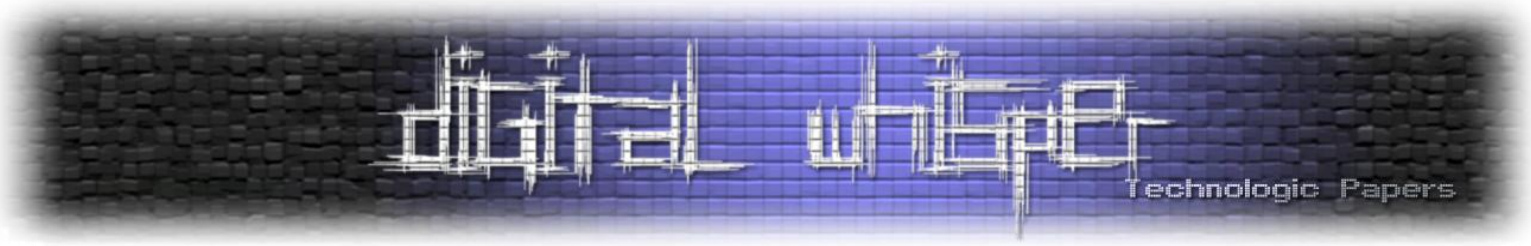


Digital Whisper

גליון 14, נובמבר 2010

מערכת המגזין:

מייסדים:	אפיק קסטיאל, ניר אדר
מוביל הפרוייקט:	אפיק קסטיאל
עורכים:	ניר אדר, סילאן דלאל
כתבים:	אפיק קסטיאל, עו"ד יהונתן קלינגר, אריק פרידמן, ליאור קפלן

פניות, תגובות, כתבות וכל הערה אחרת – נא לשלוח אל editor@digitalwhisper.co.il

דבר העורכים

ברוכים הבאים לגליון ה-14 של מגזין Digital Whisper. עוד חודש עבר ואנחנו שמחים שוב להציג לכם את הגליון החודשי.

בסוף כל גליון אנחנו מזכירים כי אנחנו נשמח לקבל מכם כתבות שלכם – הפעם אני רוצה דווקא להתחיל בנושא זה. נשמח לקבל מכם כתבות ולפרסם גם את מה שיש לכם להגיד בנושאי אבטחת מידע וטכנולוגיה. למגזין אלפים של קוראים בכל חודש, ומספר מגיבים גדול בבלוג שלנו (כיף לראות את כל התגובות – ממש עושה טוב שיש מקום שאפשר לדבר בו על כל הנושאים המרתקים האלה בעברית, וכיף לראות את הרמה המקצועית של הדיון בהערות).

נשמח לקבל מכם מאמרים, נשמח גם לפרסם פוסטים שלכם בבלוג כך שגם אתם תוכלו להשפיע על הדיון המתרחש באתר. תודה שאתם קוראים את המגזין שלנו, ואנחנו מקווים להמשיך להביא לכל הקהילה מאמרים מרתקים כאלה במשך זמן רב.

ואחרי נאום הציונות שלנו – נעבור לתוכנית האומנותית של גליון זה ☺. המאמרים בגליון:

- במאמר "Chasing Worms (Koobface Pwning)" **אפיק** מציג ניתוח מרתק ויוצא דופן של התולעת Koobface עליה סיפרנו בבלוג.
- "אין סודות בחברה", מאת **אריק פרידמן**, מדבר על (חוסר) יעילותה של סודיות כאמצעי לאבטחת מידע.
- **עו"ד יהונתן קלינגר**, במאמרו "מתי אפשר לתפוס שרתים, מחשבים ודיסקים" סוקר את הדרכים בהן ניתן לבקש תפיסה של חומר מחשב וכיצד מבוצעת התפיסה בפועל.
- לסיום, במאמר "אבטחת חבילות תוכנה" סוקר **ליאור קפלן** את אבטחת המידע של חבילות התוכנה של מערכות לינוקס השונות.

ברצוננו להודות לכל הכותבים ולאחל לכם קריאה מהנה. נשמח לשמוע בתגובות את דעתכם על הכתבות השונות.

ניר אדר אפיק קסטיאל

תוכן עניינים

Chasing Worms (Koobface Pwning)

מאת cp77fk4r (אפיק קסטיאל)

הקדמה

החלטתי לכתוב את המאמר הזה לאחר כתיבת הפוסט שלי על תולעת ה-Koobface. בפוסט הצגתי צד אחד של התולעת- הצד שמעל פני השטח, מה התוצר שלה בסופו של דבר ואת הממשק שלה עם המשתמש הפשוט (הודעה תמימה בפייסבוק).

במאמר זה לקחתי את הנושא צעד אחד קדימה - הקמתי "סביבת מחקר" - מכונה וירטואלית מבודדת שנמצאת תחת מעקב (WireShark + Proccess Monitor). הורדתי את התולעת למכונה והרצתי.

למה שארצה לעשות דבר כזה? ראשית- בכדי לחקור את התולעת, לראות מה היא עושה ואיך היא עושה את מה שהיא עושה. שנית, וזאת הסיבה העיקרית- רציתי לאתר את ה-DropZone של התולעת, לבדוק אם אוכל להשיג גישה אליו- ואולי אף להשבית את התולעת.

אך לפני שנתחיל, קצת מידע על דרכי פעולה של תולעים מסגנון זה בכלליות ועל ה-KoobFace בפרט.

KoobFace ושאר ירקות – רקע כללי

כיום מסתובבות בסייבר מספר רב של תולעים, כאשר כל תולעת מנצלת חולשה אחרת, תוקפת מטרה אחרת, מפיצה את עצמה בדרכים אחרות ומחפשת אחר מידע שונה. אפשר לטעון כי רב התולעים עובדות באופן דומה - כמובן שהפרטים עצמם שונים, אך הארכיטקטורה שלהן זהה ברב המקרים. תולעת ה-KoobFace היא תולעת שוקטור התפוצה שלה מתבסס על רשתות חברתיות.

לפי ויקיפדיה, ל-KoobFace קיימות שש וריאציות, כל אחד מהן מתבססת על רשת חברתית אחרת:

- Worm:Win32/Koobface.gen!F, [Facebook] Microsoft Virus Definition
- Net-Worm.Win32.Koobface.a, which attacks MySpace
- Net-Worm.Win32.Koobface.b, which attacks Facebook.[4]
- WORM_KOOBFACE.DC, which attacks Twitter.[5]
- W32/Koobfa-Gen, which attacks Facebook, MySpace, hi5, Bebo, Friendster, myYearbook, Tagged, Netlog, Badoo and fubar.[6][7]
- W32.Koobface.D[8]

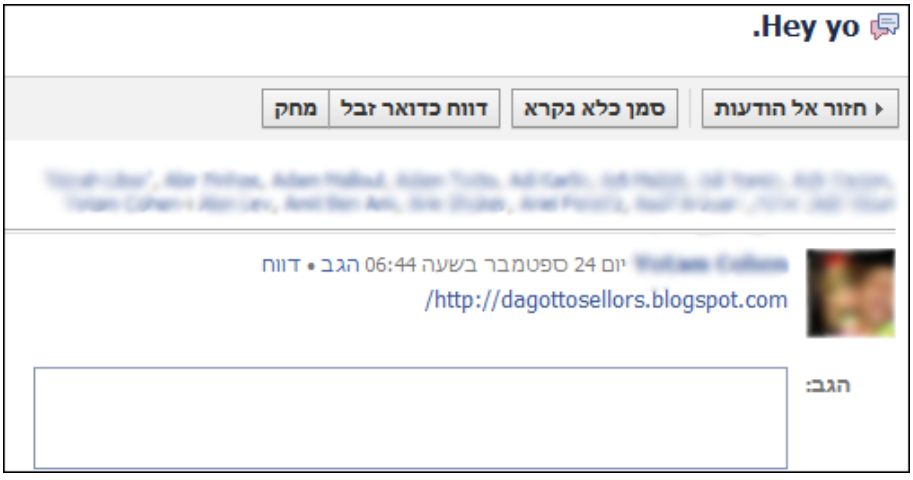
הלוגיקה מאחורי התולעת אינה מנצלת שום חולשה או מנגנון לקוי, והיא מתבססת על תמימותו של המשתמש. הרעיון הוא פשוט:

כותב התולעת מעלה עמוד אינטרנט שנראה כמו עמוד עם סרטון לגיטימי ב-Youtube ומפיץ את העמוד-בהרצה הראשונה העמוד מבקש מהמשתמש להוריד את העדכון האחרון לנגן הפלאש שלו (כמובן שמדובר בקובץ נגוע). לאחר מכן, ברגע שהורץ ה-"עדכון" על המחשב, התולעת פורסת את עצמה על המחשב, מדווחת לשרת השליטה והבקרה שלה על ההדבקה, ומבצעת מספר פעולות כגון: גונבת למשתמש את קבצי ה-Cookies של הרשת החברתית בה הוא חבר (במקרה שלנו מדובר ברשת החברתית Facebook), מבצעת בשמו פעולות, כגון: שליחת הודעה פרטית לכלל חבריו ברשת ופרסום הודעה ב"קיר" האישי של כלל החברים שלו. בהודעה שהתולעת שולחת בשמו של המשתמש קיים קישור לעמוד עם הסרטון שדורש עדכון... וחוזר חלילה.

