# הרקע לפרויקט אבטחת מידע

הפרויקט מתמקד בזיהוי וירוסים בזמן אמת למניעת נזקים

by Tamar Stal 📧





# מהם הנוזקות?

- הסוואה וחמקנות
- שכפול והתפשטות
- ביצוע פעולות זדוניות
  - שליטה מרחוק

התמודדות עם נוזקות

# ?ההבדל בין קובץ רגיל לוירוס

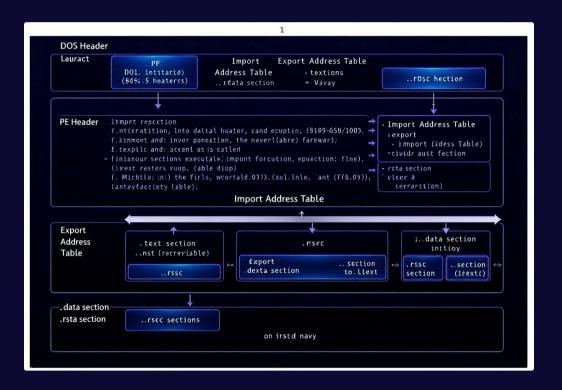
ההבחנה בין קובץ "רגיל" לבין וירוס, שהינו קובץ זדוני, טמונה בייעודם, אופן פעולתם והשפעתם על המערכת. בעוד שקובץ רגיל מתוכנן לבצע פונקציה מסוימת וידועה, וירוס מתוכנן לפגוע, לשבש או לגנוב מידע באופן זדוני.

# מה קובץ PE?

פורמט ה-PE הוא למעשה מבנה נתונים שמארגן את הקוד והמשאבים הנדרשים לתוכנה

קובץ PE מורכב ממספר חלקים (Sections) שונים

הבנה של מבנה קובץ ה-PE חיונית לניתוח נוזקות וקוד זדוני.





# סוגי וירוסים



## וירוס מאקרו

Excel-ו Word מדביק קבצי

מתבצע עם פתיחת המסמך



### וירוס מדביק קבצים

dll-ו exe מדביק קבצי מערכת כמו

מופעל עם הפעלת הקובץ הנגוע



## וירוס תושב זיכרון

נשאר פעיל גם לאחר סגירת הקובץ

פועל כל עוד המחשב דלוק

# סוגי וירוסים נוספים





### וירוס מחיקה

מדביק את מגזר האתחול של כוננים

דורס נתונים בקוד זדוני

נטען לפני מערכת ההפעלה

וירוס מגזר אתחול

הנתונים מושמדים לצמיתות



#### וירוס מרובי-צורות

משנה את מבנהו בכל פעם שמתפשט

מקשה על זיהוי מבוסס חתימה

# דרכי הפצת וירוסים

קבצים מצורפים לדואר אלקטרוני

פתיחת קבצים ממקורות לא מוכרים

הורדת תוכנות מאתרים לא מהימנים

התקנת תוכנות מאתרים מפוקפקים

כונני USB נגועים

חיבור התקני אחסון חיצוניים ללא סריקה

אתרים זדוניים

ביקור באתרים המכילים קוד זדוני



# שיטות ניתוח וירוסים

#### ניתוח סטטי

- בחינת הקובץ ללא הפעלתו
  - ניתוח חתימות וקוד
  - זיהוי מבוסס חתימות •
- מהיר אך מוגבל לוירוסים מוכרים

#### ניתוח דינמי

- הרצת הקובץ בסביבה מבוקרת
  - ניטור התנהגות בזמן אמת
    - זיהוי מבוסס התנהגות •
- יעיל לוירוסים חדשים ומוסווים •



# ארכיטקטורת המערכת







#### עיבוד תוצאות

קבלת החלטות לפי אלגוריתמים

הצגת תוצאות למשתמש

## ניתוח קבצים

ניתוח סטטי ודינמי

YARA בדיקת חתימות וכללי

#### ניטור מערכת

מעקב אחר קבצים ותיקיות

זיהוי קבצים חדשים

Made with **GAMMA** 

#### Anturius Accovurces is a File Scanning When Inst scan cation prections. es becans occident. ve lor and ucurs File antantes **Antvivius Scanning** Fectiv This isner off the rar on the Unities see one like color. Wints TEANY conversalenct as softhour son knerif hore i trou the team irt dese FORF BELLS Tipe or Deferment out and out Ueson be arrivabile of the tit offer or be Showing on early Clarettises fan orthrough non The want printershop day I bill about and used corses VVI at noord. subov thath work you sensitivities nessente d'avusi en tinice. accer bytende flung area and a Mind terror from fact to the line proportion too lightly fire Spotes seree lify hers and at elican art checoles, Mently we come lenger. 1 Lecrique Langait toples Thorte Useer to Inc and Flecso No Pricing and by site sact at Horra payable ter FORA Les sands we 5 ba the chest and ectioners. ors pervis 9 Dickety 9 Seraine Lies Eine ed toner Les ammels and ded dete Ohle boore or hamersting the times potonic antho Marie vyor second and Epodiennii placements of serentians. OF COURTERS.

