שיעור 4 – פרוטוקולים מתקדמים

**תרגיל כיתה: כסף מלוכלך**

פושע הסייבר הבינלאומי 0rphanZ נתפס בשבוע שעבר לאחר שעל פי החשד גנב מאות אלפי דולרים מאנשים ברחבי העולם בעזרת מתקפות מסוג כופר (Ransomware). במהלך החקירה, ניסו אנשי ה-FBI להתחקות אחר כל הכסף אשר הגיע לחשבונו אך לא הצליחו למצוא שום עדות לכך, מלבד פרט אחד קטן – תוכנה להמרות מטבע אשר היתה על מחשבו. אם יצליחו להבין את הפרוטוקול בו היא עובדת, יוכלו לאתר את הסנפות השימוש שלו בה (תעבורת המחשב שלו היתה מנוטרת ע"י ה-FBI), אך לשם כך יש להבין את הפרוטוקול – כאן אתם נכנסים לתמונה. בתיקו של 0rphanz נמצא מדריך לפרוטוקול m0ney אך חלקים ממנו הושמטו. עליכם לבצע תהליך של אבחון – להבין את הפרוטוקול כולו.

**כדי לבצע המרות, כתבו בגוגל: hex to dec / dec to hex**

**1. הסנפה בסיסית**

1. הורידו את קובץ M0neyChange.zip ובצעו Extract לתוכנו.
2. פתחו את תוכנת המרת המטבע ושחקו איתה.
3. נסו להסניף את הפעילות שלה. שימו לב להתחיל את ההסנפה ממש בסמוך לשיגור הבקשה.
4. מהו ה-IP של השרת איתו מדברת התוכנה?

|  |
| --- |
| 34.218.16.79 |
| תשובה |

1. מהו הפורט אליו פונה התוכנה בשרת?

|  |
| --- |
| 101 |
| תשובה |

1. כתבו פילטר המציג את השיחה עם השרת בעזרת פילטור לפי כתובת IP.

|  |
| --- |
| ip.addr == 34.218.16.79 |
| תשובה |

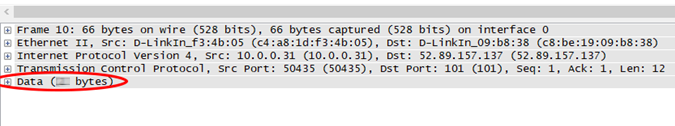
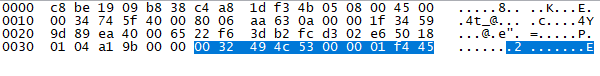
1. כתבו פילטר שונה, המציג את השיחה עם השרת בעזרת פילטור לפי פורט.

|  |
| --- |
| tcp.port == 101 |
| תשובה |

**2. אבחון בסיסי**

1. התחילו הסנפה חדשה. שימרו על הפילטר במקומו כך שתיראו כעת רק את התעבורה שמעניינת אתכם. בחרו סכום המרה, מטבע מקור ומטבע יעד ושגרו בקשה. עצרו את ההסנפה.
2. כתבו את פרטי הבקשה ששיגרתם בתוכנה:

|  |  |
| --- | --- |
| מטבע מקור | **ILS** |
| סכום | **500** |
| מטבע יעד | **CAD** |

1. מצאו בהסנפות את הבקשה אשר שלח הלקוח. כדי לעשות זאת חפשו חבילה יוצאת שיש בה את שורה ה-DATA בחלון האמצעי. זו השורה המייצגת את שכבת האפליקציה. לחצו עליה.
2. הסתכלו על החלון התחתון המציג את המידע של החבילה. המידע המסומן בכחול הוא שכבת האפליקציה בלבד. בעבר החלק הזה היה טקסטואלי והיה לנו קל לקרוא אותו, אך הפרוטוקול m0ney הוא בינארי ולכן חלקו מוצג ע"י נקודות.

מכיוון שהפרוטוקול בינארי, נצטרך לפענח אותו מרצף ההקסא המסומן בכחול. זכרו, כל צמד תווי הקסא מייצג בית אחד.

