Signature-based Detection Bypass

מאת הרצל לוי / InHaze

הקדמה

מוצרי אנטי-וירוס למשתמשי קצה התפתחו מאוד לכאורה בעשור האחרון, אך עד היום, רובם מבוססים על מנגנוני איתור חתימות. חתימה לצורך העניין, היא רצף בתים מסוים מתוך הקובץ שאותו מסמנים כקובץ בעל תוכן זדוני. מנגנוני האיתור סורקים קבצים שנמצאים על הדיסק וגם את מרחב הזיכרון. חשוב לציין שבמאמר זה, אציג ואדגים שיטות לעקיפת מנגנוני איתור חתימות ולא מנגנונים אחרים (כגון מנגנונים היוריסטיים) שבהם גם משתמשים מוצרי אנטי-וירוס.

כדי להבין טוב יותר מהי חתימה והיכן אפשר למצוא אותה, חשוב להכיר את המבנה הכללי של קובץ ההרצה (PE = Portable Executable).

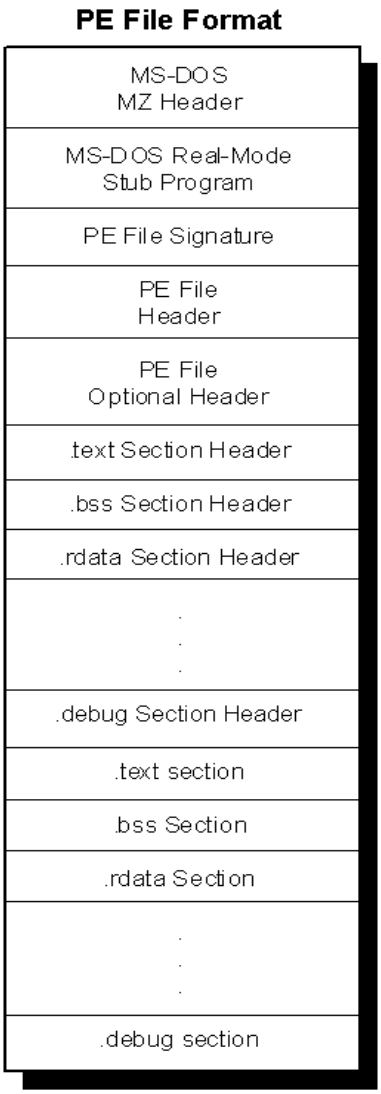
מבנה קובץ PE

בויקיפדיה יש הסבר מצוין על מבנה ה-PE:

"פורמט PE מורכב ממספר מבני נתונים שמופיעים אחד אחרי השני בתוך הקובץ. מבנה הנתונים הראשון נקרא DOS Header . מבנה זה זהה לפורמט ששימש את מערכת ההפעלה DOS עבור קבצי הרצה. בדרך כלל המבנה מכיל תוכנית קטנה שמדפיסה שורה המורה למשתמש שהתוכנה מיועדת למערכת ההפעלה חלונות, ויוצאת.

לאחר מכן מופיעים שני מבנים נוספים File Header ו-Optional Header שמכילים מידע עבור מערכת ההפעלה, כמו: סוג המעבד וגרסת מערכת ההפעלה שעליהם התוכנה מיועדת לרוץ, מספר המחלקות בקובץ, הכתובת שממנה מתחילה ריצת התוכנה ותכונות שונות של הקובץ. שאר הקובץ בנוי ממחלקות שונות, בהן: מחלקת הקוד (text section. באיור) שבה נמצא קוד ההרצה של התוכנה, מחלקת הנתונים (bss section. באיור) שבה נמצאים המשתנים בהם התוכנה משתמשת, מחלקת המשאבים (rdata section. באיור) שבה מוגדרים תפריטים, תיבות דו-שיח, סמני עכבר וכו'."

