תיעוד למיני פרויקט באבטחת רשתות

נושא המיני פרויקט ומטרתו:

מיני פרויקט זה מתמקד ביצירה של נוזקה מסוג keylogger והרצתה במחשב יעד ספציפי ללא התייחסות בהפצת הנוזקה בין מחשבים שונים.

מטרת הנוזקה:

מטרת נוזקה זו היא תיעוד חשאי של הקשות הקורבן בדפדפני האינטרנט השונים ושליחתן באמצעות דואר אלקטרוני חזרה אל התוקף.

השתלשלות האירועים בשימוש בנוזקה:

1. שימוש ב social engineering על מנת להעביר את הנוזקה אל מחשב היעד (שליחתה במייל כקובץ תמים למראה, העלאה שלה לדיסק און קי או לאתר שיתוף קבצים וליצור הטעיה שתגרום למשתמש להריץ אותה ועוד..) או לחילופין הרצתה הפיזית במחשב היעד של אדם המוכר באופן אישי.
2. לאחר הרצתה הראשונית, הנוזקה מעתיקה עצמה למיקום סודי, ומוסיפה עצמה ל registry ובכך מבטיחה את המשך הרצתה גם לאחר הפעלה מחדש של מחשב היעד.
3. במהלך פעולתה, בכל פעם שהקורבן מקליד תווים כלשהם בתוך חלון של אחד מהדפדפנים הנפוצים (Chrome, Firefox, Explorer), אותן הקשות מתועדות ונשלחות בקבוצות בדואר אלקטרוני הידוע רק לתוקף.

לוח זמנים:

שבועות 1 עד 4 – יצירה של נוזקה פשוטה המתעדת הקשות קורבן בקובץ.

שבוע 4 – מיקוד הנוזקה בתיעוד הקשות מדפדפני אינטרנט בלבד.

שבוע 5 – הפיכת הנוזקה לשרידה במערכת גם לאחר הפעלה מחדש.

שבוע 6 – שדרוג הנוזקה לכדי שליחת הקשות הקורבן בדואר האלקטרוני.

שבועות 6 עד 8 – בדיקת הרצות על מערכות הפעלה שונות ותיקון באגים.

קשיים:

תחילה, הנוזקה יועדה לפגוע במחשבים מבוססים מערכת הפעלה unix תוך הצמדתה לחבילת תוכנה נפוצה ולגיטימית אחרת. בנוסף, הנוזקה תוכננה להגיע בצורה של קובץ מקודד המופעל באמצעות קובץ וירוס אחר המבטל את הקידוד ומריץ אותה.

אם זאת, במהלך העבודה על התכנון המקורי נתגלו מספר קשיים אשר גררו שינוי בתוכנית העבודה המקורית:

1. מספר אנטי וירוסים עליהם נוסה השימוש בקובץ וירוס נוסף, זיהו אותו כחשוד ומנעו את הרצתו. האפשרות לעקוף את אבטחת האנטי וירוסים הללו התגלתה כמאתגרת במיוחד.
2. הצמדה של נוזקה זו לחבילת תוכנה נפוצה ומוכרת, העלתה סוגיות בקשר לחוקיות המהלך שכן נעשה שימוש בכלי אחר ללא אישור. בנוסף, יכולת ההפצה של הנוזקה נפגעה ונתחמה רק לאותם קורבנות אשר ישתמשו בחבילת התוכנה.

3. ריבוי הפלטפורמות במערכות הפעלה מבוססות unix מנעו את האפשרות לבצע בדיקה לנוזקה אשר תגרום לה להתאים לכל הפלטפורמות. בנוסף, בשוק הישראלי מרבית המשתמשים ה"רגילים" נשארים נאמנים למערכת ההפעלה של windows ובשל כך יכולת ההפצה של הנוזקה היה מצומצם ביותר.

בעקבות קשיים אלו, נעשה שינוי מהותי בתוכנית העבודה המקורית אשר גרם למעבר של הפוקוס ממערכות הפעלה מבוססות unix, למערכות הפעלה מבוססות windows (7, 8 ו 10), תוך שימוש בקובץ נוזקה בודד, קל להעברה, המדביק את מחשב היעד.

<u>הרצת הנוזקה:</u>

על מנת להריץ את הנוזקה יש צורך להעתיק את הקובץ dwm.exe אל מחשב היעד (אין חשיבות למיקום), ולהריצו באמצעות לחיצה כפולה.

אל קובץ הנוזקה עצמו, מצורף גם קובץ הקוד בפייתון אשר ממנו נוצרה הנוזקה. קובץ זה מכיל בין היתר את הפרטים לכתובת הדואר האלקטרוני אליה נשלחות ההקשות, המיקום אליו הנוזקה מעתיקה עצמה והערך בregistry אותו היא מוסיפה.

על מנת להפוך קובץ זה לקובץ נוזקה הניתן להרצה, נעשה שימוש בתוכנת py2exe אשר איננה מצורפת בחבילת הנוזקה.