עד כאן וקטור התפוצה של התולעת - נכון לעכשיו לא מדובר בשום דבר "מזיק" במיוחד, אך לתולעת יש מספר מאפיינים נוספים, בין היתר היא מהווה Dropper לסוסים טרויאנים שיהפכו את העמדה הנגועה לזומבי הנשלט תחת שרת IRC.

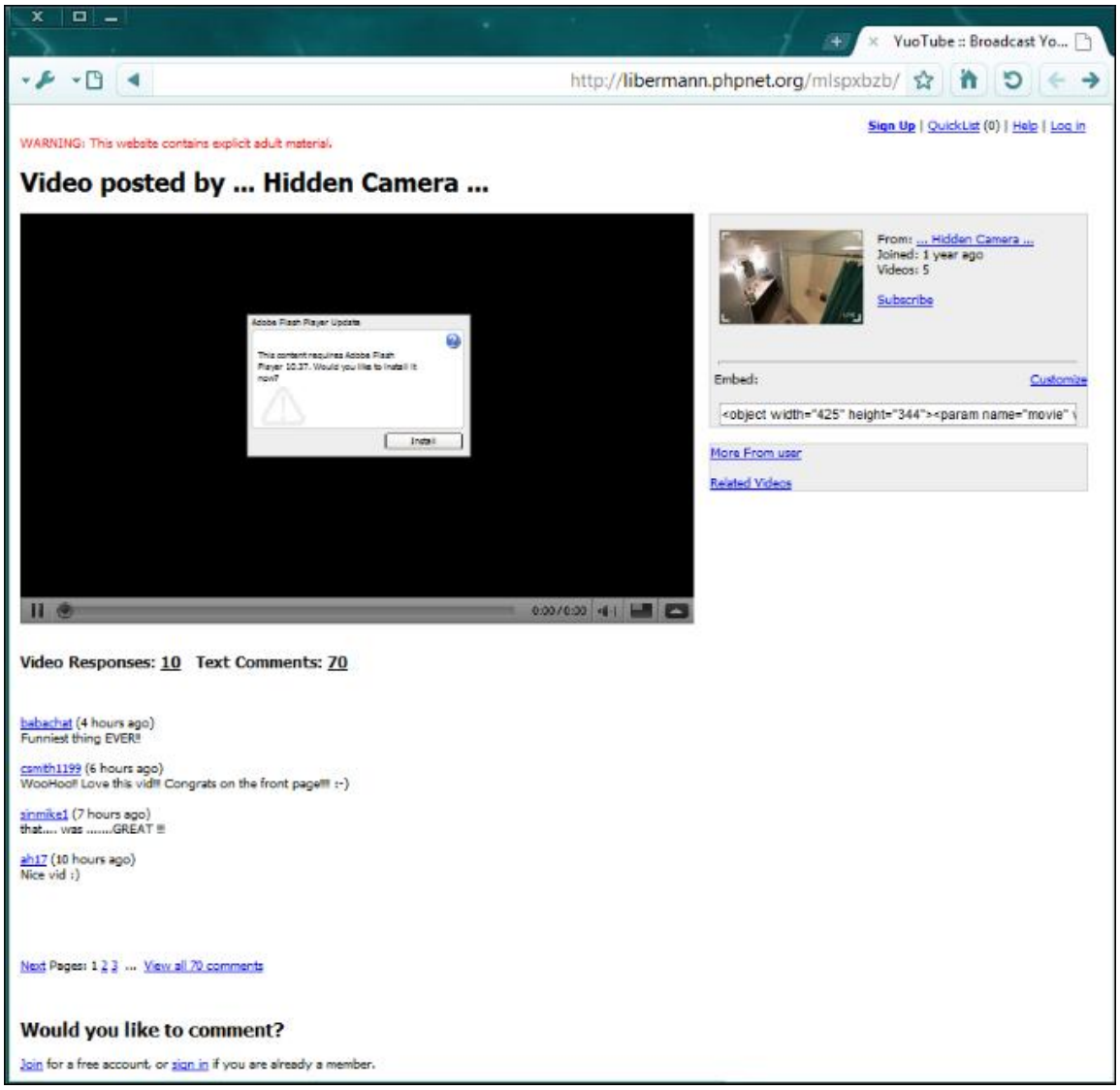
אז איך הכל התחיל?

מי שקרא את הפוסט מכיר את הסיפור: לפני בערך שבועיים קיבלתי הודעה פרטית ברשת פייסבוק מחבר ששירת איתי, וזאת הלשון:



כמו שאפשר לראות: לינק אחד קצר, ומספר רב של מכותבים. (כלומר 90 אחוז שמדובר בתולעת)

לחיצה על הלינק העבירה אותי לעמוד ב-Blogspot.com שהעביר אותי שניה לאחר מכן לעמוד הבא:

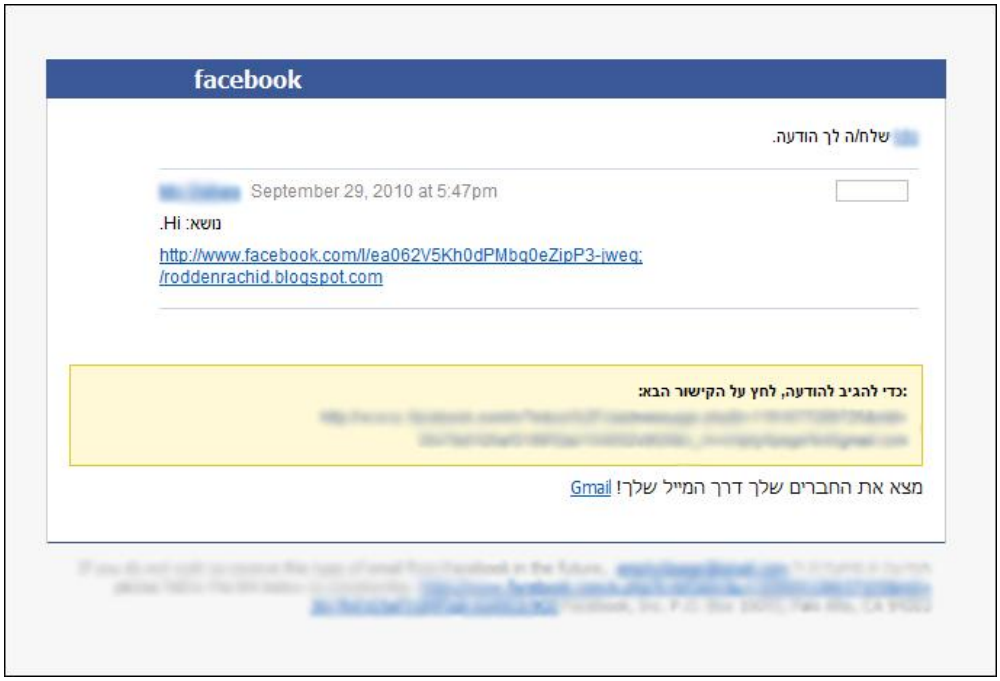


ה-10 אחוז שנשארו נעלמו כלא היו ולאחר שהעמוד עוד ביקש ממני להוריד קובץ exe מאותו שרת בטענה שמדובר ב-"עדכון האחרון של נגן הפלאש שלי" (כן, בטח) – לא נשארה כל אפשרות אחרת, מדובר בתולעת.

העלתי את הבינארי ל-VirusTotal והבנתי שככל הנראה מדובר בגל חדש של התולעת KoobFace. עדכנתי את הבחור המסכן שהחשבון שלו נפרץ ושכך הנראה יש לו תולעת על המחשב, הסברתי לו איך להסיר את התולעת וחזרתי לעיסוקי המעניינים ביותר.

מספר ימים לאחר מכן, קיבלתי התראה בתיבת הדוא"ל שלי, על כך שיש לי הודעה חדשה בפייסבוק.