או באופן מופשט יותר:



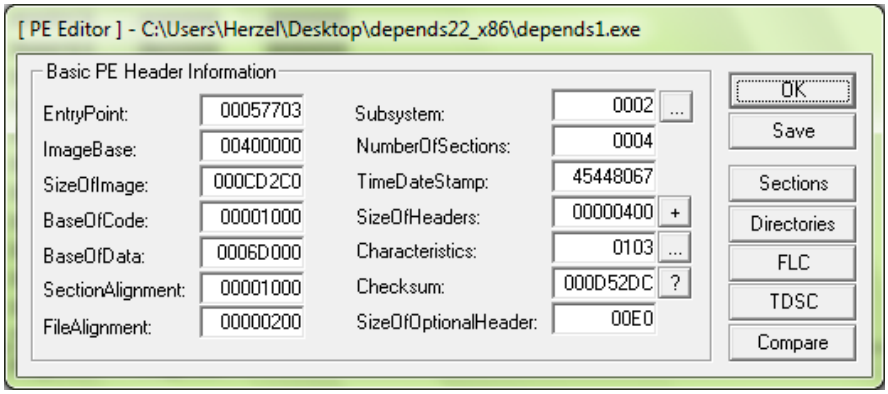
(מקור: http://www.skynet.ie/~caolan/pub/winresdump/winresdump/doc/pefile.html)

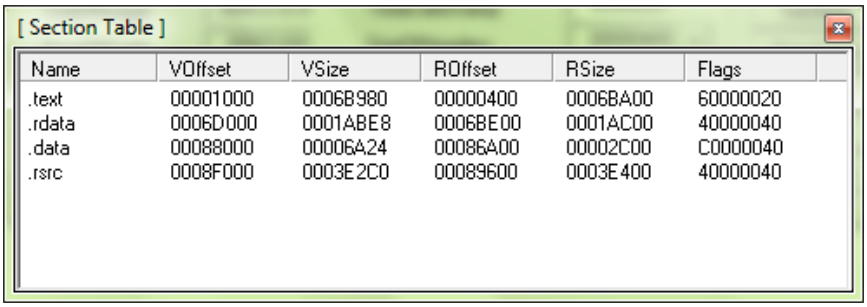
בגליון השמיני של Digital Whisper, יוסף רייסין פרסם מאמר בשם "קבצי הרצה בתקופות השונות" - מומלץ לעבור עליו בכדי להבין טוב את הנושא.

חתימות ומבנה קובץ ההרצה PE

חתימה יכולה להופיע בכל אחד מהמבנים הנ"ל, לכן לפני שאציג את השיטות לשינוי חתימות, צריך לדעת באיזה מבנה (או מבנים) נמצאת החתימה, כדי להשתמש בדרכים הרלוונטיות לשינוי החתימה. שיטה פשוטה לאיתור החתימה היא פיצול הקובץ לחלקים קטנים (ידנית או ע"י אינספור תוכנות לפיצול קבצים שפזורות באינטרנט) וסריקה של כל חלק ע"י האנטי-וירוס שאותו רוצים לעקוף (למרות שאותו קובץ מזוהה ע"י מספר תוכנות אנטי-וירוס, סביר להניח החתימה של הקובץ היא שונה בכל אנטי-וירוס). השיטה המועדפת עלי היא בצורה של חיפוש בינארי: פיצול הקובץ לשניים כל פעם, סריקה של החלקים ואז שוב פיצול לשניים של החלק שעליו האנטי-וירוס התריע. ממשיכים בפעולה זו עד שהאנטי-וירוס כבר לא מתריע יותר על החלקים, שזה אומר שכנראה הפיצול האחרון פיצל גם חלק מהחתימה. כלומר - החתימה נמצאה.

לאחר שהחתימה נמצאה ע"י השוואת תווים ניתן לדעת את הסטייה מתחילת הקובץ. כדי לדעת בנוסף באיזה מבנה החתימה נמצאת אפשר להשתמש בעורך ה- PE של התוכנה LordPE:





מה שמעניין במקרה זה הוא ה-ROffset (Raw Offset) - ההיסט של המבנים מתחילת הקובץ (המבנים DOS Header, File Header, ו-Optional Header נמצאים לפני המבנה הראשון שמצוין ב- Section Table).

