תרגיל סיום - מבוא לאבטחת סייבר

# מטרת התרגיל

ניתוח מתוך מידע ציבורי של אירוע תקיפה והתמודדות מולו בכדי להוכיח שליטה בחומר הנלמד.

# הנחיות לביצוע התרגיל

* YNET ואירועי חדשות (בעיקר בעברית) אחרים יכולים לשמש מקור מידע אבל לא מקור מידע עיקרי.
* נא לא לבצע העתק/הדבק מאתרי חדשות
* שפת ההגשה עברית
* מאמר בן 3-5 עמודים (אפשר יותר, לא נחוץ) יש לענות על כל השאלות בסעיף 3.
* לכל נקודה מספיקה פסקה או שניים
* הגשת העבודה באמצעות הידעון

# תוצרים נדרשים

מאמר בן 3-5 עמודים (אפשר יותר, לא נחוץ) אשר יכיל את כל הסעיפים הבאים (חובה):

## תיאור האירוע

ניקוד – 50

### האירוע (10 נקודות)

1. שם מקובל לאירוע בקהילת הגנת הסייבר

**C**omputer **E**mergency **R**esponse **T**eam (CERT) : גוף מקצועי שנועד לעזור לארגונים להתמודד עם אירועי סייבר. היא מספקת את השירותים הנחוצים להתמודדות עם אירוע אלקטרוני, ומסייעת בהחלמה והגנה על נזקיה

תאריך התקיפה – באם התקיימו יותר מקמפיין תקיפה אחד, נא לפרט

תאריך התקיפה 10/4/2012

תקף את 217 בנקים ויותר מ 8000 אתרים

והרס המצב הכלכלי של חברות ואתרים בכל רחבי העולם.

תיאור קצר

חמזה בן דאלג 'הוא האקר אלג'יראי, יליד 1988 באלג'יריה, סיים את לימודיו באוניברסיטת באב עזואר למדע וטכנולוגיה באלג'יריה כמהנדס במדיה ממוחשבת בשנת 2008. בן דאלג 'למד תחזוקת מחשבים במשך שלוש שנים, לאחר מכן הוא עבר לעולם ההאקרים, והוא לא עבר את גיל העשרים. המסווג בין ההאקרים המסוכנים ביותר בעולם, כאשר פרץ לאתרי חשבונות בנק ביותר מ- 217 ברחבי העולם, משך כמעט 4 מיליארד דולר וחילק אותם לקבוצת בנקים במדינות עניות כמו פלסטין, ותקף קבוצת אתרים אמריקאית וצרפתית ועצר אותם וגרם להפסדים כספיים אדירים. בשנת 2013 עצרו אותו הרשויות בתאילנד, בשיתוף פעולה עם סוכנות האינטרפול הבינלאומית, בבירה, בנגקוק, באשמת מעורבות בפשעי סייבר על ידי מעצרו בעת חציית שדה התעופה, כיוון שנחשף כי הוא היה אחד מעשר הדמויות המבוקשות ביותר על ידי ה- FBI, כשהיה שם בחופשה עם משפחתו, והוא ליווה אותו. שני מחשבים ניידים ושבב טלפון לוויני תוראיה, בנוסף למספר מנהלי התקנים למחשבים. חמזה הועבר למדינת ג'ורג'יה האמריקאית, שהוציאה נגדו צו חיפוש, בתהליך חקירה שנמשך שלוש שנים. בתורו, דלאג 'הכחיש את טענות הרשויות התאילנדיות כי הוא נכלל ברשימת עשרת האנשים המבוקשים ביותר על ידי ה- FBI, והוא גם הכחיש את כל ההאשמות שהופנו נגדו על ידי ה- FBI, שעוקב אחר צעדיו מזה 3 שנים, ובן דלאג' אמר במסיבת העיתונאים שנערכה כדי להודיע ​​על מעצרו: "אני לא מבוקש ואני לא מחבל."

ה- FBI האשים את הצעיר האלג'יראי בפירטיות של חשבונות פרטיים ב -217 בנקים וחברות פיננסיות ברחבי העולם, והאשים אותו כי גבה סכומי עתק באמצעות פיראטיות של חשבונות אלה. והוא הוסיף כי צבר הון שהוערך בכ -3.4 מיליארד דולר, וכי הרווח החלש ביותר של שוד היה חמזה עם 10 מיליון דולר. דלאג 'תקף גם יותר מ- 8,000 אתרי אינטרנט בצרפת, גרמה לסגירתם, חילקה ויזות בחינם לנוער אלג'יראי ותקפה אתרים רבים בישראל, כמו כן הצליח לדלוף לפלסטינים מידע סודי בצבא הישראלי, וישראל ניסתה לגייס אותו שוב ושוב לטובתו, בתמורה לשחרורו. עם זאת, הוא סירב להצעה זו מספר פעמים.