פתחתי את ההתראה, שנראתה כך:



והבנתי מיד, כנראה גם הוא נדבק. כנראה שמדובר באותה התולעת, בחשבון Blogspot שונה, והפעם כותב התולעת הגדיל והשתמש בחולשת ה-"Open Redirection" שקיימת זמן רב ברשת פייסבוק. עדכנתי גם אותו, וכתבתי פוסט ב-Digital Whisper.

בסוף השבוע האחרון, לאחר שראיתי את התגובות לפוסט, בחרתי לפנות קצת זמן והחלטתי לחקור את התולעת.

הכלים שלי:

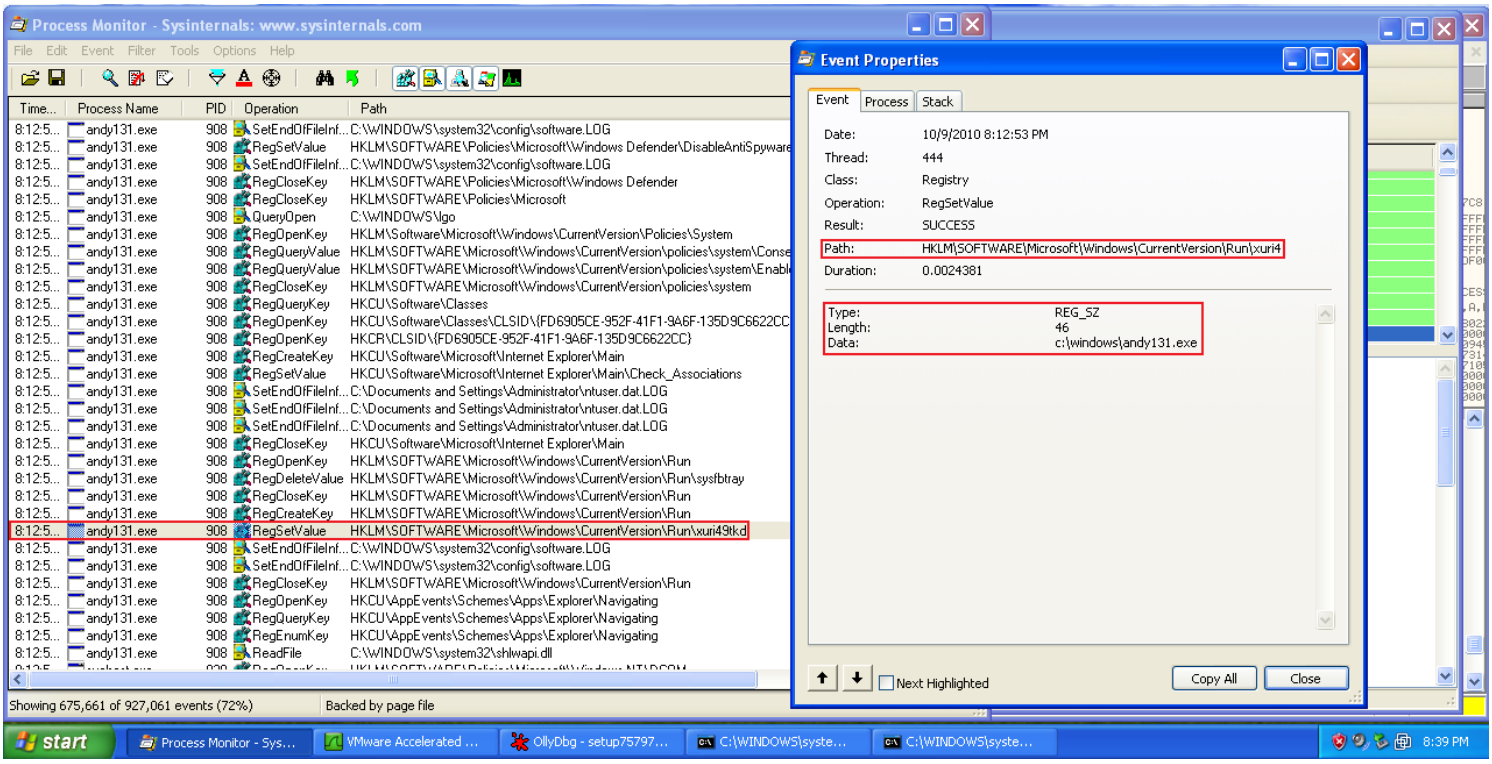
- **מכונה וירטואלית (VMWare) של Windows XP Professional SP3** - לצורך סביבת ההרצה של התולעת.
- **WireShark** - לקבלת תמונה של מה עובר לי ברשת.
- **Proccess Monitor של SysInternals** - לקבלת תמונה של מה רץ לי במערכת הפעלה.
- **OllyDBG** - לחקור את הקוד של התולעת עצמה.
- **חשבון Facebook טרי** - החשבון עליו התולעת תשתלט.
- **בינארי חם חם חם של התולעת.**

לאחר קינפוג קל של המכונה הוירטואלית, התמקמות של ה-WireShark ושל ה-ProcMonitor, התחברות לחשבון ה-Facebook החדש ("זכור אותי" – דלוק), יצרתי Snapshot של המכונה (לכל מקרה) והרצתי את התולעת תחת Olly. הקובץ עצמו מכונה "setup757978.exe", שוקל קצת פחות מ-150kb וכל תפקידו הוא להגיע למחשב ולהוריד לעמדה קובץ חדש, גדול יותר, בשם "Andy151.exe" (כמובן שהמספרים בשמות הם ערכים ראנדומלים).

לאחר הורדה של הקובץ Andy151.exe, הוא מורץ תחת תהליך חדש והקובץ הישן- נמחק. הפעולה הראשונה ש-Andy עושה היא לגבות את עצמו בתיקית מערכת ההפעלה ולוודא שרידות לאחר כיבוי על ידי הכנסת ה-Path שלו לערך:

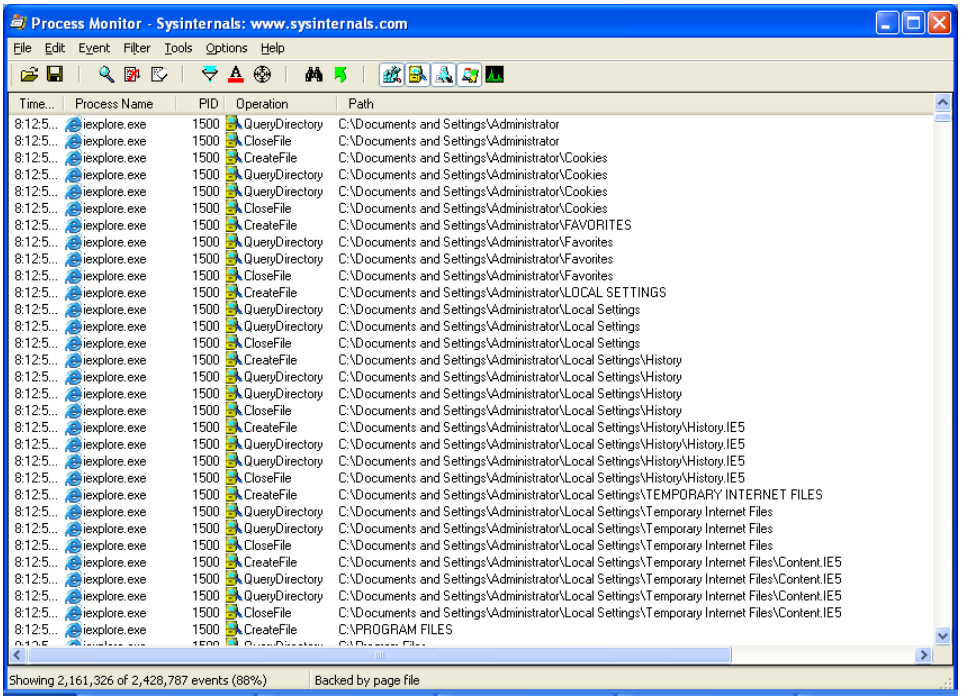
```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

בעורך הרישום תחת מחרוזת ראנדומלית. ניתן לראות זאת כאן:



זהו המנגנון היחיד בו משתמשת התולעת בכדי לדאוג לכך שהיא תשרוד לאחר כיבוי מערכת ההפעלה והפעלתה מחדש. אותי אישית זה הפתיע.

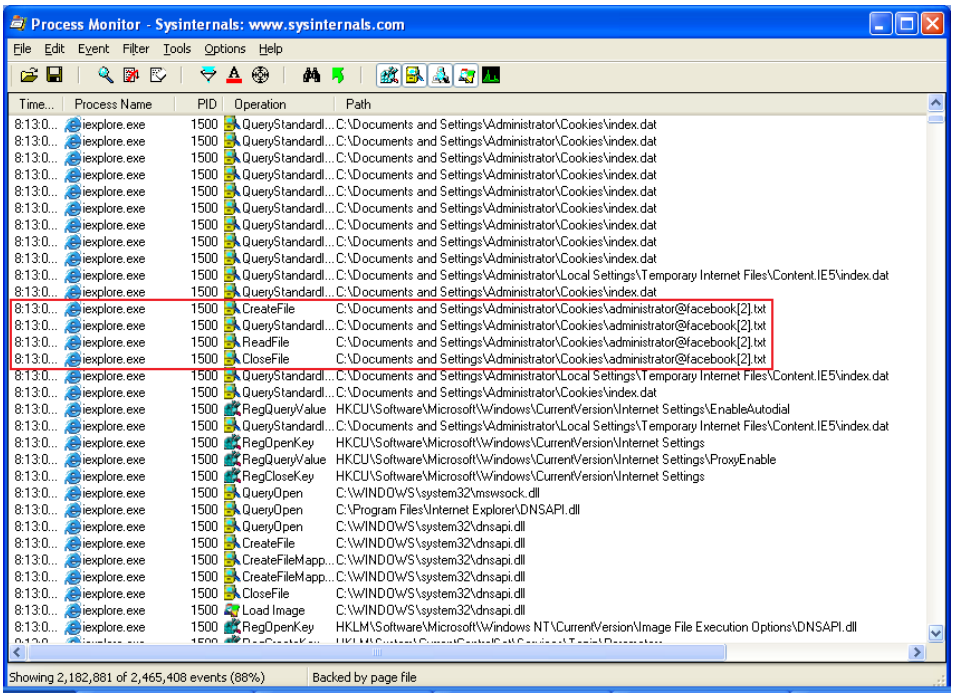
מספר שניות לאחר מכן, ניתן היה לראות את Andy רותמת את iexplorer.exe לטובתה ומפלסת לעצמה את הדרך לעבר תיקית ה-cookies של המשתמש הנוכחי (administrator):