כפי שציינתי קודם, חשוב להכיר את מבנה ה-PE. אופן שינוי החתימה קשור למיקום החתימה. ישנם חלקים ב- PE שאינם ניתנים לשינוי, או חלקים ששינויים עלול לגרום ל-PE להיות פגום ובלתי ניתן להרצה. למשל, אם נשנה את ה-EntryPoint שנמצא ב- Optional Header, נגרום לכך שה- PE יתחיל לרוץ מכתובת שונה, דבר שעלול לגרום לשגיאת ריצה. מצד שני, ישנם חלקים ב- PE שמשותפים כמעט לכל PE, כמו המחרוזת "MZ" (Magic Bytes), לכן כנראה שחלקים אלו לא יהיו חלק מהחתימה. חתימה שנמצאת במחלקת הקוד, היא קטע קוד מכונה (opcode) והיא ניתנת לשינוי ע"י עריכה או החלפת הקוד הקיים בצורה שלא תשפיע על פונקציונאליות הקוד.

למרות שזה יכול להיות מסובך לפעמים לשנות חתימה, הרבה פעמים זה גם מאוד פשוט. חשוב לזכור שחתימה של קובץ חייבת להיות ייחודית, דבר שמאוד מגביל את יוצרי החתימות של חברות האנטי-וירוס. ישנם קטעי קוד שהם מאוד נפוצים ובלתי ניתנים לחתימה מכיוון שהם ייצרו הרבה התרעות שווא (False-Positives). כתוצאה ממגבלה זו, הרבה פעמים החתימה מורכבת ממחרוזות ייחודיות שנכתבו ע"י יוצר ה-PE (במיוחד מחרוזות כגון "Coded by Hack3r"), לכן שינוי מחרוזות כאלו קודם, יכול לחסוך הרבה זמן.

