Operating Systems Security Vulnerabilities and Cyber Defenses

תרגיל 3

תאריך הגשה –

התרגיל ניתן להגשה ביחידים או בזוגות

תרגיל Hooking

בתרגיל זה תכתבו Hook וגם תתארו דרך להגן בפני הקוד שכתבתם.

רקע

לצורך ניטור מע"ה נרצה לא פעם לעשות Interception לפונקציות API ולעקוב אחר מה תוכנות שונות עושות.

דוגמה לצורך לגיטימי, Chrome מחליף עושה Interception (שם נרדף ל-Hooking) לעצמו, כדי לעקוב אחר פניות למע"ה ולבדוק שהם לגיטימיות ובכך למנוע תקיפות שיגרמו לדפדפן לפנות למע"ה באופן לא לגיטימי (נניח לפתוח קבצי משתמש).

בתרגיל זה נממש מנגנון Hooking גנרי שידווח לנו מה תוכנות עושות ובו זמנית נכתוב קוד שיזהה האם יש Hook על פונקציות מע"ה.

דרישות תרגיל

עליכם לכתוב תוכנה אשר תבצע Hook ל-CreateFileW בכל התוכנות הנגישות לה, כל Hook יכתוב את שמות הקבצים שהתוכנה פונה אליהם לקובץ בעל השם [Pid].log שיכתב לתיקייה C:\temp.

הפלט יהיה בפורמט של שם קובץ וירידת שורה.

כלומר, בהינתן 3 תוכנות רצות, (Notepad (PID=337), Explorer (PID=35), ShareX(Pid=12512 יווצרו 3 קבצים בשמות 337.txt, 35.txt, 12512.txt.

כאשר תוכן אחד מקבצים יכול להיות

Desktop.ini

folder.jpg

driverquery.txt

וכך אלאה ללא צורך ב-header.

שימו לב למספר דברים

1) הדרישה היא לבצע Hook רק לתהליכים שיש לכם גישה אליהם. כלומר אם אתם עוברים על כלל התהליכים במע"ה (דוגמה מ-MSDN) ואז לנסות לפתוח אותם לגישה כלשהי (OpenProcess) והתהליך נכשל, אז אין צורך "להתחכם" ולהשיג גישה.
2) לא חסר חומר עזר על הנושא מהקורס (מצגת 0x9), חלק באינטרנט עיתון Digital Whisper הישראלי)

הגשה

עליכם להגיש שתי דברים

1) קוד עובד (תבחרו שפה) שמבצע Hooking לפי הדרישות
2) הסבר **טכני** כיצד תוכנה יכולה לזהות שבוצע לה Hooking לפונקציות מע"ה.

יינתן בונוס למי שיראה שהשיטה שלו עובדת על API-ים ציבוריים שאינם CreateFileW על ידי כתיבת קוד מתאים שמבצע hook לפונקציית מע"ה נוספת.

יינתן בונוס נוסף למי שתכתוב תוכנה שתזהה שבוצע Hooking לפונקציות מע"ה שלה.

תזכורת יש להגיש בקובץ ZIP בצירוף מספר תעודת זהות.

הערות לבדיקה

כקודם, על הקוד לעבוד על Windows 7 32-bit