```
Time...   Process Name   PID   Operation        Path
8:12:5... iexplore.exe   1500  QueryDirectory   C:\Documents and Settings\Administrator
8:12:5... iexplore.exe   1500  CloseFile        C:\Documents and Settings\Administrator
8:12:5... iexplore.exe   1500  CreateFile       C:\Documents and Settings\Administrator\Cookies
8:12:5... iexplore.exe   1500  QueryDirectory   C:\Documents and Settings\Administrator\Cookies
8:12:5... iexplore.exe   1500  QueryDirectory   C:\Documents and Settings\Administrator\Cookies
8:12:5... iexplore.exe   1500  CloseFile        C:\Documents and Settings\Administrator\Cookies
8:12:5... iexplore.exe   1500  CreateFile       C:\Documents and Settings\Administrator\FAVORITES
8:12:5... iexplore.exe   1500  QueryDirectory   C:\Documents and Settings\Administrator\Favorites
8:12:5... iexplore.exe   1500  QueryDirectory   C:\Documents and Settings\Administrator\Favorites
8:12:5... iexplore.exe   1500  CloseFile        C:\Documents and Settings\Administrator\Favorites
8:12:5... iexplore.exe   1500  CreateFile       C:\Documents and Settings\Administrator\LOCAL SETTINGS
8:12:5... iexplore.exe   1500  QueryDirectory   C:\Documents and Settings\Administrator\Local Settings
8:12:5... iexplore.exe   1500  QueryDirectory   C:\Documents and Settings\Administrator\Local Settings
8:12:5... iexplore.exe   1500  CloseFile        C:\Documents and Settings\Administrator\Local Settings
8:12:5... iexplore.exe   1500  CreateFile       C:\Documents and Settings\Administrator\Local Settings\History
8:12:5... iexplore.exe   1500  QueryDirectory   C:\Documents and Settings\Administrator\Local Settings\History
8:12:5... iexplore.exe   1500  QueryDirectory   C:\Documents and Settings\Administrator\Local Settings\History
8:12:5... iexplore.exe   1500  CloseFile        C:\Documents and Settings\Administrator\Local Settings\History
8:12:5... iexplore.exe   1500  CreateFile       C:\Documents and Settings\Administrator\Local Settings\History\History.IE5
8:12:5... iexplore.exe   1500  QueryDirectory   C:\Documents and Settings\Administrator\Local Settings\History\History.IE5
8:12:5... iexplore.exe   1500  QueryDirectory   C:\Documents and Settings\Administrator\Local Settings\History\History.IE5
8:12:5... iexplore.exe   1500  CloseFile        C:\Documents and Settings\Administrator\Local Settings\History\History.IE5
8:12:5... iexplore.exe   1500  CreateFile       C:\Documents and Settings\Administrator\Local Settings\TEMPORARY INTERNET FILES
8:12:5... iexplore.exe   1500  QueryDirectory   C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files
8:12:5... iexplore.exe   1500  QueryDirectory   C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files
8:12:5... iexplore.exe   1500  CloseFile        C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files
8:12:5... iexplore.exe   1500  CreateFile       C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5
8:12:5... iexplore.exe   1500  QueryDirectory   C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5
8:12:5... iexplore.exe   1500  QueryDirectory   C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5
8:12:5... iexplore.exe   1500  CloseFile        C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5
8:12:5... iexplore.exe   1500  CreateFile       C:\PROGRAM FILES

Showing 2,161,326 of 2,428,787 events (88%)   Backed by page file
```

לאחר שהתיקיה נמצאה, התולעת מאתרת את קבצי ה-Cookies של Facebook ושולפת ממנה את הנתונים הדרושים לה לצורך ביצוע ההזדהות לחשבונו של הקורבן:



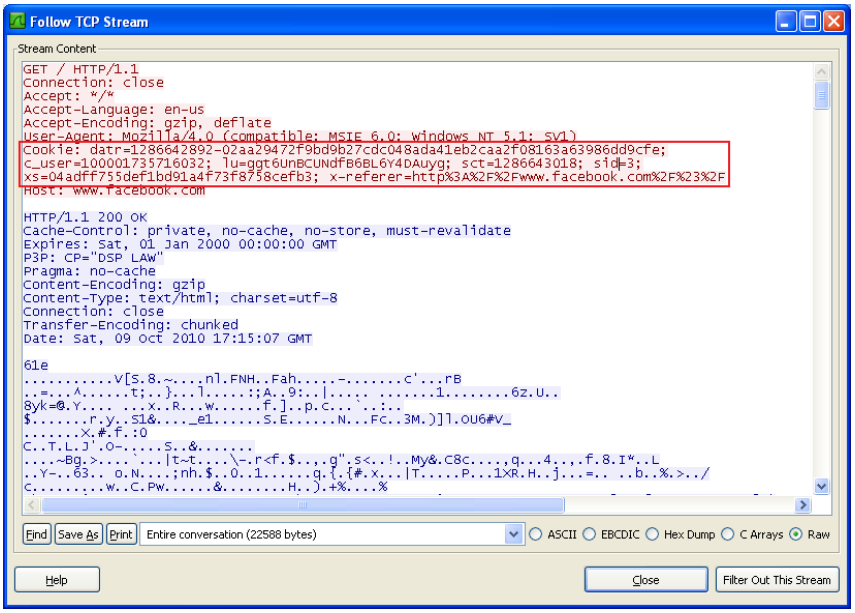
```
Time...   Process Name   PID   Operation         Path
8:13:0... iexplore.exe   1500  QueryStandardI... C:\Documents and Settings\Administrator\Cookies\index.dat
8:13:0... iexplore.exe   1500  QueryStandardI... C:\Documents and Settings\Administrator\Cookies\index.dat
8:13:0... iexplore.exe   1500  QueryStandardI... C:\Documents and Settings\Administrator\Cookies\index.dat
8:13:0... iexplore.exe   1500  QueryStandardI... C:\Documents and Settings\Administrator\Cookies\index.dat
8:13:0... iexplore.exe   1500  QueryStandardI... C:\Documents and Settings\Administrator\Cookies\index.dat
8:13:0... iexplore.exe   1500  QueryStandardI... C:\Documents and Settings\Administrator\Cookies\index.dat
8:13:0... iexplore.exe   1500  QueryStandardI... C:\Documents and Settings\Administrator\Cookies\index.dat
8:13:0... iexplore.exe   1500  QueryStandardI... C:\Documents and Settings\Administrator\Cookies\index.dat
8:13:0... iexplore.exe   1500  QueryStandardI... C:\Documents and Settings\Administrator\Cookies\index.dat
8:13:0... iexplore.exe   1500  QueryStandardI... C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat
8:13:0... iexplore.exe   1500  QueryStandardI... C:\Documents and Settings\Administrator\Cookies\index.dat
8:13:0... iexplore.exe   1500  CreateFile        C:\Documents and Settings\Administrator\Cookies\administrator@facebook[2].txt
8:13:0... iexplore.exe   1500  QueryStandardI... C:\Documents and Settings\Administrator\Cookies\administrator@facebook[2].txt
8:13:0... iexplore.exe   1500  ReadFile          C:\Documents and Settings\Administrator\Cookies\administrator@facebook[2].txt
8:13:0... iexplore.exe   1500  CloseFile         C:\Documents and Settings\Administrator\Cookies\administrator@facebook[2].txt
8:13:0... iexplore.exe   1500  QueryStandardI... C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat
8:13:0... iexplore.exe   1500  QueryStandardI... C:\Documents and Settings\Administrator\Cookies\index.dat
8:13:0... iexplore.exe   1500  RegQueryValue     HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\EnableAutodial
8:13:0... iexplore.exe   1500  QueryStandardI... C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat
8:13:0... iexplore.exe   1500  RegOpenKey        HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings
8:13:0... iexplore.exe   1500  RegQueryValue     HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable
8:13:0... iexplore.exe   1500  RegCloseKey       HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings
8:13:0... iexplore.exe   1500  QueryOpen         C:\WINDOWS\system32\mswsock.dll
8:13:0... iexplore.exe   1500  QueryOpen         C:\Program Files\Internet Explorer\DNSAPI.dll
8:13:0... iexplore.exe   1500  QueryOpen         C:\WINDOWS\system32\dnsapi.dll
8:13:0... iexplore.exe   1500  CreateFile        C:\WINDOWS\system32\dnsapi.dll
8:13:0... iexplore.exe   1500  CreateFileMapp... C:\WINDOWS\system32\dnsapi.dll
8:13:0... iexplore.exe   1500  CreateFileMapp... C:\WINDOWS\system32\dnsapi.dll
8:13:0... iexplore.exe   1500  CloseFile         C:\WINDOWS\system32\dnsapi.dll
8:13:0... iexplore.exe   1500  Load Image        C:\WINDOWS\system32\dnsapi.dll
8:13:0... iexplore.exe   1500  RegOpenKey        HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DNSAPI.dll

