הרקע לפרויקט אבטחת מידע

הפרויקט מתמקד בזיהוי וירוסים בזמן אמת למניעת נזקים

by Tamar Stal TS

מהם הנוזקות?

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

התמודדות עם נוזקות

ההבדל בין קובץ רגיל לוירוס?

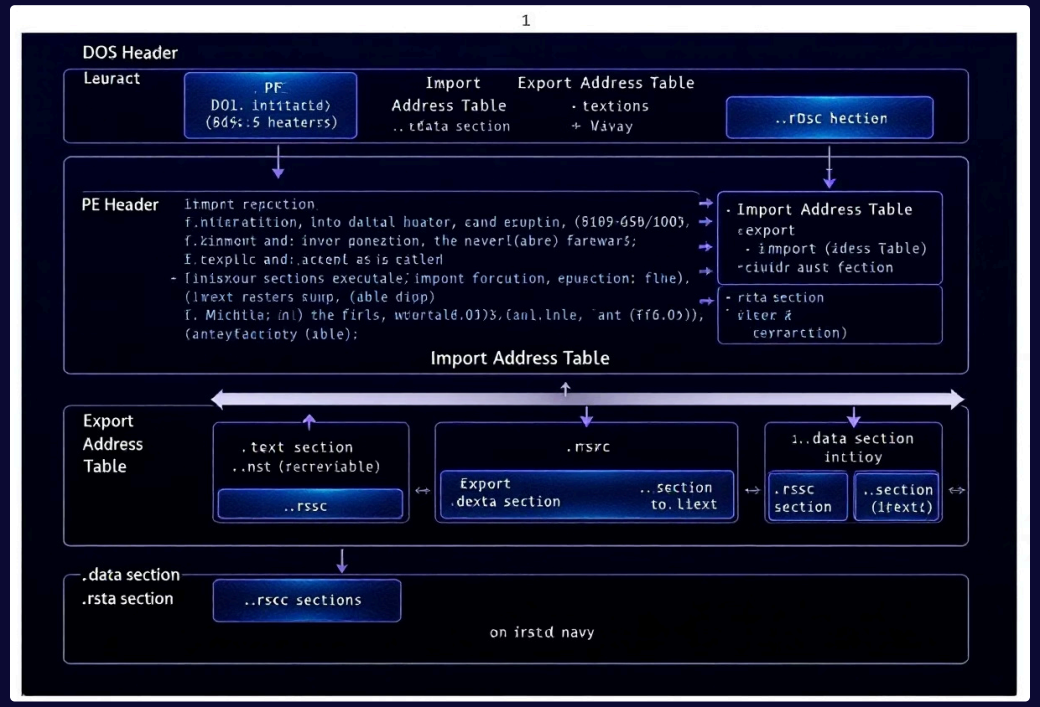
ההבחנה בין קובץ "רגיל" לבין וירוס, שהינו קובץ זדוני, טמונה בייעודם, אופן פעולתם והשפעתם על המערכת. בעוד שקובץ רגיל מתוכנן לבצע פונקציה מסוימת וידועה, וירוס מתוכנן לפגוע, לשבש או לגנוב מידע באופן זדוני.

