שם: _____ תאריך: _____ ציון: _____

התקפות תוכנת כופר ועסקים התאוששות

הפעלת המטען, הצפנת קבצים קריפטוגרפית, גיבויים לא מקוונים, נהלי בלימה והתאוששות מאסון.

סקירת למידה: התקפות תוכנת כופר

ברוכים הבאים! חוברת הפעילויות הזו תדריך אתכם דרך התקפות תוכנות כופר והתאוששות עסקית. תחקרו הרצת מטען, הצפנת קבצים, גיבויים לא מקוונים, הכלת איומים, תשלומים במטבעות קריפטוגרפיים ותוכניות התאוששות מאסון.

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**

אובטח

הצפנת נתונים

תקן AES של 256 סיביות

תואם

תקנים עולמיים

מסגרות GDPR ו-CCPA

אפס אמון

מדיניות גישה

אימות רב-גורמי

פתחו את מדריך אבטחת הסייבר של VPN.com

URL: https://www.vpn.com/cybersecurity/ransomware-attack/

מפת הלמידה שלכם: התאוששות מכופרה

- הבחינו בין מטענים של סוס טרויאני, כופרה ותוכנת ריגול.
- נתחו קבצים זדוניים בתוך סביבות ארגז חול מאובטחות.
- גבשו נהלים להפרדה ובלימה מהירה של רשת.

הוראות מדריך התקפות תוכנת כופר

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 התאוששות מתקיפת כופרה. ולסיום, פעילות הבונוס "חשבו מהר".

התקפות תוכנת כופר והתאוששות מאסון (מבוא)

מטענים של תוכנת כופר נועלים באופן קריפטוגרפי את אחסון המערכת ודורשים תשלום במטבע קריפטוגרפי תמורת מפתחות פענוח. צמצום האיום כולל כללי בידוד רשת, ניתוח נוזקות בארגז חול וגיבויי קור חזקים מנותקי רשת (air-gapped).

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

נקודת ביקורת 1: אתגר שאלות אמריקאיות

1. מהו המנגנון העיקרי של התקפת כופרה?

- A. הצפנה קריפטוגרפית של קבצי משתמש כדי למנוע גישה למערכת
- B. הזרקת פקודות SQL זדוניות לשדות טפסים
- C. האזנה לחבילות רשת בחיבור Wi-Fi ציבורי
- D. זיוף כותרות דוא"ל כדי לעקוף אימות SPF

2. מהו גיבוי לא מקוון (קר)?

- A. עותק אחסון שמנותק מהרשת כדי להגן עליו מהתפשטות נוזקות
- B. גיבוי המאוחסן בכונן הקשיח של שרת האינטרנט הראשי
- C. מטמון זמני של יומני רישום המערכת (registry)
- D. כלי ניהול לאיפוס סיסמאות משתמשים

3. כיצד על צוותי אבטחה לבודד מערכות נגועות במהלך התקפת כופרה?

- A. לנתק מיד כבלי רשת ולהשבית ממשקים אלחוטיים
- B. שדרוג מסד נתוני החתימות של האנטי-וירוס
- C. כיבוי שרת ה-DNS הראשי
- D. שינוי שם סיומות הקבצים שנפגעו

4. מדוע גופי ביטחון ממליצים שלא לשלם דרישות כופר?

- A. תשלום כספים מעודד תוקפים ואינו מבטיח מסירה של מפתח הפענוח
- B. הוא מבטל אוטומטית את כל פוליסות הביטוח הארגוניות
- C. הוא מודיע אוטומטית לכל לקוח בדוא"ל
- D. הוא משחית את שאר קבצי הגיבוי של המערכת

5. מהי תוכנית התאוששות מאסון (DRP)?

- A. תהליך מובנה לשחזור פעילות ונתונים לאחר פגיעה במערכת
- B. תצורת חומת אש הממפה פורטי רשת נכנסים
- C. סכמת מסד נתונים המפרטת הרשאות ניהול של משתמשים
- D. פרוטוקול אימות דוא"ל הדוחה דומיינים מזויפים

נקודת ביקורת 2: אתגר נכון או לא נכון

שאלה 6

6. מטענים של תוכנת כופר עלולים להתפשט בקלות לגיבויים מקוונים המחוברים לרשת.