היו שמועות סותרות על העונש שההאקר האלג'יראי יקבל, וכמה כלי תקשורת אישרו שהוא הגיע לעונש המוות וכי העונש בוצע. אולם שגריר ארה"ב באלג'יריה, ג'ון בלושק, הכחיש את הוצאתו להורג של הפיראט האלג'יראי, חמזה בן דאלג ', שהדגיש כי הפשעים שבוצעו אינם עונשים עונש מוות. עונש המאסר הוא המקסימום שניתן להעמיד לדין. על ההאקרים, הוסיף השגריר האמריקני, כי חמזה הודה בעובדות שיוחסו לו ב- 26 ביוני, כאשר שתל תוכניות זדוניות לחדירת חשבונות כספיים, עד להכרעה סופית בחודשים הקרובים.

1. זהות התוקף וכיצד נקבעה (ייחוס – Attribution)

זהות התוקף :חמזה בן דאלג

הוא נעצר בשנת 2013 על ידי ה- FBI והמשטרה התאילנדית והועבר לידי ארצות הברית של אמריקה,

כאשר העביר 20 מליון דולאר לסניף בנק בתאילנד ואחרי 3 שנים נסע לתאילנד ורצה למשוך את הכסף

ותפסו אותו המשטרה התאילנדית.

### סוג התקיפה (10 נקודות)

1. לדוגמה – כופרה (Ransomware), גניבת מידע, מניעת שירות (DoS / DDoS) ועוד.

גניבת מידע: גניבת מידע מצבא ישראלית ומסירתו לפלסטינים

SYN : התקפה זו מנצלת את לחיצת היד התלת-ממדית של TCP, טכניקה המשמשת ליצירת קשר בין לקוח, מארח ושרת באמצעות פרוטוקול TCP.

בדרך כלל לקוח מגיש לשרת הודעת SYN (סנכרון) לבקשת חיבור.

כאשר מתקפת מבול של SYN, פושעים שולחים שפע של הודעות אלה מכתובת IP מזויפת.

כתוצאה מכך, השרת המקבל הופך לא מסוגל לעבד ולאחסן כל כך הרבה מנות SYN ושולל שירות ללקוחות אמיתיים.

1. האם מכוונת כנגד ארגון מסוים או תקיפה רחבה

היתה תקיפה רחבה ללא לארגון מסוים היתה האחד התיקפות הגדלות בעולם. תקיפה לקבוצת אתרים אמריקאית וצרפתית ועצר אותם וגרם להפסדים כספיים אדירים. ותקיפה מידע מאטרים ישראלים .ותקיפה מעל 200 בנקים בכל רחבי העולם

### הנפגעים (10 נקודות)

1. פירוט של מספר נפגעים עיקריים

217 בנקים בכל רחבי העולם

תקפת יותר מ 8,000 אתרים צרפתים וגרמו להם להיסגר

1. האם היו המטרה או נזק משני?

נזק משני: תקיפה חברות אמריקאית וצרפתית ועצר אותם וגרם להפסדים כספיים אדירים

217 בנקים בכל רחבי העולם וגרם להם להפסיד 4 מליאר דולר

### השיטה (10 נקודות)

1. באיזו טכנולוגיות השתמש התוקף?
   * משפט או שניים לפירוט הטכנולוגיה

**התוקף השתמש ב** טכנולוגיה **HOIC**

שהיא אפליקציה נגישה לציבור אשר החליפה את תוכנית LOIC שהוזכרה לעיל ובעלת פוטנציאל שיבוש גדול בהרבה מקודמתה.

ניתן להשתמש בה כדי להגיש שפע של בקשות GET ו- HTTP POST לשרת במקביל, מה שבסופו של דבר מכה באתרים יעד במצב לא מקוון. התוקף הצליח לתקוף ולסגר יותר מ 8000 אתרים דרך הטכנלוגיה הזו.

1. באילו פגיעויות?
   * משפט או שניים על כל פגיעות שנוצלה

פגיעה בשרתים של אתרים גדולים:

דרך הגשות שפע של הבקשות POST GET , מה שבסופו של דבר מכה באתרים יעד במצב לא מקוון.

### התמודדות הארגון (10 נקודות)

1. מה עשה הארגון בכדי להתמודד מול התקיפה
   * אמצעי הגנה

* זיהוי ומיפוי – IDENTIFY (ID)
* הגנה – ROTECT (PR)
* איתור תקיפה – DETECT (DE)
* התאוששות – RECOVER (RC)
  + זיהוי האירוע

התוקף שולח הודעת SYN מפוברקת דרך כתובות ה- IP של המקור ויעד זהות.