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 מדביק קבצים

מדביק קבצי מערכת כמו exe ו-dll

מופעל עם הפעלת הקובץ הנגוע

וירוס מאקרו

מדביק קבצי Word ו-Excel

מתבצע עם פתיחת המסמך

וירוס תושב זיכרון

נשאר פעיל גם לאחר סגירת הקובץ

פועל כל עוד המחשב דלוק

סוגי וירוסים נוספים

וירוס מגזר אתחול

מדביק את מגזר האתחול של כוננים

נטען לפני מערכת ההפעלה

וירוס מחיקה

דורס נתונים בקוד זדוני

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 דינמי

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

ניתוח סטטי

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

ארכיטקטורת המערכת

ניטור מערכת

מעקב אחר קבצים ותיקיות

זיהוי קבצים חדשים

ניתוח קבצים

ניתוח סטטי ודינמי

בדיקת חתימות וכללי YARA

עיבוד תוצאות

קבלת החלטות לפי אלגוריתמים

הצגת תוצאות למשתמש

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 התנהגות לפי כללי YARA

קבלת החלטה

סיווג הקובץ: תקין/חשוד/וירוס

הצגת תוצאות למשתמש

ממשק המשתמש

יכולות עיקריות

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

מסכי המערכת

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

ניתוח סטטי – נקודות עיקריות:

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

ניתוח דינמי מול ניתוח סטטי:

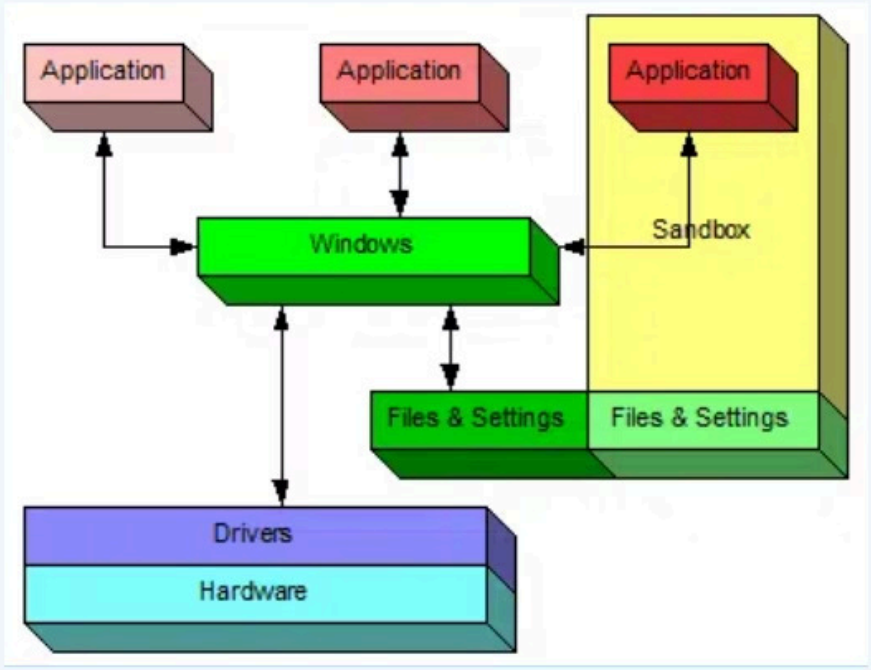
ניתוח דינמי של תוכנות זדוניות	ניתוח תוכנות זדוניות סטטי	תכונה
כדי (VM) מפעיל תוכנות זדוניות בארגז חול או במכונה וירטואלית לצפות בפעילות בזמן אמת.	מנתח את מבנה הקובץ, הקוד הבינארי והחתימות מבלי להפעיל את התוכנה הזדונית.	הוֹצָאָה לְפוֹעַל
שימוש בזיהוי מבוסס התנהגות כדי לנטר שינויים במערכת, הפעלת תהליכים,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

שלבי ניתוח דינמי :

