ו-WMI, חסמו סקריפטים לא מאושרים באמצעות AppLocker, ואז הפעילו מחדש כדי לנקות את המטען.