נכון לא נכון

שאלה 7

7. תשלום כופר בקריפטו מבטיח שהקבצים יפוענחו בהצלחה.

נכון לא נכון

שאלה 8

8. ניתוק מערכות נגועות מהרשת עוזר לעצור את התפשטות תוכנת הכופר למערכות סמוכות.

נכון לא נכון

שאלה 9

9. כופרה לעולם אינה משתמשת בהצפנה סימטרית כדי להצפין אחסון מערכת.

נכון לא נכון

שאלה 10

10. בדיקה סדירה של נהלי שחזור נתונים היא חלק קריטי בהתאוששות מאסון.

נכון לא נכון

נקודת ביקורת 3: השלמת מונחי מפתח

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

1. מניעת גישה לקבצים מקומיים נעשית באמצעות _____ קריפטוגרפית.
2. הקוד הזדוני הפעיל שמורץ במערכת נקרא _____ .
3. עותקי אחסון מנותקים מחוץ לאתר מהווים _____ מאובטח.
4. עצירת התפשטות נוזקה מחייבת _____ של נקודות הקצה ברשת.
5. תשלום המטבע הקריפטוגרפי שדורשים פושעי סייבר נקרא דמי _____ .
6. החזרת קובצי נתונים תפעוליים מהווה _____ מאסון.

בנק מילים

אסון | בידוד | גיבוי קר | הצפנה | התאוששות | כופר | מטען | סוס טרויאני

כתבו את תשובותיכם כאן:

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

נקודת ביקורת 4: התאמת מושגים באבטחה

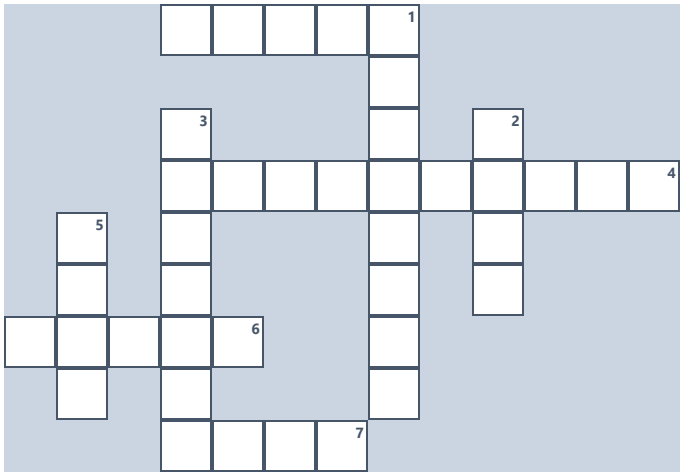
התאמת הגדרות

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

1. הצפנה	A	ניתוק מערכות רשת נגועות.
2. מטען נתונים	B	קובץ זדוני המחופש לקובץ תקין.
3. גיבוי קר	C	נעילת קבצים באמצעות הצפנה.
4. בידוד	D	אירוע שיבוש מערכתי רחב היקף.
5. כופר	E	הרצת תוכנה זדונית.
6. התאוששות	F	עותק לא מקוון ומנותק.
7. אסון	G	שחזור מסד נתונים מגיבוי.
8. סוס טרויאני	H	בקשת תשלום של מפתח קריפטוגרפי.

נקודת ביקורת 5: תשבץ

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



מאוזן

1. נעילת קבצים בשיטות קריפטוגרפיות (5)

4. קובץ זדוני המוסווה כנקי (10)

6. ניתוק מערכות רשת נגועות (5)

7. בקשת תשלום תמורת מפתח קריפטוגרפי (4)

מאונך

1. שחזור מסד נתונים מגיבוי (8)

2. הרצת תוכנה זדונית (4)

3. עותק מנותק לא מקוון (7)

5. אירוע של שיבוש מערכתי חמור (4)

נקודת ביקורת 5 – פעילות חלופית: רמזים נגישים לתשבץ

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

מאוזן

1 מאוזן: נעילת קבצים בשיטות קריפטוגרפיות (5 אותיות):