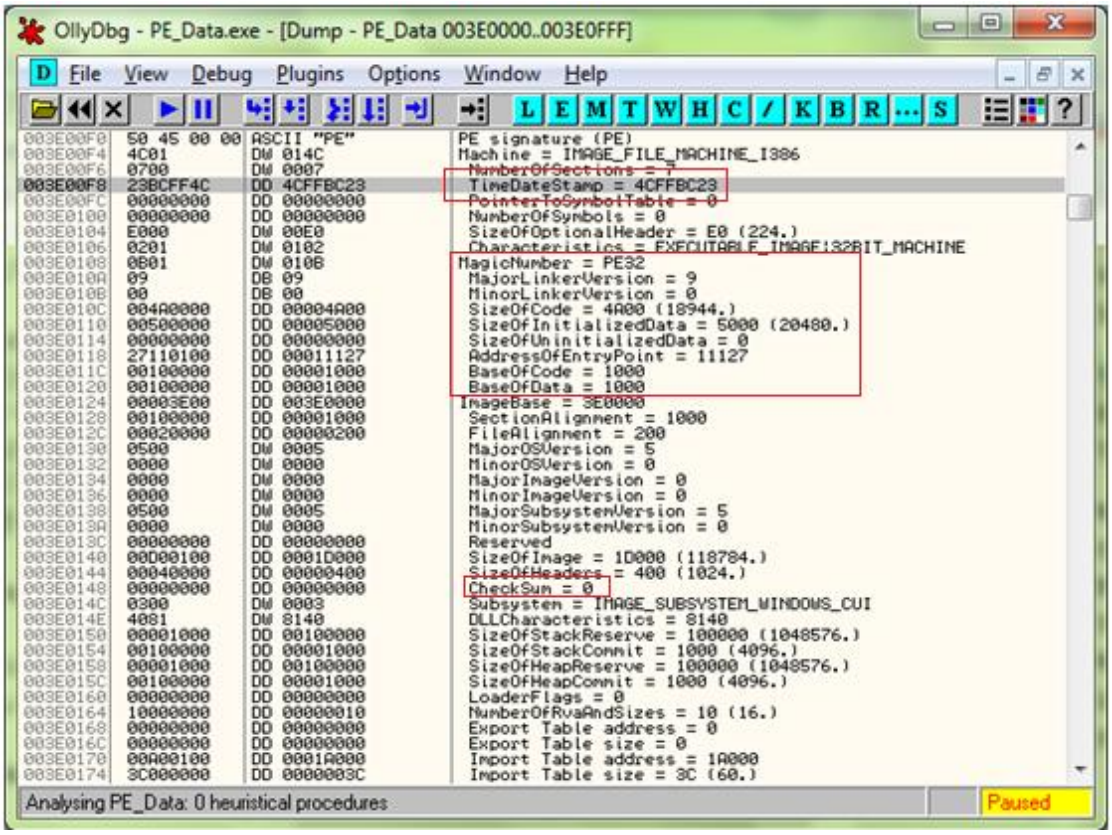
שיטות נוספות לשינוי חתימות

קיימות מספר רב של שיטות לשינוי חתימות שאפשר להשתמש בהן. שיטות אלו רלוונטיות בד"כ לשינוי חתימה שנמצאת במבנה מסוים ב-PE. השיטות הנפוצות הן:

1. **שינוי קוד המקור של התוכנית, שמות משתנים ומחרוזות** – רלוונטי לחתימה שנמצאת במחלקת הקוד, הנתונים ומחלקת המשאבים.

2. **עריכת משאבי ה-PE** – ידנית או ע"י תוכנות כמו Resource Hacker - רלוונטי לחתימה שנמצאת במחלקת המשאבים.

3. **שינוי מאפייני קובץ PE** – שינויים כגון חותמות זמן (time stamps), גדלי מחלקות, כתובות של מחלקות – רלוונטי לחתימות שנמצאות במבנה ה-File Header. דרך אחת לעשות זאת היא ע"י OllyDbg:



הערה: צריך לזכור ששינויים בחלק זה של הקובץ עלולים לגרום לכך שהקובץ יהיה פגום ובלתי ניתן להרצה, מצד שני חלק מהעניין הוא גם ניסוי וטעייה.

4. **אריזת/קידוד קובץ ה-PE** - הלל חימוביץ' מסביר מצוין את הנושא בגיליון הראשון של Digital Whisper:

http://www.digitalwhisper.co.il/files/Zines/0x01/DW1-2-ManualPacking.pdf

שיטת אריזת הקובץ רלוונטית לחתימה שנמצאת במחלקת הקוד, הנתונים ומחלקת המשאבים.

5. **Binary Obfuscation** – זהו שם כללי לנושא מאוד רחב של שיטות לשינוי המבנה או חלקים בקובץ ה-PE בצורה שלא תשפיע על הפונקציונאליות של אותו קובץ. מדובר כאן בעיקר על

שינויים במחלקת הקוד של ה-PE ישירות או בעקיפין ע"י שינויים בקוד המקור. הסבר ודוגמאות על הנושא ניתן למצוא במאמר מצוין מהאתר Tuts4You:

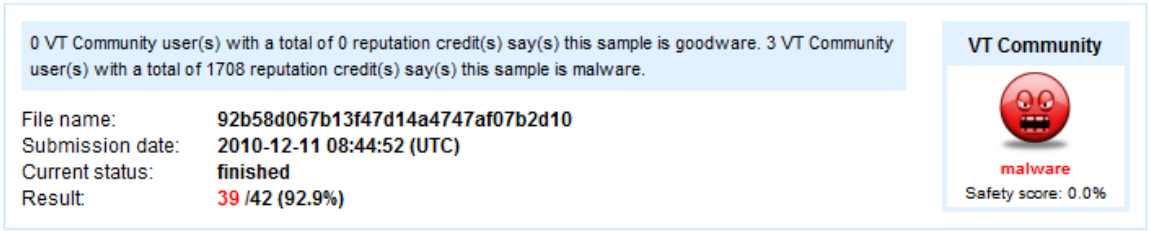
http://tuts4you.com/download.php?view.2979

6. **קוד פולימורפי** – קוד שמשנה את צורתו אך לא את הפונקציונאליות שלו בכל הרצה – רלוונטי לחתימות שנמצאות במחלקת הקוד.