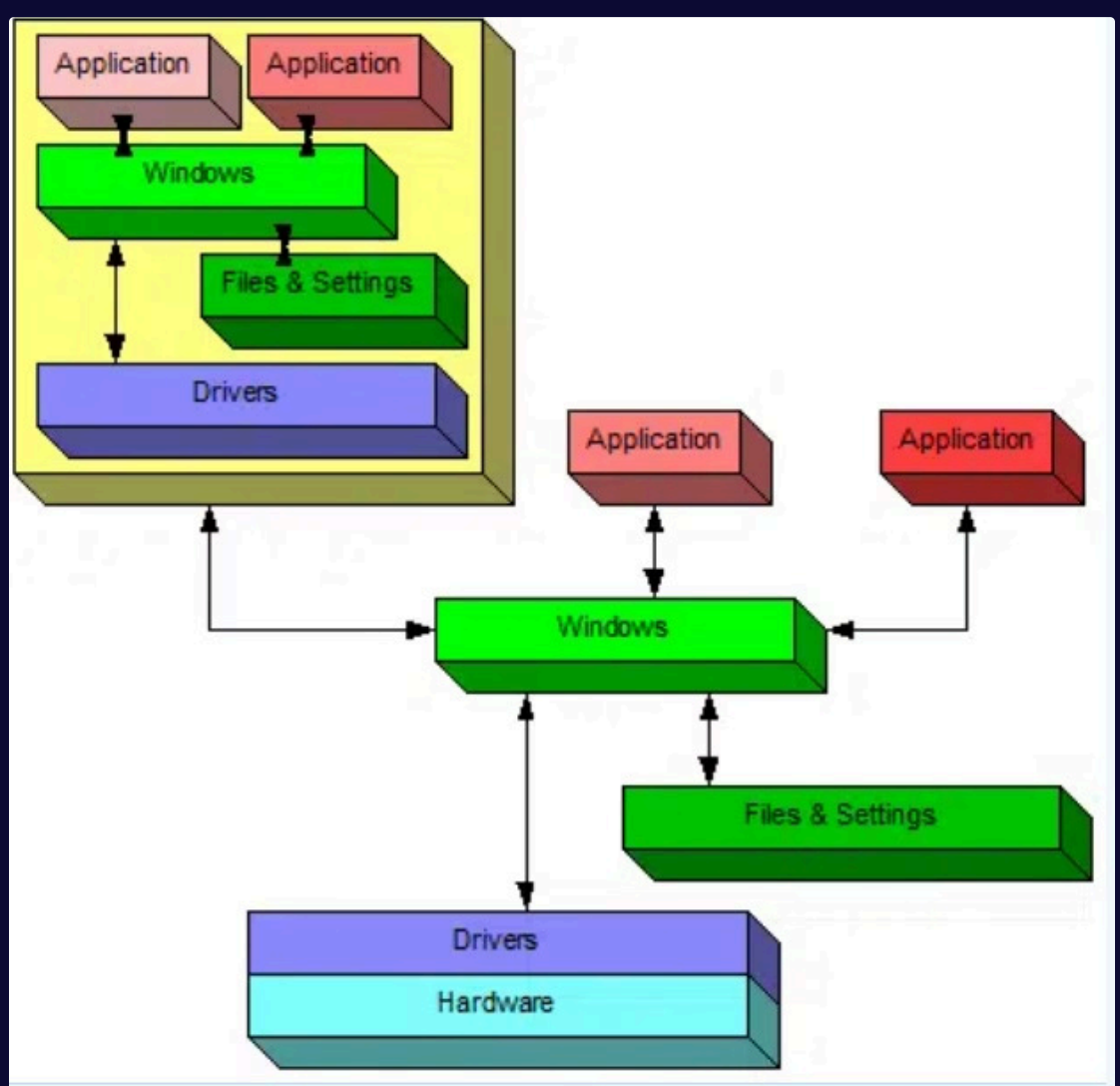
הרצת תוכנה זדונית בתוך סביבה מבוקרת כדי לצפות בהתנהגות שלה בזמן אמת.