Showing 2,182,881 of 2,465,408 events (88%)   Backed by page file
```

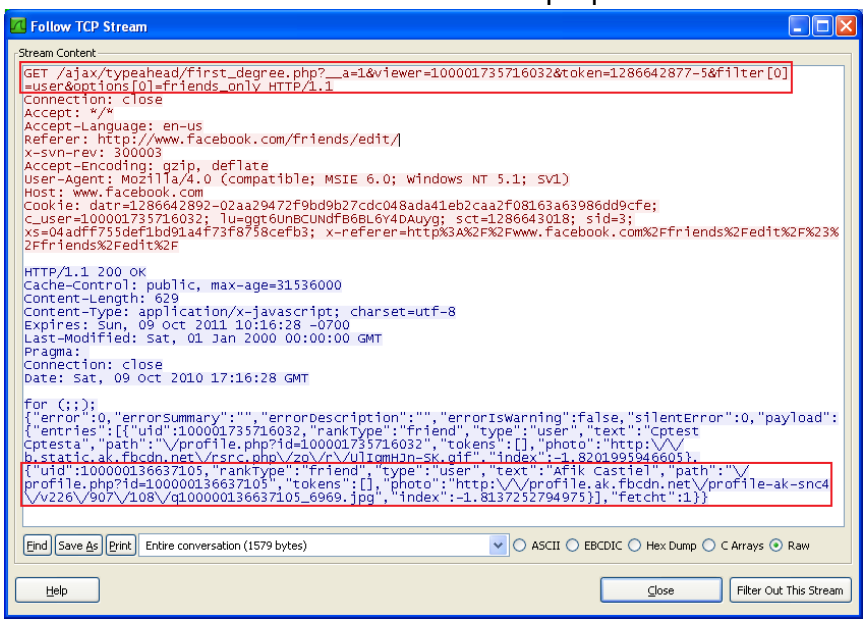
מנגנון ההפצנה

כאן עברתי להסתכל בלוגים של ה-WireShark בכדי לזהות מה מתבצע עם המידע שנשלף מה-Cookies של הקורבן, והתשובה לא איחרה לבוא:

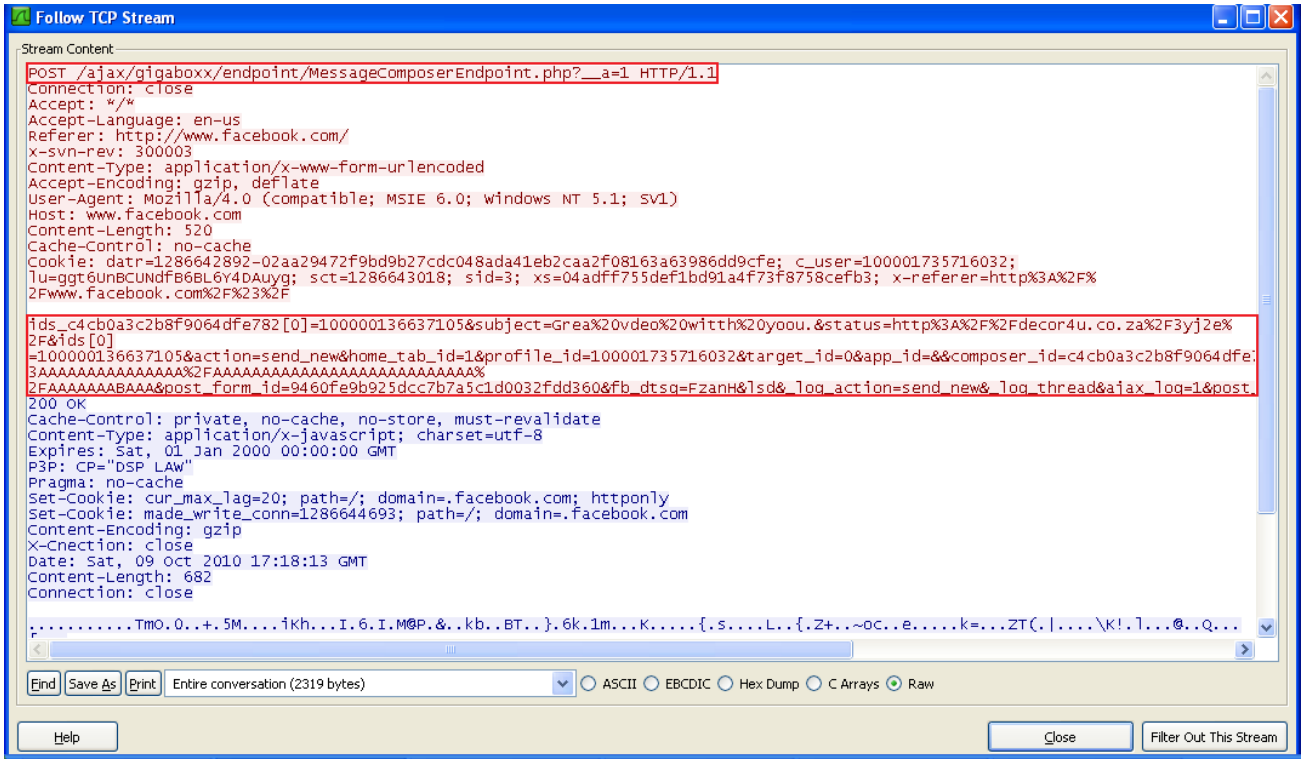
<u>שלב 1:</u> התחברות לרשת Facebook עם ה-Cookies של המשתמש:



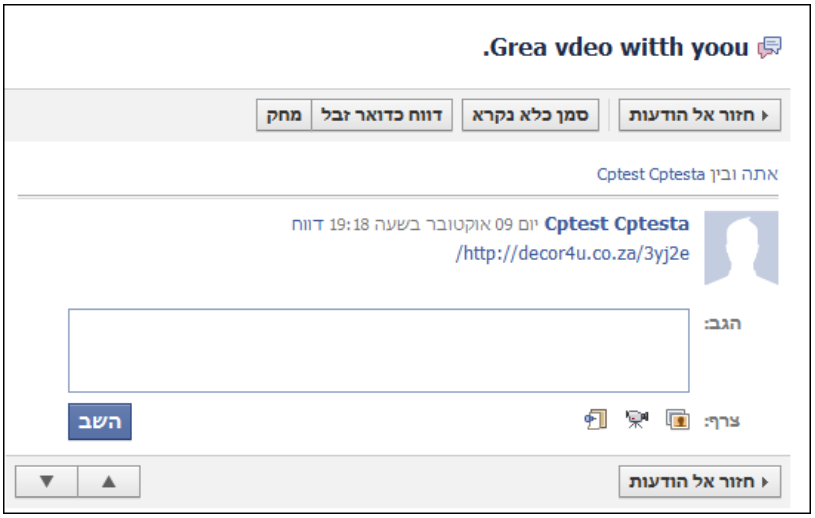
<u>שלב 2:</u> השגת שמות החברים של הקורבן:



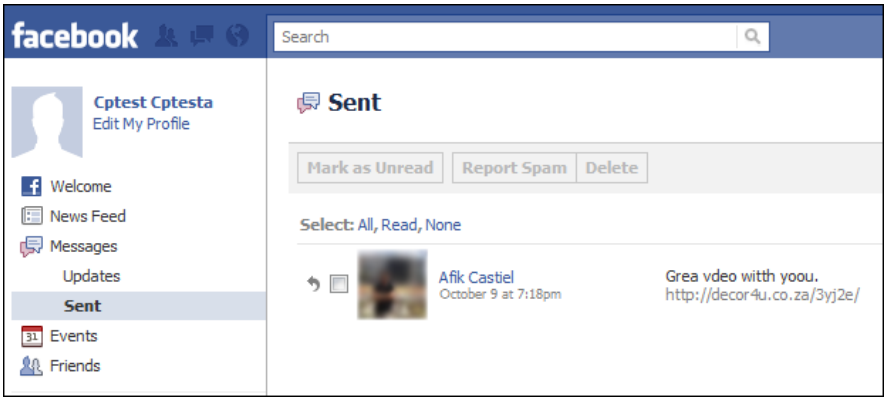
<u>שלב 3:</u> שליחת הודעה פרטית לחברי הקורבן לפי המידע שנבנה בשלב הקודם:



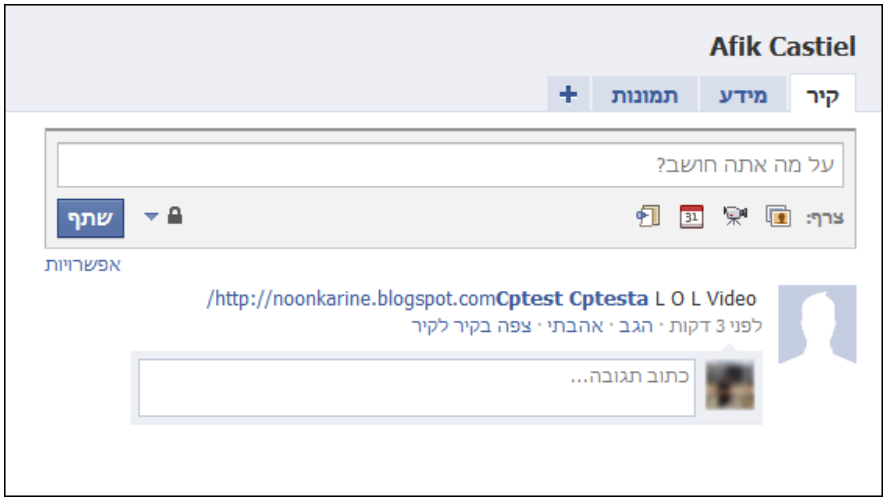
וכמובן- ששניה לאחר מכן, קיבלתי הודעה פרטית מהחשבון הפרוץ:



אגב, מבדיקה שערכתי, מתברר שהתולעת אינה מוחקת את ההודעות שהיא שולחת מחשבונו של המשתמש – "חוסר מקצועיות" מצד כותב התולעת:



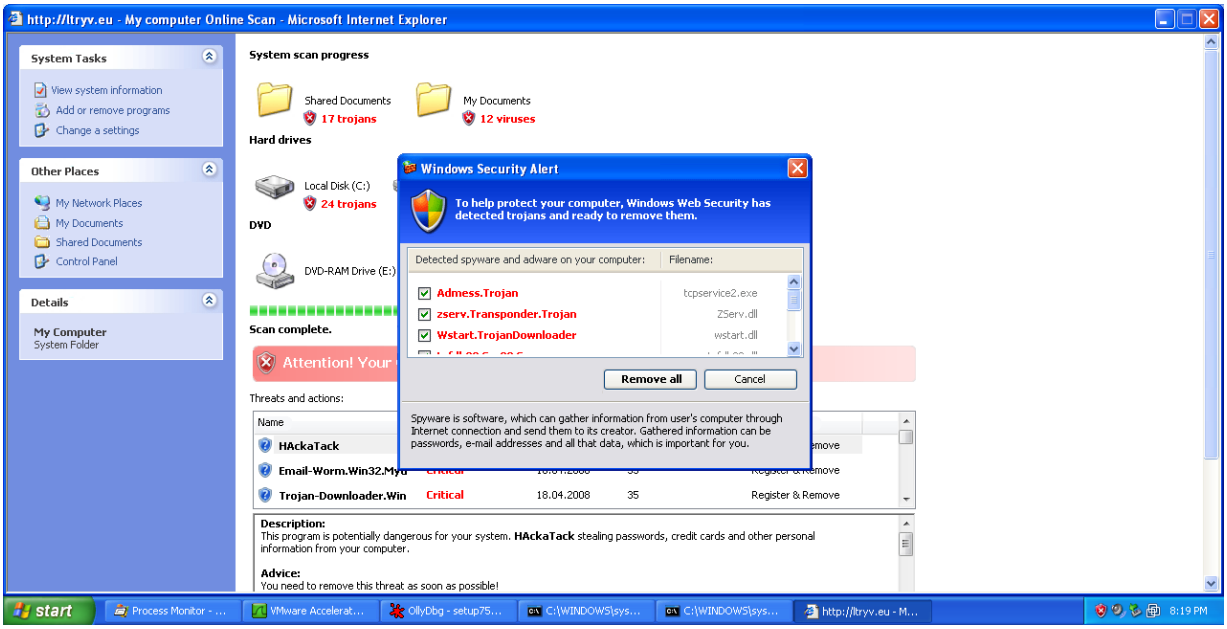
<u>שלב 4:</u> כתיבה בקיר ("Wall") האישי של חברי הקורבן:



(כמובן שלאחר לכידת המסך מחקתי את הפרסום.)

זהו בעצם, כאן פחות או יותר נגמר מנגנון ההפצה של התולעת ברשת החברתית והכל מתחיל מהתחלה- כל מי שיפול בפח, יכנס לעמודים שהתולעת פרסמה דרך החשבון הפרוץ ויוריד את העדכון, ידבק גם הוא וימשיך להדביק הלאה.

דבר נוסף שחשוב להזכיר וקצת סוגר בשבילי מעגל הוא העובדה שכל חמש דקות בעמדה הנגועה, נפתח חלון Full-Screen של Internet Explorer (בלי סרגלי כלים) שנראה כך:



שימו לב שמלבד שורת ה-Title (המראה על ה-URL ממנו נטען העמוד) ושורת ה-Start, ממנה אפשר לראות שמדובר בסך הכל בחלון של הדפדפן, העמוד נראה ממש כאילו אכן מדובר ב- Windows Security Alert אמיתי. מזכיר לכם משהו? לי כן. ☺

כמובן שכל לחיצה על "Remove all", או בכלל על החלון תקפיץ הודעה של הורדת קובץ. וזה גרם לי לתהות לגבי שני דברים:

- העמוד עצמו לא נטען באופי מקומי (Local Zone) אלא מה-Internet Zone, כך שאין לו הרשאות מיוחדות וזה מוזר, הרי לכותב יש את השליטה על המחשב ואת האפשרות לטעון עמודים הרבה יותר חזקים.
- למה הקבצים לא יורדים פשוט מעצמם, במקום להקפיץ את ההודעות האלה כל הזמן ולהמתין שהמשתמש יועיל בטובו להוריד את הקבצים ויריץ אותם? הרי לתהליך שמקפיץ את החלון הזה יש את הרשאות המשתמש על העמדה, כך שהוא יכול לבצע תחת הרשאותיו הכל.

והאמת? אין לי תשובות לשאלות אלו.

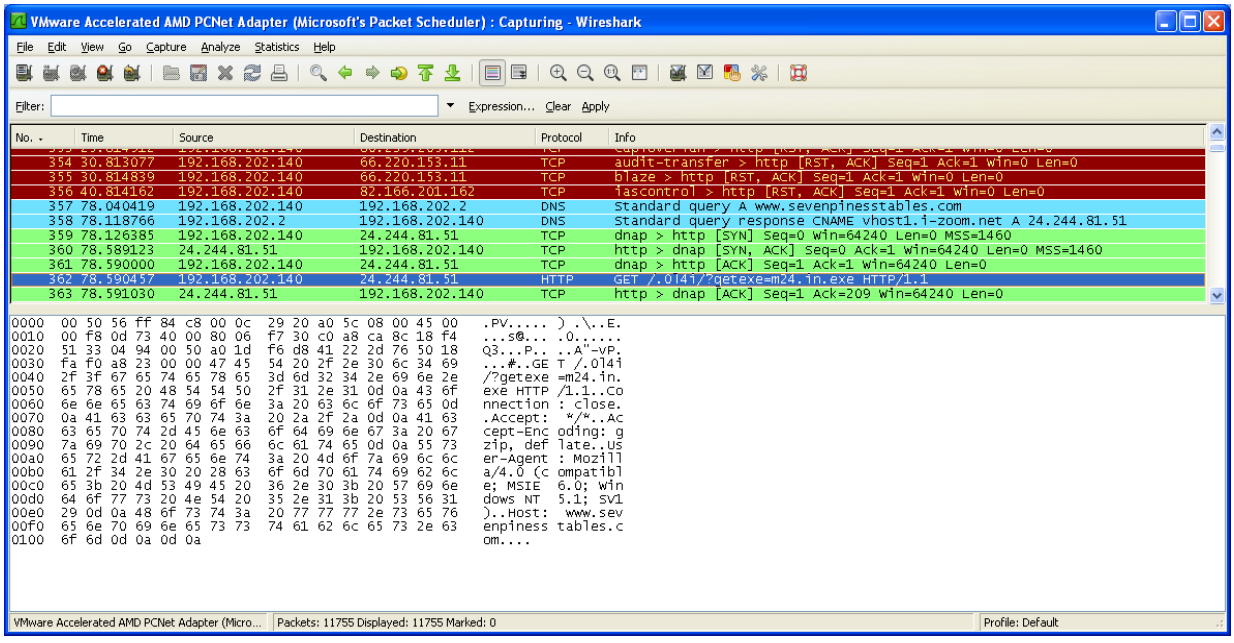
אז מה רוצה התולעת?

חוץ מלשלוח הודעות ברשת Facebook ולכתוב על קירות, מה בעצם עושה התולעת? בארכיטקטורה של התולעים המודרניות, מנגנון התפוצה נפרד בדרך כלל מהמנגנון שאחראי על הפעילות העיקרית של התולעת. למה זה? מפני שכך קל יותר לכותב התולעת למכור אותה לגופים השונים, הוא פשוט מאוד יוצר קובץ חיצוני לתולעת שמבצע את הפעולות בהן אותם גופים מעוניינים (או שהוא מקבל מהם קובץ כזה והם משלמים על הפצתו) ופוקד על התולעת (החלק הבינארי שאחראי על התפוצה – כמו שראינו) להוריד את אותו קובץ חיצוני (קובץ זה נקרא "Payload" ולקובץ שאחראי להוריד אותו קוראים "Dropper"). בדרך כלל כותב התולעת מרוויח כסף בהתאם לכמות העמדות שהוא מצליח להדביק ב-Payload, במקרים שכותב התולעת מעוניין להרוויח יותר אפשר למצוא ש-Dropper אחד אחראי על הורדה והרצה של מספר Payloads.

בהרבה מקרים, ה-Payload מבצע איסוף של מידע הקיים על המחשב (כגון כרטיסי אשראי), מבצע מתקפות כגון Man In The Browser או Sniffing לתעבורה בכדי לחפש סיסמאות/מידע ספציפי כזה או אחר, את המידע שהוא מוצא- הוא "זורק" בשרת יעודי המכונה "DropZone".

