תיק עיצוב – פרויקט אישי

DaitO

Detection And Identification Tool

by Ori Rinat

תוכן עניינים

1. יעדים 4

1.1. כללי 4
1.2. לקוח 4
1.3. בעיות 4
1.3.1. בעיות שהמערכת אמורה לפתור 4
1.3.2. בעיות שהמערכת איננה אמורה לפתור 4

2. יישום 5

2.1. אופי ומצב כללי של היישום 5
2.1.1. אופי המערכת 5
2.1.2. סוג המערכת 5
2.1.3. סוג הפעילויות הצפויה במערכת 5
2.1.4. אילוצים כלליים 7
2.2. משתמשים ומערכות משיקות - תיחום חיצוני 7
2.2.1. משתמשי פנים וחוץ 7
2.3. מודולים - תוכניות 9
2.4. מילון פריטי מידע 11
2.4.1. רשימת כל פריטי המידע 11
2.4.2. תיאור מפורט לכל פריט מידע 11

3. טכנולוגיה 13

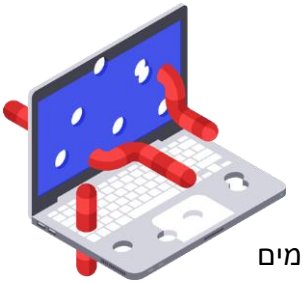
4.1. חומרה מרכזית 13
4.2. מערכת הפעלה 13
4.3. בסיס נתונים 13

4. מימוש 14

5.1. גורם מבצע 14
5.2. פתרון נדרש 14
5.2.1. ספריות 15
5.3. תכנית עבודה מלאה 15

1. יעדים

1.1. כללי



כיום אנו נמצאים בתקופה בה משתמשים מבצעים מיליוני פעולות בשנייה במרכב הדיגיטלי.
רבות הפעמים שקשה לזהות את המשתמש מאחורי המסך אשר מבצע את הפעולה.
לעיתים קיים צורך לזהות את הבן אדם שעמד מאחורי המסך וביצע את הפעולה, כמו לדוגמה במקרה של מבצע פשעי סייבר או כל פעולה אחרת שדורשת בדיקה על המבצע. נכון להיום קיימים כלים שיכולים לעזור לאתר את המבצע של הפעולה מאחורי המסך אך כלים אלו אינם מקיפים ואינם מאפשרים איתור משתמש על פי פרופיל חלקי או מלא.
DaitO מציעה פתרון מקיף לאיתור וזיהוי משתמשים מבוקשים על פי קלט מפרט פרופיל חלקי או מלא וקבלת אופציות אפשריות לזהות ומיקום המשתמש המבוקש.

1.2. לקוח

לקוחות פוטנציאלים של המערכת הם גופים / ארגונים גדולים ואפילו מדינות אשר זקוקים ליכולת מתקדמת של מעקב, איתור וזיהוי משתמשים אשר זהותם אינה ידוע. לדוגמה : בסמ"ח, צה"ל, CIA וכוו.

1.3. בעיות

1.3.1. בעיות שהמערכת אמורה לפתור

תחום	תיאור הבעיה	חשיבות
איבוד עקבות משתמשים מבוקשים	במצב הקיים קשה מאוד לאתר ולזהות משתמשים מבוקשים אפילו אם קיים למחפש מידע שיכול לשמש לבניית פרופיל על המבוקש. במצב זה מבוקשים יכולים לברוח מעונש בקלות.	גבוהה

1.3.2. בעיות שהמערכת אינה אמורה לפתור

תחום	תיאור הבעיה	חשיבות
מניעת פעולות של משתמשים	המערכת אשר תהיה בצד הנבדק הינה אחראית על ניטור, האזנה ובניית פרופיל מלא לנבדק **ולא** אחראית על מניעת פעילותיו.	בינונית
יצירת פרופיל חלקי או מלא	המערכת אינה אחראית על יצירת פרופיל חיפוש למבוקש, מי שאחראי על יצירת פרופיל חיפוש למבוקש הוא המפעיל.	בינונית

2. יישום

2.1. אופי ומצב כללי של היישום

2.1.1. אופי המערכת

חדשה לגמרי, ללא כל זיקה למערכת קיימת (ידנית או ממוכנת).

2.1.2. סוג המערכת

DaitO מורכבת משלושה תת מערכות –

צד נבדק – מערכת מוסוות (Rootkit) אשר מתפשטת בצורה עצמאית ומוסוות (Worm) לכלל המחשבים ברשת

צד שרת – שרת לינוקס מרובה משתמשים

צד מפעיל – מערכת עם ממשק משתמש המאפשרת צפייה וסינון מידע המתקבל מהשרת

2.1.3. סוג הפעילויות הצפויה במערכת

צד נבדק – אין פעילות משתמש, המשתמש אינו מודע לקיום המערכת.

