Operating Systems Security Vulnerabilities and Cyber Defenses

תרגיל 1

הגשה – תאריך 04.12.2016

התרגיל ניתן להגשה ביחידים או בזוגות

יש להגיש את כל התשובות במסמך (txt,docx,pdf), במידה וקיימים מספר קבצים יש לארוז את כולם בקובץ zip. התרגיל יוגש למערכות המטלות של האוניברסיטה.

בכל אחד מהתרגילים, הכינו מסמך/קובץ שמסביר מה התשובה וכיצד גיליתם אותה. יש לענות בטקסט ולצרף תמונות של שלבים רלוונטיים.

בתרגיל זה יש להשתמש בכלי Sysinternals (להורדת הכלים ניתן להשתמש בלינק הבא: https://technet.microsoft.com/en-us/sysinternals/bb842062).

חלק א' - מחקר אפליקציות

1. שינוי High Scores

השתמשו ב-process monitor כדי לגלות היכן minesweeper (שמצורף לתרגיל) שומר את ה-high scores שלו ותדאגו לכך שכל הזמנים בטבלת שיאים יהיו מספרים ראשוניים.

2. להריץ תוכנה כמה פעמים

בכל מחשב Windows יש עותק של Windows Media Player , תוכנה זו ניתנת להרצה רק פעם אחת בכל logon session (למה?).

בעזרת process explorer, תגלו מה מונע מהתוכנה לרוץ מספר פעמים ותגרמו לכך שתוכלו לפתוח עוד instance של התוכנה.

3. כל דפדפן שומר cookies, פרטי מידע שאתר אינטרנט יכול לשמור על המחשב שלכם כדי להקל על הזיהוי שלכם. בעזרת process monitor תמצאו את ה-cookie jar של Internet Explorer.

חלק ב' – ניתוח דינאמי וסטטי של נוזקה (Malware Static Analysis & Dynamic Analysis)

בעיה במחקר נוזקות היא הבנה מה בדיוק ה-malware עושה. יש מגוון שיטות לזה, אבל אחת מהן נקראת process stalking והיא מעקב מדויק אחר מה תוכנה עושה מול מערכת הפעלה. הרעיון הוא שבעזרת log מדויק של כל מה שתוכנה עושה (פתיחת קבצים, גישה לרשת, גישה להגדרות) ניתן להבין מה היא עושה מבלי לקרוא את הקוד שלה או להפעיל כלים יותר מסובכים.

יש הרבה כלים שמבצעים process stalking בשיטות שונות. במע"ה Linux עושים את זה מעל כלים כמו strace ו-ltrace, בזמן שב-Windows יש מגוון כלים פומביים ומסחריים. בתרגיל הזה נשתמש ב-process monitor (מבית sysinternals) לבצע את המחקר.

מצורפת לתרגיל תוכנה שמדמה תולעת שמנסה להתפשט ברשת ארגונית. תולעת זו "בטוחה" במובן שהיא לא מקריסה מחשבים וגם לא מפעילה אף כלי שעלול לגרום נזק למחשב.

אנחנו רוצים להבין מה בדיוק התוכנה עושה ברמת הרשת.

הריצו את התוכנה ובעזרת כלים שונים (בעיקר process monitor אך ניתן להשתמש בכלים נוספים מבית sysinternals) ספקו הסבר מפורט ככל הניתן מה התוכנה עושה. דוגמה למידע להוציא – מול איזה שרת הכלי מתקשר, באיזה אופן הוא סורק ידע, איפה קובץ ה-logging נשמר, באיזה שפה הוא נכתב.

<u>הערות חשובות</u>:

- הריצו את התוכנה במכונה וירטואלית בלבד.
- הריצו את התוכנה ברשת ביתית ולא ברשת האוניברסיטה. כדי שהתוכנה תבצע דברים מעניינים כדאי שיהיו גם עוד כמה מכשירים מחוברים.
- יש להריץ את התוכנה עם הפרמטר m0nk3y אחרת היא לא תעשה כלום.
- התוכנה בטוחה לחלוטין.

בונוס: האם יש משמעות לכתובת של שרת ה- C&C[1] של הנוזקה מנסה להתחבר אליו?

בהתאם לרישיון GPLv3, קוד התוכנה יהיה נגיש לכם בסיום התרגיל.

בהצלחה!!!

[1] https://en.wikipedia.org/wiki/Command_and_control_(malware)