בנוסף לכך, כמעט כל Payload רציני מחבר את העמדה הנגועה לשרת שליטה (Command And Control) ומחכה לפקודות נוספות. לרוב מדובר בשרתי IRC, מפני שנוח מאוד לעבוד איתם כאשר מדובר בכמות גדולה של מחשבים נגועים. אגב, למחשבים אלה נקראים "זומבים" ולרשת כזאת של מחשבים קוראים "Bot-net", לא אכנס כאן לעומק הענין מפני שכתבתי בעבר מאמר שלם העוסק בעולם הבוטנטים בשם "Botnet – מה זאת החיה הזאת?" שפורסם בגליון השישי של DigitalWhisper.

הבה נחזור לתולעת שלנו... מצפיה בלוגים של הכריש שלנו, ניתן לראות מקרים כגון זה:



מקרים אלו המעידים על נסיונות (ובמקרים שאין שום תוכנת Anti Virus, Firewall או כל מני "פורענויות" בדרך, אז גם על הצלחות) של הורדות נוספות, אלה הם ה-Payloads שהזכרנו. כל Payload תוכנן לבצע פעולות שונות, ולעיתים מתבצעות פעולות חופפות שגורמות להתנגשויות (כמו במתקפות מסוג Man In The Browser מקבילות).

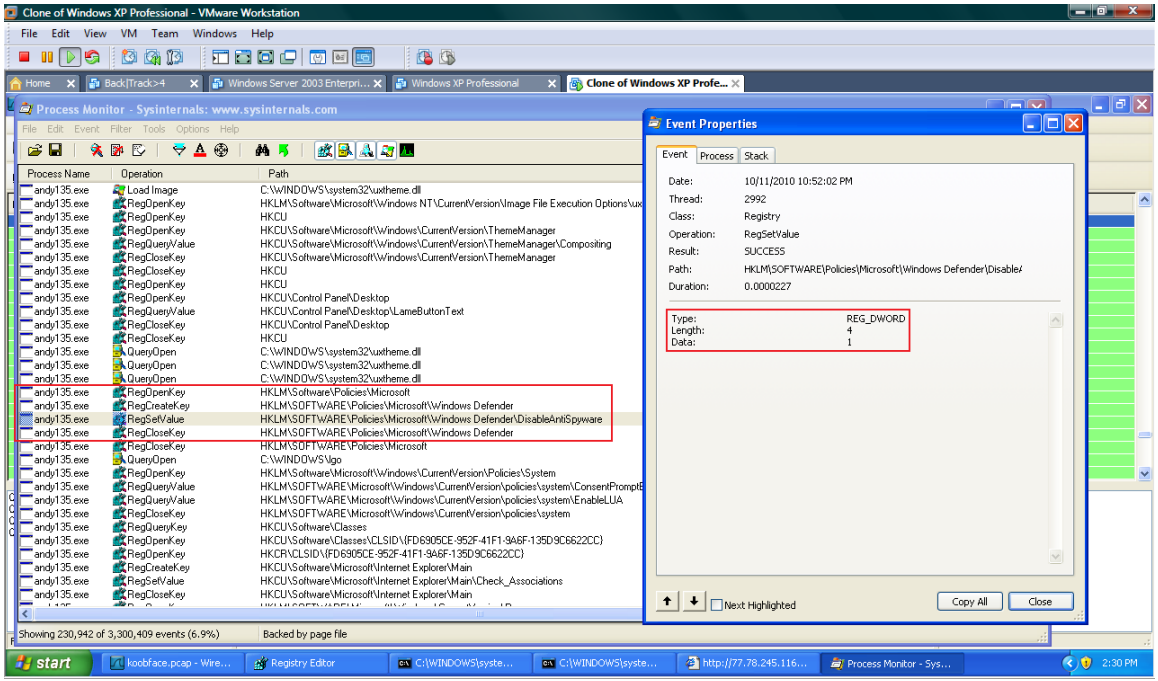
במקרה שלנו נמצאו שישה Payloads שונים (לפי סדר הופעתם על העמדה הנגועה):

- Andy131.exe
- Andy135.exe
- fd1a245s4_868.exe
- zpskon_1286827802.exe
- zpskon_1286832181.exe
- zpskon_1286832181.exe

את Andy131.exe אנחנו כבר מכירים, הוא חלק מתהליך ההפצה של התולעת, הוא אוסף את ה-Cookies של המשתמש, מבצע את הפעולות ברשת החברתית ואחראי לשרידות התולעת, כך שהוא לא בדיוק "Payloads" אלא חלק בלתי נפרד מהתולעת עצמה.

ניתוח של Andy135.exe (שלפי שמו, אפשר לנחש שגם הוא לא בדיוק "Payload", אלא סט פקודות לביצוע, או אולי עדכון של התולעת) לימד על מספר דברים, ככל הנראה תפקידו הוא לקנפג מספר חלקים במערכת כך שלתולעת ולשאר ה-Payloads יהיה קל יותר לבצע את תפקידם:

- דוגמא ראשונה:



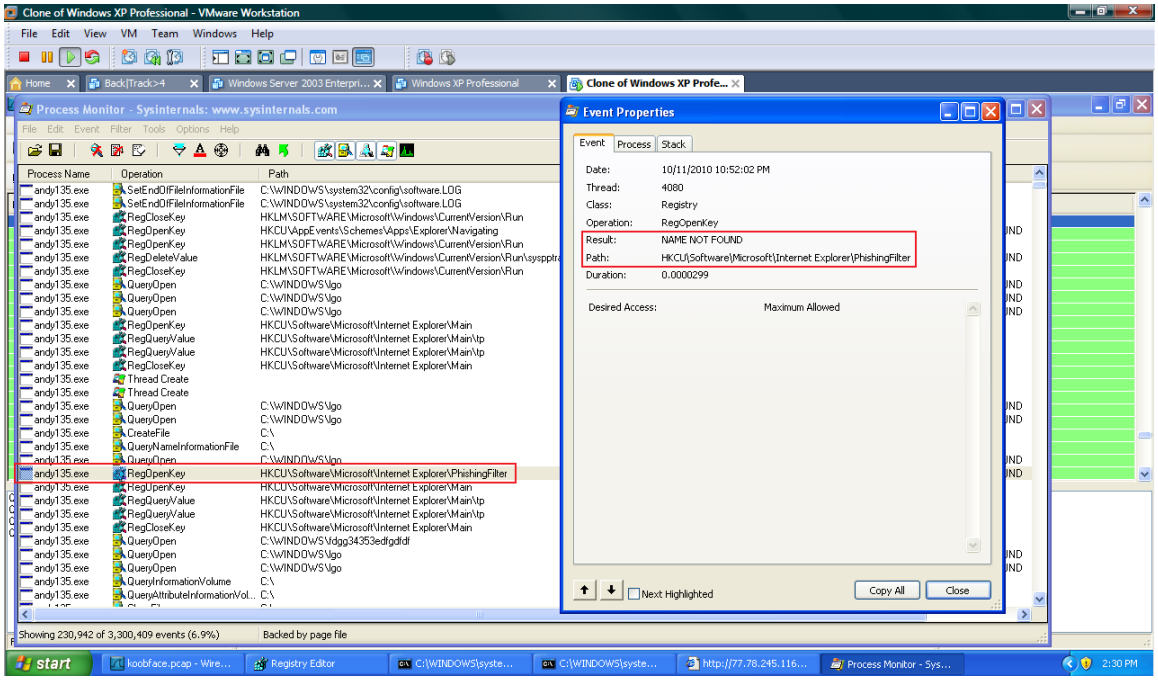
Andy135.exe - משנה ל-"True" את ערך המפתח:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows
Defender\DisableAntiSpyware
```