צד שרת – מקבל נתונים מצד הנבדק, אוגר ומתחזק את נתונים המתקבלים וליצירת פרופיל עבור כל נבדק.

בצד המפעיל – Data Entry (הזנת נתונים) ופליטת מידע לאחר חישובים.

2.1.4. מפרט פרופיל נבדק

כאמור, DaitO בצד הנבדק מנטרת מידע שיעזור לאיתור וזיהוי המבוקש. כל המידע שנאסף על כל נבדק מהווה פרופיל המורכב ממספר רב של קטגוריות. פירוט מפרט פרופיל מלא עבור נבדק יחיד :

- **רשת** :
  - **Ip**
    - Ip פנימי או חלק ממנו "192.168.x.2"
    - Ip חיצוני או חלק ממנו "212. x.x.142"
  - **אתר בהם הנבדק ביקר**
    - www.evilsite.com
    - facebook.com/personname
    - ww.bankname.co.lk
- **התנהגות במחשב**
  - **זמנים בהם הנבדק היה פעיל במחשב**
    - 24.05.2019@04:45 — 24.05.2019@12:52
  - **אפליקציות בהן הנבדק השתמש**
    - Safari
    - Vim
    - Curl
    - Gitbash
  - **מילים בהם המבוקש השתמש**
    - Attack

- Cyber
- 317318
- myemail@gmail.com

- **חומרה ותוכנות במחשב הנבדק**
  - **מערכת ההפעלה של מחשב הנבדק**
    - Windows
    - Linux
  - **גרסת מערכת ההפעלה של מחשב הנבדק**
    - 3.1.4
    - 9
  - **ארכיטקטורת המעבד של מחשב הנבדק**
    - Arm
    - ice lake
  - **שם המעבד של הנבדק**
    - i7
  - **יצרן המעבד של מחשב הנבדק**
    - Intel
    - Amd
    - Nvidia
  - **שם כרטיס הגרפי של מחשב הנבדק**
    - Nvidia Titan X
    - AMD Radeon HD
- **ניתוח תוכן קבצי המחשב - File forensics**
  - **קובץ המופיע במחשב בנבדק**
    - test.txt
    - virus.sh
  - **קובץ בעל md5 checksum מסוים**
    - 7ED0097D7E9EE73CF0952A1F0A07C07E
  - **ניתוח קובצי image שבאופן פוטנציאלי יכולים להיות מכונה וירטואליים בהם המבוקש השתמש על מחשב הנדבק**
- **פרטי המבוקש - במידה וכן ידועים פרטים על מבצע הפעולה והמפעיל מעוניין לדעת מאיזה מחשב התבצע הפעולה**
  - **שם ושם משפחה המבוקש**
  - **עיר**
  - **רחוב**
  - **ארץ**
  - **אימייל**
  - **גיל**

כאשר המפעיל במצע חיפוש של מבוקש על פי מודיעין שאסף על המבוקש ממקורות.

המפעיל יכול להכניס ל -DaitO את הנתונים שהוא יודע על המבוקש ובכך למלא את הפרופיל בצורה מלאה או חלקית.

מידה והפרופיל הנתון (מלא או חלקי) עונה על פרופיל הנמצא בממסד הנתונים

של DaitO יוצג למפעיל הפרופיל/ים הנמצאים.

2.1.5. אילוצים כלליים

1. מערכות קיימות בארגון ומחוצה לו: ככל הנראה מערכות דומות או חופפות מפותחות ברגע או כבר נמצאות בשימוש, אולם אין להן השפעה על מערכת זו.
2. סביבה טכנית קיימת או מתוכננת: בזמן פיתוח המערכת, מחשב PC בעל מערכת הפעלה **Linux**.
3. על המערכת להישמר בסודיות מוחלטת, המערכת תופץ לכל המחשבים בארגון / גוף / מדינה כך שכל מחשב יוכל להיבדק על ידי המפעיל, בשביל שמשתמשים לא יחבלו בתקינות הניטור או הנתונים חשוב שהמערכת מצד הנבדק ובכלל תשמר בסודיות מוחלטת.

2.2. משתמשים ומערכות משיקות - תיחום חיצוני

2.2.1. משתמשי פנים וחוץ

משתמש	ספק/צרכן מידע	חיוניות המערכת	תיאור הפעילות
מפעיל	ספק וצרכן מידע	גבוהה	מכין פרופיל חלקי או מלא של המשתמש המבוקש בפורמט נתון. מקבל רשימה של כל המשתמשים העונים על הפרופיל הנתון.
נבדק	ספק מידע	גבוהה	תוכנת צד הנבדק מאזינה ומנטרת נתונים רלוונטיים לאפיון פרופיל המשתמש, את נתונים אלה שולחת לשרת להמשך העיבוד ואחסון.