סדנה מעשית: שינוי חתימה של התולעת Zbot ע"י אנטי-וירוס מבית Symantec

Zbot זו תולעת שנשלטת ע"י רשת הבוטים הידועה לשמצה בשם Zeus, בחרתי דווקא בתולעת זו, מכיוון שהיא מוכרת ונפוצה מאוד, אך יותר בכדי להראות עד כמה זה פשוט לפעמים לשנות חתימה. דרך אגב, כאשר הקובץ שלו רוצים לשנות את החתימה הוא זדוני, הרבה פעמים הוא כבר ארוז (packed) ע"י Packer כלשהו, עניין שיכול להקשות או להקל על תהליך שינוי החתימה.

נניח שעל מחשב המטרה שלנו, שאותו אנו רוצים להדביק, מותקן אנטי-וירוס מבית Symantec. נעלה את התולעת שלנו ל-VirusTotal כדי לבדוק קודם כל אם היא מזוהה ע"י האנטי-וירוס:

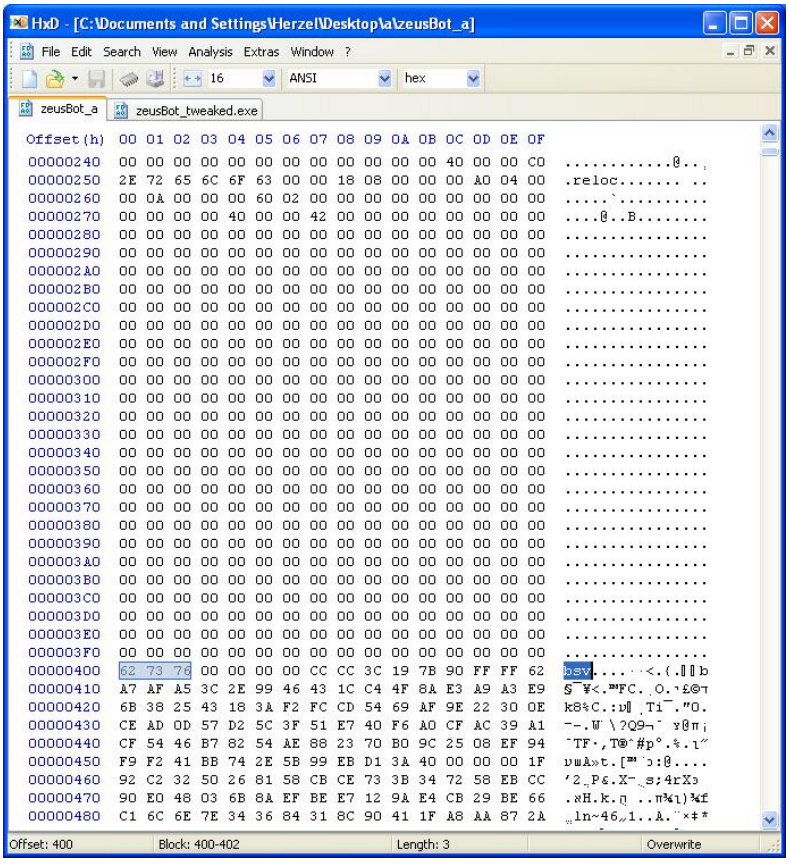


אין ספק, הקובץ מזוהה והוא אכן Zbot:

SUPERAntiSpyware	4.40.0.1006	2010.12.11	-
Symantec	20101.3.0.103	2010.12.11	Infostealer
TheHacker	6.7.0.1.098	2010.12.11	Trojan/Spy.Zbot.alcg
TrendMicro	9.120.0.1004	2010.12.11	TSPY_ZBOT.CGA