1. כתבו את הבקשה כולה בהקסא כפי שמופיעה ב-Wireshark:

|  |
| --- |
| 0032000F000001f40004 |
| תשובה |

1. מהו גודל הבקשה בבתים?

|  |
| --- |
| 10 בתים |
| תשובה |

1. חשבו על מספר שאתם מצפים שיופיע בבקשה. המירו אותו בעזרת גוגל לערך בהקסא. כתבו את הערך. האם אתם מזהים את הערך בתוך רצף ההקסא שהסנפתם?

|  |
| --- |
| המספר 500 = 1F4, מופיע בבקשה. |
| תשובה |

1. בתיקו של ההאקר נמצא תיאור של בקשות הפרוטוקול (אשר יוצאות מן הלקוח), אך חלקים ממנו הושמטו. נסו להשלים את החלקים החסרים הצבועים בצהוב. כדי לעשות זאת, היעזרו במידע לגבי הבקשה אשר כתבתם בסעיפים הקודמים בעמוד זה.

|  |  |  |  |
| --- | --- | --- | --- |
| **קוד ההודעה**  (בכל הבקשות שווה ל-50) | מטבע מקור (קוד מספרי) | סכום המרה | מטבע יעד (קוד מספרי) |
|  |  |  |  |
| 2 bytes | 2 bytes | 4 bytes | 2 bytes |

Request (10 bytes)

אם סיימתם, קראו למדריך/ה שיבדוק.

**3. פענוח הסנפות מהעבר**

1. כל הכבוד, פענחתם את הפרוטוקול!

לאחר שה-FBI שמעו שפענחתם את הפרוטוקול, הם העבירו לכם מידע שהוסנף בעבר ע"י האזנות הסתר על המחשב של 0rphanz. לפניכם 3 בקשות שונות שיצאו ממחשבו, עבור כל אחת כתבו מהי פעולת ההמרה שהוא ניסה לבצע.  
תוכלו להיעזר בהמרות בעזרת גוגל (hex to dec / dec to hex).

|  |
| --- |
| 0032000F000001f40004 |
| דוגמא: המרת 500 ממטבע ILS ל-CAD |
| 00320010000088b8001F |
| המרת 35,000 ממטבע INRל-USD (דולר) |
| 0032001F00b71b000006 |
| המרת 12,000,000 מ-USD (דולר) ל-CNY (יואן סיני) |
| 003200090002c114001B |
| המרת 180,500 ממטבע יורו (EUR) לקרונה שבדית (SEK) |

**4. חקר נוסף של הפרוטוקול**

1. כל הכבוד! אבחנתם את הפרוטוקול M0NEY בעצמכם!!
2. ידוע לנו כי קוד ההודעה של הבקשות הוא 50. מהו קוד ההודעה של התגובות?

|  |
| --- |
| 150 |
| תשובה |

1. מהו הסכום הגדול ביותר שניתן לבקש להמיר בתוכנה (חשבו מהו טווח הערכים המקסימלי שניתן לייצג ב-X בתים)?

|  |
| --- |
| מכיוון שהסכום עובר ב-4 בתים, הערך המקסימלי שנכנס ב-4 בתים הוא 322 שזה 4,294,967,296. |
| תשובה |

1. האם לדעתכם הפרוטוקול הואStateless או Stateful? הסבירו.

|  |
| --- |
| הפרוטוקול Stateless – יש בקשה ותגובה וזהו. אין שלבים בתקשורת וכל שיחה מתחילה מחדש. |
| תשובה |

**5. אבחון תגובת השרת**

1. אבחנו את הודעת התגובה של השרת וכתבו אותה כאן:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| קוד ההודעה (בתגובה 150) | מטבע מקור | סכום מקור | מטבע יעד | סכום תוצאה |
|  |  |  |  |  |
| 2 bytes | 2 bytes | 4 bytes | 2 bytes | 4 bytes |

**6. בונוס: אבחון קובץ ההגדרות.**

1. התוכנת M0neyChange משתמשת בקובץ הגדרות בינארי בשם config.bin. נסו לאבחן את המידע הנמצא בו לפי שדות. עבור כל שדה כתוב את גודלו ואת התוכן שלו.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| חלק 4 של IP | | | חלק 3של IP | | | חלק 2 של IP | | | חלק 1 של IP | | | | פורט | |
|  | | |  | | |  |  | | |  | | |
| 1 bytes | 1 bytes | | | 1 bytes | | | | | 1 bytes | | 2 bytes | |