כאשר השרת מנסה להגיב להודעה זו, הוא נכנס לולאה על ידי יצירת תשובות לעצמו או חוזר.

מי מוביל לתרחיש שגיאה, ומארח היעד עשוי בסופו של דבר להתרסק.

וכך מזהים שיש תקיפה

* + טיפול באירוע

צריך להגין על המידע ותהליכים ונהלים ותהליכי תחזוקה

לשתמש בטכנולוגיות הגנה

ניטור שוטף של היבטי אבטחה

פעולות מעקב עבור פעולות התקפה

* + התאוששות (אם בכלל)

•תכנון התאוששות והמשכיות עסקית

•הפקת לקחים ושיפור

•תקשורת פנימית וחיצונית

## ניתוח האירוע

ניקוד – 25

### מטרות התוקף (5 נקודות)

1. מה הייתה מטרת התוקפים?

1. רווח כלכלי הרווח של התוקף 4 מליון דולאר

2. היא גניבת כסף מכול רחבי העולם ושליחה אותו לקבוצת בנקים במדינות עניות .

### השגת מטרת התוקף (5 נקודות)

1. האם הושגה מטרה זו?

כן הצילח לתוקף 217 בנקים ו משך כמעט 4 מיליארד דולר וחילק אותם לקבוצת בנקים במדינות עניות כמו פלסטין, ומספר מדינות אפריקאיות עניות.

### יעילות התקיפה (10 נקודות)

1. הנזק לגוף הנתקף המקורי

תקיפת 217 בנקים ברחבי העולם וגרם להם להפסיד 4 מליאר דולאר

1. הנזק ההיקפי לגופים אחרים

תקיפת קבוצת אתרים וחברות אמריקאית וצרפתית ועצר אותם וגרם להפסדים כספיים אדירים

1. הרווח אם קיים לתוקף

הרווח של התוקף 4 מליון דולאר

### חוות דעתכם על התקיפה (5 נקודות)

* חוות דעתכם על התקיפה מההיבט הטכני בלבד

לפי דעתי תקיפות אתרים וחברות בכול רחבי העולם זה

מוביל להרס המצב הכלכלי בין מדינות ולחבלה ביחסים ביניהם, וכתוצאה מכך זה מוביל למלחמות ביניהן

* ללא התייחסות לנושא זהות התוקף והנתקף או שיקולים מוסריים – ניתן לציין, לא ייתקבל ניקוד עליו.

## המלצות

ניקוד – 20

כיצד הייתם מתמודדים מול אירוע כזה?

כולל היבטים של:

### אמצעי התגוננות למניעת האירוע (5 נקודות)

• צריך לדעת רכיבים קריפטוגרפיים ומערכות היחסים ביניהם סוגי אלגוריתמים סימטריים, א-סימטריים וסיבוב

מנגנוני תשתית מפתח ציבורי (PKI)

• יישום מערכות קריפטוס

• סוגי קריפטאנליזה והתקפות

• פיתוח אדריכלות מערכת פורמלית

• גרעין ואבטחת בסיס מחשוב מהימן

• ארכיטקטורות חומרה ומערכות הפעלה

• ניהול זיכרון והגנה

• אבטחה בתוך וירטואליזציה ומחשוב ענן

• דגמי בקרת אבטחה רשמיים

• קריטריון ודירוג אבטחה

• תהליכי הסמכה והסמכה

### אמצעי זיהוי האירוע (5 נקודות)

מיפוי נכסיםAsset Management (ID.AM)

מיפוי סביבה עסקיתBusiness Environment (ID.BE)

ממשל תאגידיGovernance (ID.GV)

הערכת סיכוניםRisk Assessment (ID.RA)

ניהול סיכוניםRisk Management Strategy (ID.RM)

### תהליך הטיפול באירוע (5 נקודות)

טיפול באירוע באמצעות כלי טיפול ייעודיים

מודיעין ומחקר סייבר של אירועים קודמים ודומים מאפשר לנו טיפול מהיר ויעיל

עצירת המתקפה ומניעת התפשטותה לרבדים נוספים

מתן הנחיות לצוותה IT והעברת המשך הטיפול לידיו

הפקת לקחים מסקנות ושיפור מערך האבטחה בארגון

### תהליך התאוששות (5 נקודות)

גבש סדרה של נהלים שנועדו לשמור על תכניות התאוששות ושיקום כתוצאה מאירוע סייבר. ההחלמה מאפשרת חזרה מהירה לפעולה רגילה תוך צמצום ההשלכות השליליות של תאונת סייבר. תחום זה מתייחס בין היתר להיבטים הבאים: תכנון התאוששות והמשכיות עסקית, שיפורים ותקשורת, הפקת לקחים ושיפור.

## רשימה ביבליוגרפית

ניקוד – 5

רשימה ביבליוגרפית – חובה !