4 מאוזן: קובץ זדוני המוסווה כנקי (10 אותיות):

6 מאוזן: ניתוק מערכות רשת נגועות (5 אותיות):

7 מאוזן: בקשת תשלום תמורת מפתח קריפטוגרפי (4 אותיות):

מאונך

1 מאונך: שחזור מסד נתונים מגיבוי (8 אותיות):

2 מאונך: הרצת תוכנה זדונית (4 אותיות):

3 מאונך: עותק מנותק לא מקוון (7 אותיות):

5 מאונך: אירוע של שיבוש מערכתי חמור (4 אותיות):

נקודת ביקורת 6: חיפוש מילה נסתרת

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

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

רשימת מילים

הצפנה | מטען | גיבויקר | בידוד | כופר | התאוששות | אסון | סוסטרואיאני

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. הצפנה
B. מטען
C. גיבויקר
D. בידוד
E. כופר
F. התאוששות
G. אסון
H. סוסטרויאני

הגדרות ושדות התאמה	
1. עותק מנותק לא מקוון.	
2. קובץ זדוני המוסווה כנקי.	
3. נעילת קבצים בשיטות קריפטוגרפיות.	
4. בקשת תשלום תמורת מפתח קריפטוגרפי.	
5. ניתוק מערכות רשת נגועות.	
6. אירוע של שיבוש מערכתי חמור.	
7. הרצת תוכנה זדונית.	
8. שחזור מסד נתונים מגיבוי.	

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. נ פ ה ה צ
2. ג ב ר ק י ו י
3. ר כ פ ו
4. ן ו א ס
5. ן מ ע ט
6. ו ב ד ד י
7. ה ת ש ש ו ת ו א
8. נ ט ו י ס ר ו י א ס

פעילות בונוס: חשבו מהר

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

1	מידע שלעולם אסור לשתף		
2	מכשירים שאפשר לפרוץ אליהם		
3	סיבות לא לשלם כופר		
4	הרגלים בטוחים שאפשר להתחיל כבר היום		
5	כלי אבטחה שאתם מכירים		
6	דרכים להגן על החשבונות שלכם		
7	סימנים לכך שמחשב נדבק		
8	מקומות לשמור בהם גיבוי		
9	קבצים שלעולם לא תרצו לאבד		
10	דרכים שבהן תוכנת כופר מתפשטת		
11	דברים שעושים בשעה הראשונה של התקפה		
12	אנשים לפנות אליהם בזמן התקפה		
13	דברים שתוכנת כופר יכולה לנעול		
14	מילים הקשורות לאבטחת סייבר		
15	ארגונים שלרוב הם מטרה להתקפות		

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

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

מקרה בוחן 2: הערכת ארכיטקטורות גיבוי לא מקוונות

👷

תרחיש: ארגון רוצה לתכנן אסטרטגיית גיבוי נתונים שמפחיתה את הסיכון שהגיבויים ייפגעו, גם אם הרשת המקומית הראשית נחטפת לחלוטין על ידי תוכנת כופר.

שאלה לדיון: תכננו מערכת כספת לאחסון גיבויים לא מקוונים ומאובטחים.

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

24	10	14	6	22	14		22	11	20	16	13		6	20	7	8	21
20	19		10	6	2	10	3	13		22	14	17	18	6	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 כופרה?

תוכנת כופר היא תוכנה זדונית שנועדה לחסום גישה למערכות מחשב או לקבצים עד לתשלום סכום כופר.

Q2: כיצד כופרה מתפשטת?

באמצעות קבצים מצורפים בהודעות פישינג, פגיעויות בתוכנה שלא תוקנה ומערכות גישה מרחוק שנפרצו. [1]

Q3: מדוע מבקשים תשלום במטבע קריפטוגרפי?

מטבעות קריפטוגרפיים כמו Bitcoin מציעים אנונימיות יחסית, מה שמקשה על רשויות האכיפה לעקוב אחר הכספים.

Q4: האם אנטי-וירוס חוסם תוכנות כופר?

כן, אך אנטי-וירוס מבוסס חתימות עלול להיכשל מול מטעני כופרה חדשים מסוג zero-day.

