תוכנה לאיתור וזיהוי מבוקשים

למי מיועדת המערכת :
גופים / ארגונים גדולים / מדינות. לדוגמה : צהל, ישראל, CIA

מטרת המערכת :
איתור וזיהוי מבוקשים על ידי הגוף המפעיל על בסיס פרופיל מלא או חלקי

פרופיל נבדק/מבוקש על פי קטגוריות הבאות :
- רשת
IP
בקשות DNS
- התנהגות במחשב
שעות שימוש במחשב
אפליקציות שבשימוש סדיר
קילוגר, שימוש במילים מסוימות בתקופה האחרונה
- חומרה ותוכנות במחשב
כרטיס גרפי
מעבד
מערכת הפעלה
גירסאות של אפליקציות
- קבצים שנמצאים במחשב
חתימות קבצים
checksum של קבצים
ניתוח קבצי image של הדיסק הנבדק
זיהוי מכונה וירטואלית על מחשב הנבדק וניתוח שלה

צדדי המערכת :
- **צד נבדק :**
בצד זה מותקנת תוכנת שקטה RootKit, אשר יודעת להתפשט למחשבים אחרים - worm/botnet. תוכנה זו מאזינה ומנטרת את מחשב הנבדק לפי הפרמטרים הנבדקים, אשר אותם היא שלוחת בפורמט מסוים לשרת C&C שמאחסן ומטפל במידע.

- **צד שרת :**
צד זה אחראי על קבלת הנתונים מכל הנבדקים באופן שוטף ואחסון הנתונים בצורה נוחה ומהירה לשליפה. כל התעבורה מוצפנת ומוטממת.

- **צד מפעיל :**
בצד זה הקסם מתרחש. כאשר מתקבלת החלטה למצוא אדם או מחשב מכל סיבה שהיא, המפעיל מתחיל לאפיין את פרופיל הנבדק ומעלה בקשה לשרת לקבלת רשימה של אופציות של נבדקים העונים על הפרופיל הנתון.

טכנולוגיות בהן אשתמש לפיתוח המערכת :

צד נבדק :
- Rootkit
- botnet
- worm
- hidden communication - http
- cross platform programming
- encryption
- obfuscating
- OS internals
- keyloogers
- logs readers
- file system analyser
- data forensics
- c++

צד שרת :
- שרת מורבה משתמשים
- DB
- big data
- הסוואה
- SQL
- c++

צד מפעיל :
- פיתוח ממשק ניהול (אולי GUI)
- תקשורת עם השרת
- profiling
- c++