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

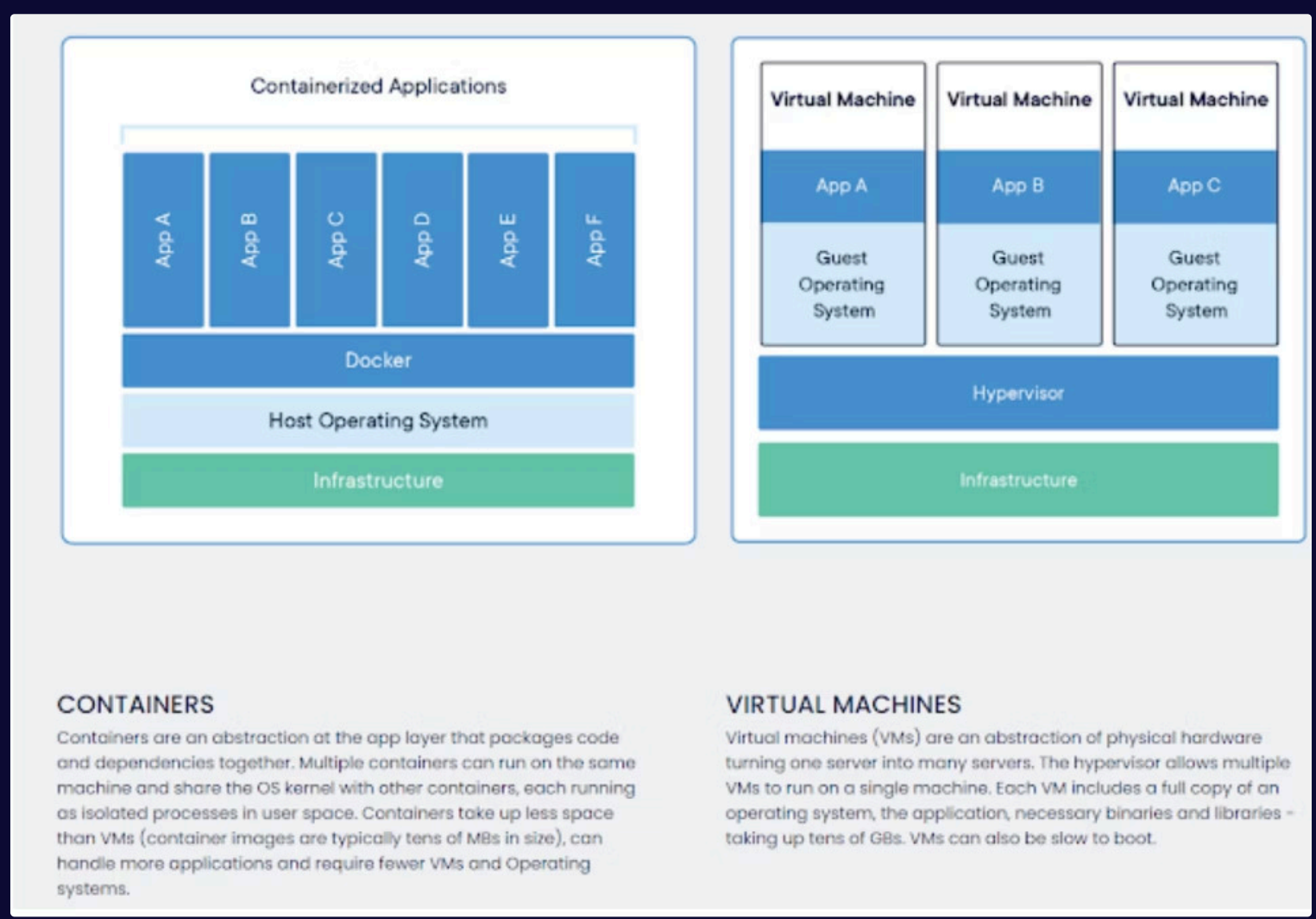
סביבות מבודדות לניתוח דינמי וההבדלים :



Windows sandbox: a conceptual diagram.



Windows virtual machine: a conceptual diagram.



על פי התרשימים שבתמונה, ניתן לראות הבדלים מהותיים בין Virtual Machine ,Docker ו-Windows Sandbox, הן במבנה והן בהיבטי אבטחה

השוואה בין VM, Sandbox ו-Docker:

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 **ETW** 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