Q5: מהו גיבוי מנותק מהרשת (air-gapped)?

עותק גיבוי שאין לו חיבור פיזי או לוגי לרשת הראשית, ובכך מוגן מפני התפשטות.

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

עיינו בשאלות ותשובות נפוצות בנושא צמצום איומים ברשת.

Q6: מהי סחיטה כפולה?

כשתוקפים לא רק מצפינים קבצים אלא גם גונבים נתונים רגישים כדי לאיים בדליפה פומבית אם לא ישולם כופר.

Q7: מהו מפענח (decryptor)?

כלי תוכנה שמכיל את המפתח הקריפטוגרפי הנדרש לשחזור קבצים נעולים לטקסט גלוי.

Q8: כיצד מזהים תוכנת כופר מוקדם?

על ידי ניטור מערכות קבצים לאיתור פעילות פתאומית ורחבה של שינוי ושינוי שם של קבצים.

Q9: מה תפקידו של ביטוח?

ביטוח סייבר יכול לסייע בכיסוי עלויות התאוששות, אך תנאי הכיסוי וכללי תשלום כופר משתנים בין פוליסות.

Q10: האם כדאי להפעיל מחדש מערכת נגועה?

לא, הפעלה מחדש עלולה להשמיד ראיות בזיכרון נדיף; בודדו את המכשיר מהרשת במקום זאת. [1]

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

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

Q1: כיצד כופרה משתמשת בהצפנה א-סימטרית?

הוא משתמש במפתח ציבורי המוטמע בנוזקה כדי להצפין קבצים, וצריך את המפתח הפרטי של התוקף כדי לפענח אותם.

Q2: מדוע נעשה שימוש גם בהצפנה סימטרית?

הצפנה סימטרית (כמו AES) מהירה ויכולה לנעול מסדי נתונים עצומים תוך דקות, בעוד מפתחות אסימטריים מאבטחים את מפתח ה-AES.

Q3: מהי חלוקה לוגית (logical segmentation)?

חלוקת רשתות לאזורים מבודדים, המונעת מנוזקות להתפשט לרוחב מצמתי תחנות עבודה לשרתי הליבה.

Q4: מהו אחסון WORM?

מדיה מסוג כתיבה-אחת-קריאה-רבות (WORM), המונעת מנוזקות כופרה לערוך, לדרוס או למחוק נתוני גיבוי.

Q5: מהם עותקי צל (shadow copies)?

צילומי גיבוי מקומיים שנוצרים בידי Windows; תוכנת כופר מוחקת אותם בדרך כלל תחילה באמצעות כלי ניהול.

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

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

Q6: כיצד גניבת אישורי גישה מאפשרת תוכנות כופר?

תוקפים רוכשים פרטי התחברות של מנהלים שדלפו כדי להתחבר דרך שולחנות עבודה מרוחקים, ומריצים ידנית כופרה ברחבי הרשת.

Q7: מהי בדיקת שחזור בהרצה יבשה (dry-run)?

שחזור סדיר של מסדי נתוני גיבוי לסביבות בדיקה מבודדות כדי לוודא שמהירות השחזור ושלמות הנתונים עומדות במדדי התאוששות מאסון.

Q8: כיצד זיהוי נקודות קצה (EDR) עוצר תוכנות כופר?

על ידי ניתוח התנהגות תהליכים (למשל הצפנה מהירה) והשעיה מהירה של האפליקציה הזדונית.

Q9: מהו מודל תוכנת כופר כשירות (RaaS)?

מודל זיכיון שבו מפתחי נוזקות משכירים בוני תוכנות כופר לשותפים תמורת אחוז מהתשלומים.

Q10: כיצד RDP שלא עודכן מוביל לכופרה?

שערי Remote Desktop Protocol חשופים וללא עדכוני אבטחה מאפשרים לתוקפים לבצע ניחוש אלים של פרטי כניסה ולהפעיל נוזקות ידנית.

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

גורמי תוכנת כופר משתמשים לעיתים קרובות בכלים כמו vssadmin.exe כדי למחוק עותקי צל של Windows ולחסום שחזורים מקומיים. [1]

2. תובנות על אבטחה

מפתחות AES-256 סימטריים משמשים בדרך כלל להצפנת מטעני קבצים, אשר ננעלים לאחר מכן באמצעות מפתחות RSA ציבוריים.