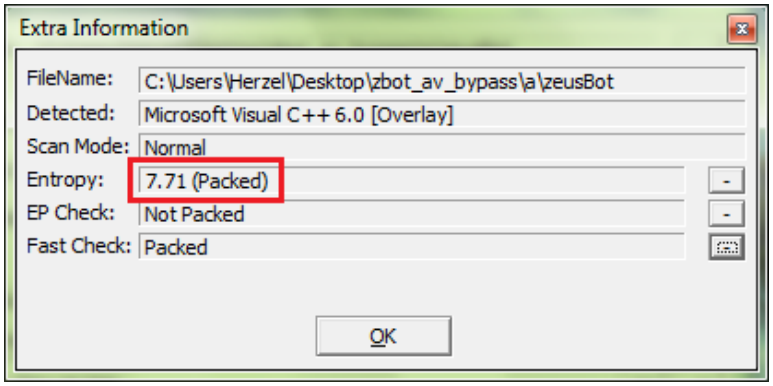
נפעל לפי השיטה שציינתי קודם לכן: פיצול הקובץ לשניים וסריקה של שני החלקים. נפצל שוב את החלק שזוהה ע"י Symantec לשניים ונסרוק שוב. הפעם, אחרי סריקה של שני החלקים לא נמצאה החתימה, מה שאומר ש**הפיצול האחרון, פיצל גם חלק מהחתימה**. לאחר השוואה של קטע התווים שמסביב לפיצול האחרון, נמצא שהחתימה נמצאת בין ה-Section Headers לסגמנט הקוד שמתחיל מהיסט 400!

נפתח את הקובץ המפוצל האחרון שהכיל את כל החתימה בעזרת Hex Editor:



הדבר הראשון שקופץ לעין הוא המחרוזת "bsv" שנמצאת בתחילת סגמנט הקוד. ניתן לראות שעד הסיט 400, אין תווים חשודים לחתימה. כפי שציינתי קודם, מחרוזות של תווים אלפא-נומריים הן חשודות

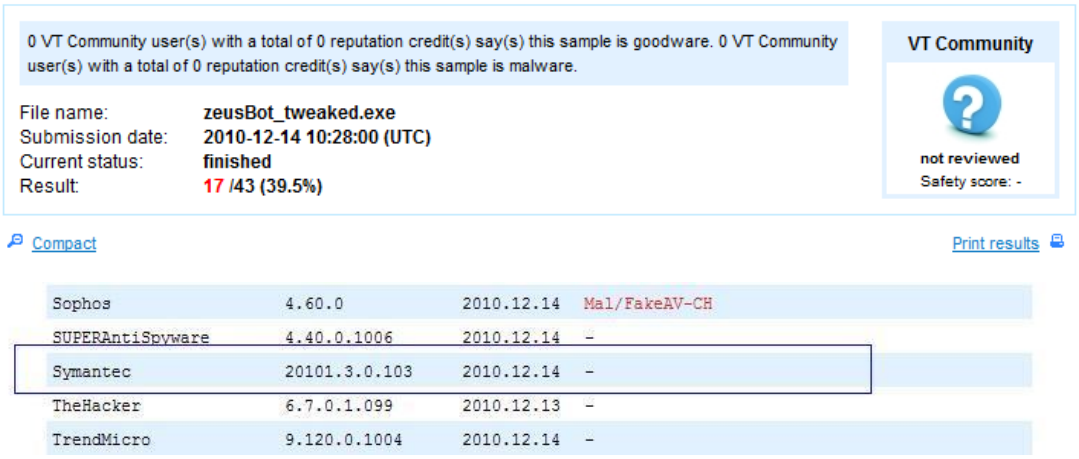
מיידיות. מחרוזת זו, היא ככל הנראה חתימה של Packer מסוים שבו השתמשו יוצרי התולעת לקודד את סגמנט הקוד. כדי לבדוק האם ה-PE ארוז אפשר להשתמש בתוכנה PEiD:



כנראה שה-PE ארוז והמחרוזת bsv היא חלק מהחתימה של אותו Packer. נשנה את החתימה ונסרוק שוב את הקובץ:

```
000003E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000003F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000400  61 61 61 00 00 00 00 CC CC 3C 19 7B 90 FF FF 62  aaa.....·<.{.ÿÿb
00000410  A7 AF A5 3C 2E 99 46 43 1C C4 4F 8A E3 A9 A3 E9  §¯¥<.™FC.ÄOŠã©£é
00000420  6B 38 25 43 18 3A F2 FC CD 54 69 AF 9E 22 30 0E  k8%C.:òüÍTi¯ž"0.
00000430  CE AD 0D 57 D2 5C 3F 51 E7 40 F6 A0 CF AC 39 A1  Î-.WÒ\?Qç@ö Ï¬9¡
00000440  CF 54 46 B7 82 54 AE 88 23 70 B0 9C 25 08 EF 94  ÏTF·‚T®ˆ#p°œ%.ï”
```

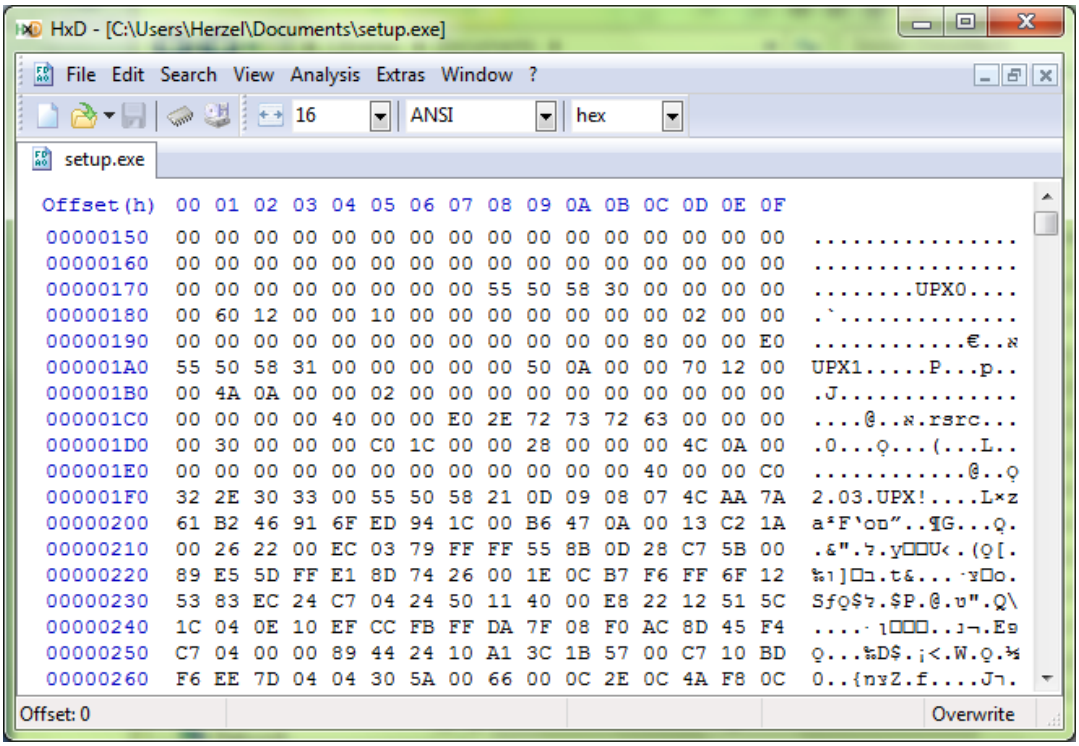
התוצאה לאחר הסריקה:



שינוי המחרוזת גרם גם לשינוי החתימה של Symantec, ביחד עם עוד כמה מוצרי אנטי-וירוס נוספים (22 מתוך 42!).