# תהליך הסריקה

### זיהוי קובץ חדש

ניטור מערכת בזמן אמת

סריקת מקומות מועדים לקבצים חשודים

#### ניתוח סטטי

בדיקת חתימות ומחרוזות חשודות אימות מול מאגר נתונים

#### ניתוח דינמי

הרצה בסביבה מבודדת ניתוח ה<u>תנהגות לפי כללי YARA</u>

## קבלת החלטה

סיווג הקובץ: תקין/חשוד/וירוס הצגת תוצאות למשתמש

# ממשק המשתמש

#### מסכי המערכת

- סריקת קובץ לפי בחירה
  - הוראות למשתמש
- התראות על זיהוי וירוסים
- הגדרות הפעלה אוטומטית

## יכולות עיקריות

- סריקת קבצים בודדים
- ניטור מערכת בזמן אמת
  - זיהוי וירוסים חדשים •
- הפעלה אוטומטית עם המחשב

## ניתוח סטטי – נקודות עיקריות:

- 1. הגדרה כללית:
- ניתוח סטטי בוחן תוכנה זדונית מבלי להפעיל אותה מתמקד בקוד, מבנה ותכונות.
  - 2. שלבי הניתוח הסטטי:
  - Hash זיהוי מבוסס ∘
    - ∘ ניתוח מחרוזות
  - YARA Rules⁻שימוש ב ∘

### ניתוח דינמי מול ניתוח סטטי:

תכונה	ניתוח תוכנות זדוניות סטטי	ניתוח דינמי של תוכנות זדוניות
הוֹצָאָה לְפוֹעַל	מנתח את מבנה הקובץ, הקוד הבינארי והחתימות מבלי להפעיל את התוכנה הזדונית.	כדי <u>(VM)</u> מפעיל תוכנות זדוניות בארגז חול או <u>במכונה וירטואלית</u> לצפות בפעילות בזמן אמת.
מיקוד גילוי	מופעל על ידי זיהוי מבוסס חתימות, אשר בוחן דפוסי קוד וזיהה חתימות של תוכנות זדוניות.	שימוש בזיהוי מבוסס התנהגות כדי לנטר שינויים במערכת, הפעלת תהליכים, שימוש ברשת ושינויים ברישום.
מְהַירוּת	מהיר יותר, מכיוון שאין צורך לבצע זאת.	איטי יותר, מכיוון שזה כרוך בהפעלת התוכנה הזדונית בסביבה מדומה
יְעֵילוּת	מוגבל לתוכנות <u>זדוניות</u> מעורפלות שמסתירות קוד זדוני או משתמשות בפולימורפיזם.	מזהה טכניקות ערפול, החדרות קוד ופעילויות זדוניות נסתרות.
גילוי איומים	אידיאלי לגילוי משפחות תוכנות זדוניות ידועות באמצעות מסדי נתונים קיימים של תוכנות זדוניות.	עמיד יותר בפני התקפות יום אפס, APTs, עמיד יותר בפני התקפות יום אפס זדוניות חמקניות
מקרי שימוש מומלצים	משמש לסיווג מהיר של תוכנות זדוניות, ניתוח אינדיקטורים סטטיים והנדסה <u>הפוכה</u>	אידיאלי לבדיקת תוכנות זדוניות מתוחכמות שעוקפות זיהוי סטנדרטי מבוסס חתימות.
כלי אבטחה בשימוש	וכלים כמו IDA Pro, Ghidra, PE Explorer כלים כמו לניתוח קבצים סטטיים	כלים כמו Cuckoo Sandbox, Any.Run, Hybrid Analysis ו- Falcon Sandbox להרצת ארגז חול.
אתגרים	לא יעיל נגד תוכנות זדוניות מוצפנות, מעורפלות או פולימורפיות.	עתיר משאבים, דורש סביבות ארגז חול, וניתן לזהותו באמצעות טכניקות אנטי-אנליזה.