3. תובנות על אבטחה

התאוששות מהתקפת תוכנת כופר מוצלחת עלולה להימשך שבועות, ולכן גיבויים לא מקוונים שנבדקו חשובים.

4. תובנות על אבטחה

ה-FBI אינו תומך בתשלום כופר ומזהיר שתשלום אינו מבטיח שתקבלו בחזרה נתונים כלשהם. [2]

5. תובנות על אבטחה

תוכניות להתאוששות מאסון (DRP) צריכות להגדיר יעד זמן התאוששות (RTO) ויעד נקודת התאוששות (RPO).

6. תובנות על אבטחה

ה-FBI ממליץ על גיבויים מוצפנים ובלתי ניתנים לשינוי, כלומר כאלה שאי אפשר לשנות או למחוק. [3]

7. תובנה על אבטחה

מפתחי תוכנת כופר משתמשים בטכניקות ערפול מתקדמות כדי לעקוף סורקי אנטי-וירוס מסורתיים מבוססי חתימות.

8. תובנה על אבטחה

פילוח רשת מגביל תנועה לרוחב ומסייע לעצור תוכנת כופר מלהתפשט מעבר למארח הראשון שנדבק. [3]

9. תובנה על אבטחה

שירותים מרוחקים חשופים ומאובטחים בצורה לקויה, כמו Remote Desktop Protocol (RDP), הם נקודת כניסה נפוצה לכופרה. [1]

10. תובנות על אבטחה

CISA ממליצה לשמור גיבויים מוצפנים במצב לא מקוון, מכיוון שגרסאות כופרה רבות מחפשות גיבויים נגישים ומוחקות אותם. [1]

מקורות והפניות טכניים

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

מקורות אקדמיים ותעשייתיים

[1] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[2] FBI Internet Crime Complaint Center. (n.d.). Ransomware.
https://www.ic3.gov/CrimeInfo/Ransomware

[3] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[4] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-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 המנגנון העיקרי של התקפת כופרה? → הצפנה קריפטוגרפית של קבצי משתמש כדי למנוע גישה למערכת

2 שאלה 2 — **תשובה נכונה: A**

הערה למורה

מהו גיבוי לא מקוון (קר)? → עותק אחסון שמנותק מהרשת כדי להגן עליו מהתפשטות נוזקות

3 שאלה 3 — **תשובה נכונה: A**

הערה למורה

כיצד על צוותי אבטחה לבודד מערכות נגועות במהלך התקפת כופרה? → לנתק מיד כבלי רשת ולהשבית ממשקים אלחוטיים

4 שאלה 4 — **תשובה נכונה: A**

הערה למורה

מדוע גופי ביטחון ממליצים שלא לשלם דרישות כופר? → תשלום כספים מעודד תוקפים ואינו מבטיח מסירה של מפתח הפענוח

5 שאלה 5 — **תשובה נכונה: A**

הערה למורה

מהי תוכנית התאוששות מאסון (DRP)? → תהליך מובנה לשחזור פעילות ונתונים לאחר פגיעה במערכת

מפתח תשובות: נקודת ביקורת 2 – נכון או לא נכון

6 שאלה 6

תשובה נכונה: נכון

הערה למורה

מטענים של תוכנת כופר עלולים להתפשט בקלות לגיבויים מקוונים המחוברים לרשת.

7 שאלה 7

תשובה נכונה: לא נכון

הערה למורה

לא נכון: ה-FBI מזהיר ששילום אינו מבטיח שתקבלו בחזרה נתונים כלשהם.

8 שאלה 8

תשובה נכונה: נכון

הערה למורה

נכון: CISA ממליצה לנתק מארחים נגועים או להוריד את הרשת מהאוויר כדי לבלום התפשטות.

9 שאלה 9

תשובה נכונה: לא נכון

הערה למורה

לא נכון: תוכנת כופר מצפינה בדרך כלל קבצים בצפנים סימטריים מהירים כמו AES.