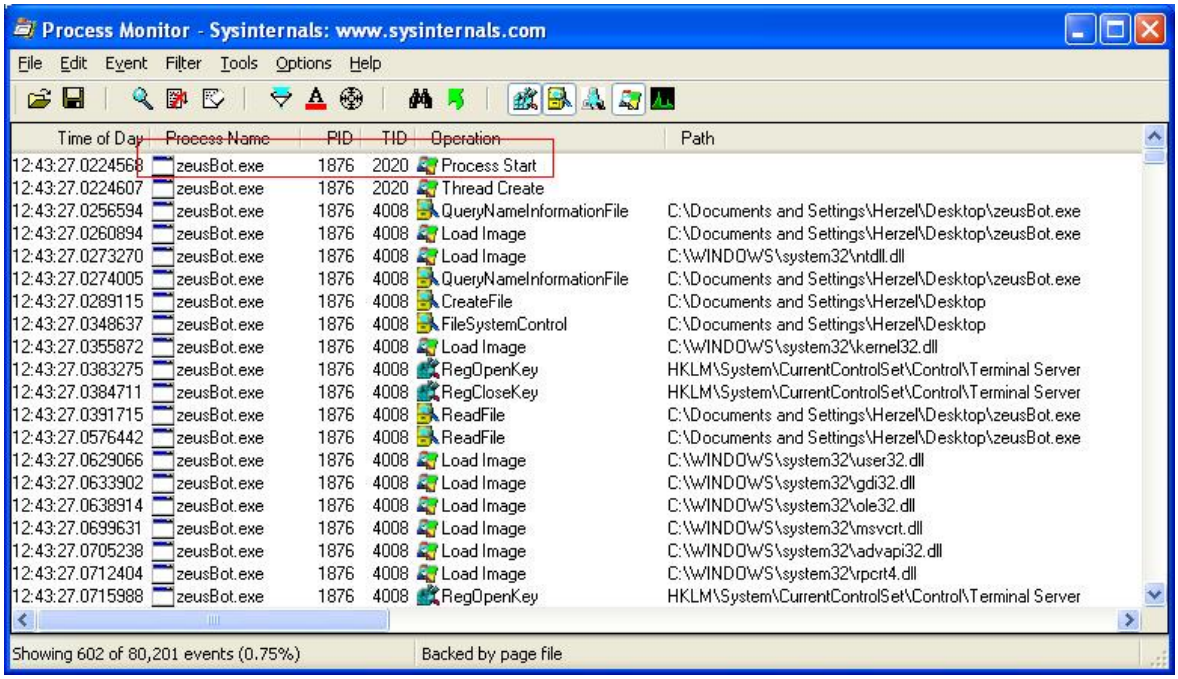
למה Symantec ושאר מוצרי האנטי-וירוס חותמים דווקא את ה-Packer? כדי שהם ידעו לפענח את המידע הארוז/מקודד, הם צריכים לדעת באיזה Packer יוצרי ה-Malware השתמשו. כאשר משנים את החתימה של ה-Packer, האנטי-וירוס אינו יודע כיצד לפענח את המידע (ספק אם הוא יודע שהמידע מקודד בכלל).

דוגמה לקטע מקובץ שארוז בעזרת UPX:



מה אתם הייתם משנים כדי שהאנטי-וירוס לא יזהה שזה UPX Packer? ☺

כל שנותר הוא לוודא שתוכן קובץ התולעת אינו פגום והתולעת רצה כמו שצריך:



סיכום

מוצרי אנטי-וירוס למשתמשי קצה ברובם עדיין מתבססים על מנגנוני איתור חתימות, מנגנונים שאינם דורשים מיומנות גבוהה כדי לעקוף אותם. כיום עדיין לא ניתן להתבסס על הגנת האנטי-וירוס בלבד וצריך לנקוט באמצעי הגנה וזהירות נוספים. מאמר זה בן היתר בא להציג את הפשטות היחסית שבה ניתן לעקוף מנגנוני איתור חתימות של מוצרי אנטי-וירוס.