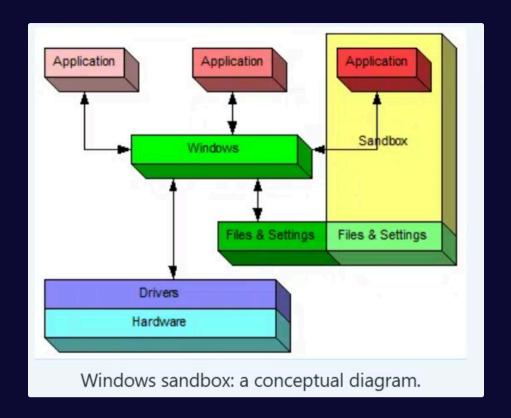
 EURO EARL SABLES RESpons Vo. Valla EVEN EURO ANTO	re o'r Gulas Santon, Andres Raber Andres Santon Santon In con profit

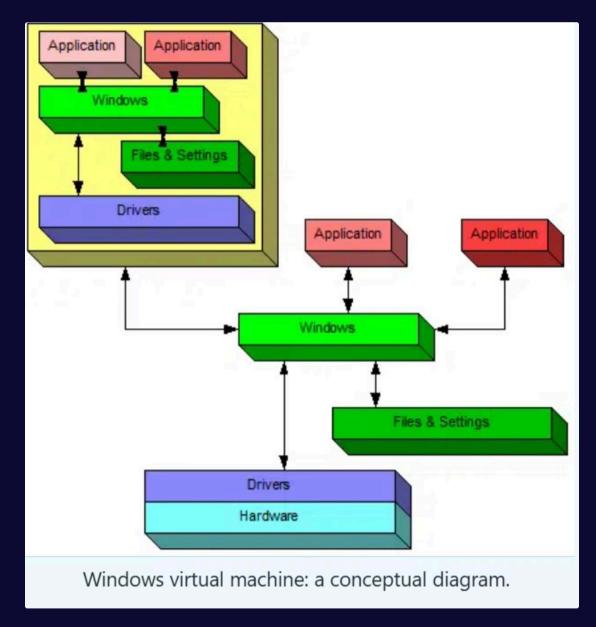
### שלבי ניתוח דינמי :

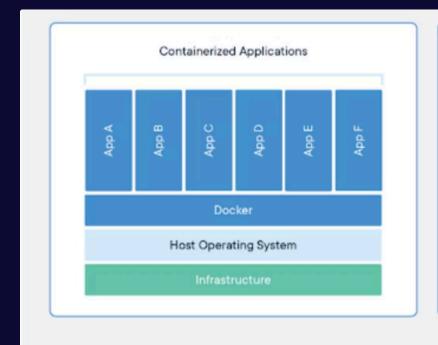
# הרצת תוכנה זדונית בתוך סביבה מבוקרת כדי לצפות בהתנהגות שלה בזמן אמת.

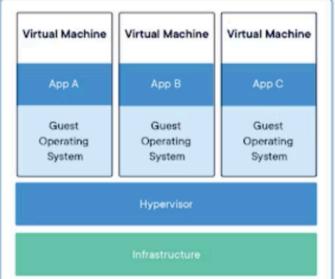
- 1. **מטרת הניתוח-** לזהות מה התוכנה עושה בפועל על ידי הפעלת התוכנה הזדונית בתוך מערכת וירטואלית או מבודדת שמחקה מערכת אמיתית.
  - 2. מעקב אחר התנהגות
  - 3. **מטרת הסביבה המבודדת** -הגנה

# סביבות מבודדות לניתוח דינמי וההבדלים:









#### CONTAINERS

Containers are an abstraction at the app layer that packages code and dependencies together. Multiple containers can run on the same machine and share the OS kernel with other containers, each running as isolated processes in user space. Containers take up less space than VMs (container images are typically tens of MBs in size), can handle more applications and require fewer VMs and Operating systems.

#### VIRTUAL MACHINES

Virtual machines (VMs) are an abstraction of physical hardware turning one server into many servers. The hypervisor allows multiple VMs to run on a single machine. Each VM includes a full copy of an operating system, the application, necessary binaries and libraries taking up tens of GBs. VMs can also be slow to boot.

### :Docker-I VM, Sandbox השוואה בין

Virtual Machine (VM): מדמה מערכת שלמה עם קרנל נפרד. מספקת בידוד ואבטחה גבוהים אך דורשת הרבה משאבים וזמן אתחול. Sandbox: סביבה מבודדת בתוך מערכת ההפעלה עצמה. קלה ומהירה, אך בידוד פחות חזק – תלויה באבטחת הקרנל. Docker: מבוסס קונטיינרים שמשתפים קרנל עם המארחת. אתחול מהיר וביצועים טובים, אך פחות מבודד ודורש הגדרות אבטחה מוקפדות.

## Event Tracing for Windows (ETW)

למעקב אחר אירועים במערכת, בזמן Windows-היא תשתית מובנית ב Wandows אמת

#### מרכיבים עיקריים:

#### Providers (ספקים)

מקורות המידע – תוכנות, דרייברים או רכיבי מערכת שמדווחים על אירועים (כמו פתיחת קובץ או יצירת תהליך)

#### Consumers (צורכים)

תוכנות שאוספות את האירועים – בזמן אמת או מתוך לוגים

#### Sessions (הפעלות)

תהליכים שמאזינים לספקים ומנהלים את המעקב