10 שאלה 10

תשובה נכונה: נכון

הערה למורה

בדיקה סדירה של נהלי שחזור נתונים היא חלק קריטי בהתאוששות מאסון.

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

C 1. הצפנה	E 2. מטען נתונים	F 3. גיבוי קר	A 4. בידוד
H 5. כופר	G 6. התאוששות	D 7. אסון	B 8. סוס טרויאני

נקודת ביקורת 3: מפתח תשובות – מונחי מפתח

1 הצפנה	2 מטען	3 גיבוי קר	4 בידוד
5 כופר	6 התאוששות		

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

1 C – גיבויקר	2 H – סוסטרויאני	3 A – הצפנה	4 E – כופר
5 D – בידוד	6 G – אסון	7 B – מטען	8 F – התאוששות

הערות לדיון עבור מורים

מונחי מפתח:
ודאו שהתלמידים מסבירים במילים שלהם את הצפנה, מטען נתונים ו-גיבוי קר ונותנים דוגמה לכל אחד מהם.

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

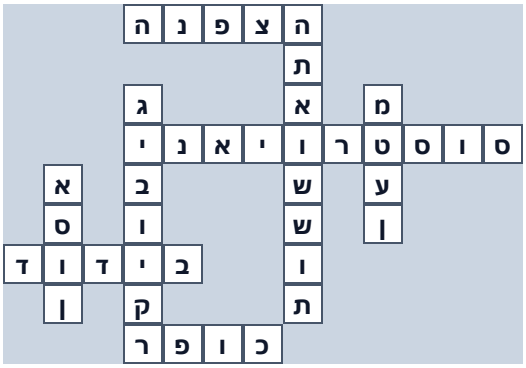
הערכת מקורות:
בקשו מהתלמידים לאמת לפחות טענה אחת במקורות של דף העבודה, ודונו מדוע נתונים, מחירים וכללים עשויים להשתנות עם הזמן.

מפתחות פאזלים והערות למורה

פתרון תפזורת

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

פתרון תשבץ



מדריך למורה לפתרונות התשבץ

מאוזן

1 מאוזן: הצפנה נעילת קבצים בשיטות קריפטוגרפיות (5 אותיות)

4 מאוזן: סוסטרואיאני קובץ זדוני המוסווה כנקי (10 אותיות)

6 מאוזן: בידוד ניתוק מערכות רשת נגועות (5 אותיות)

7 מאוזן: כופר בקשת תשלום תמורת מפתח קריפטוגרפי (4 אותיות)

מאונך

1 מאונך: התאוששות שחזור מסד נתונים מגיבוי (8 אותיות)

2 מאונך: מטען הרצת תוכנה זדונית (4 אותיות)

3 מאונך: גיבויקר עותק מנותק לא מקוון (7 אותיות)

5 מאונך: אסון אירוע של שיבוש מערכתי חמור (4 אותיות)

מפתח פתרונות: מילים מבולבלות ופענוח הצופן

מפתח הערכה לפעילות פענוח מילות אוצר המילים ולאתגר הצופן הסודי.

מפתח פענוח מילים מבולבלות

1. נפההצ — הצפנה
2. גברקיוי — גיבויקר
3. רכפו — כופר
4. וואס — אסון
5. ומעט — מטען
6. ובדדי — בידוד
7. התששותוא — התאוששות
8. נטויסרואס — סוסטרואיאני

מפתח אתגר הצופן הסודי

"שחזרו מערכת נתונים מוצפנת מגיבוי קר"

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.
- 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: הערכת ארכיטקטורות גיבוי לא מקוונות

פתרון למורה

הנחיות הערכה

תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- ניתוח תרחיש: ארגון רוצה לתכנן אסטרטגיית גיבוי שמפחיתה את הסיכון לפגיעה בגיבויים גם אם הרשת המקומית הראשית נחטפה לחלוטין בידי כופרה.
- אסטרטגיה ופתרון מומלצים: יישמו אחסון write-once-read-many (WORM). צרו ניתוק לוגי (air-gap) על ידי ניתוק מערכת הגיבוי מכל הרשתות, ואכפו החלפה יומית של מדיה פיזית.