ועל פי מיקרוסופט:

```
If you enable this policy setting, Windows Defender does not run.
Computers are not scanned for spyware or other potentially unwanted
software. If you disable or do not configure this policy setting,
Windows Defender runs, and computers are scanned for spyware and other
potentially unwanted software.
```

- דוגמה שניה:



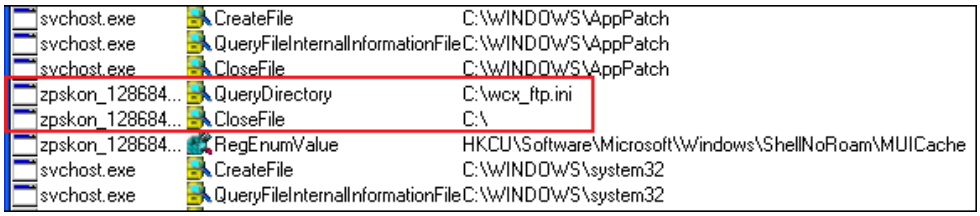
Andy153.exe מבצע בדיקה האם קיים הערך:

```
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\PhishingFilter
```

במידה והערך קיים במערכת ופעיל- הוא מבטל אותו, כך שה-IE לא יציג הודעות אזהרה בכניסה לאתרים חשודים.

מעקב מהיר אחר zpskon_12****.exe הסגיר את תפקידם: תהליך זה נבר בכל הפינות בעורך הרישום של המערכת (ה-Registry) ותר אחר סיסמאות של תוכנות לניהול והתחברות לשרתי FTP.

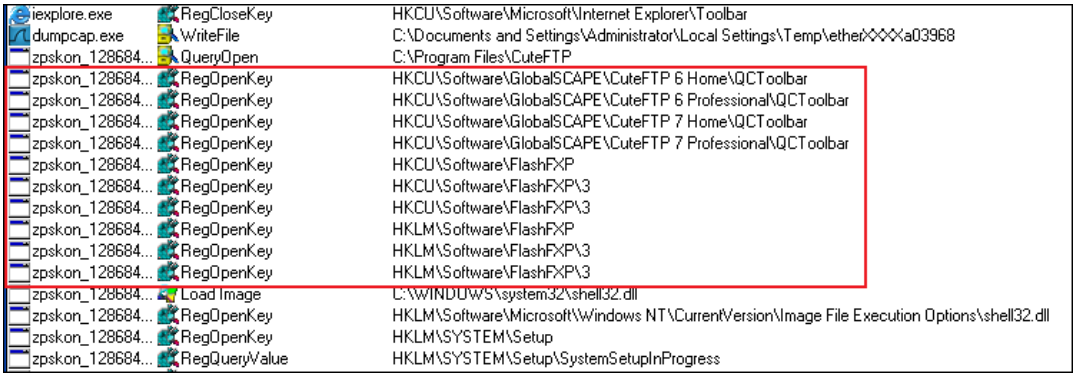
- דוגמה ראשונה:



svchost.exe	CreateFile	C:\WINDOWS\AppPatch
svchost.exe	QueryFileInternalInformationFile	C:\WINDOWS\AppPatch
svchost.exe	CloseFile	C:\WINDOWS\AppPatch
zpskon_128684...	QueryDirectory	C:\wcx_ftp.ini
zpskon_128684...	CloseFile	C:\
zpskon_128684...	RegEnumValue	HKCU\Software\Microsoft\Windows\ShellNoRoam\MUICache
svchost.exe	CreateFile	C:\WINDOWS\system32
svchost.exe	QueryFileInternalInformationFile	C:\WINDOWS\system32

מי שלא מכיר- הקובץ "wcx_ftp.ini" הוא חלק מה-Password Manager של מנהל הקבצים Total Comander. המידע אומנם נשמר באופן מוצפן אך פותחו בעבר הכלים הדרושים בכדי לפענח את ההצפנה.

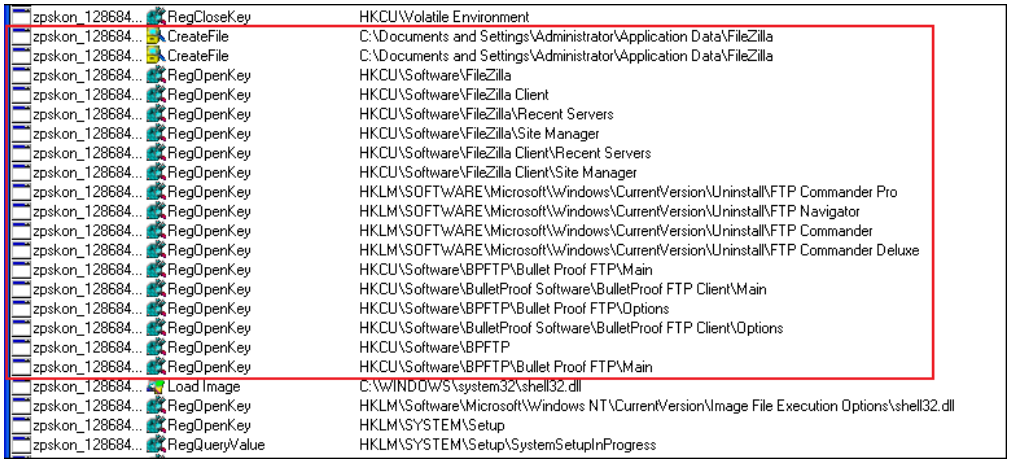
- דוגמה שניה:



iexplore.exe	RegCloseKey	HKCU\Software\Microsoft\Internet Explorer\Toolbar
dumpcap.exe	WriteFile	C:\Documents and Settings\Administrator\Local Settings\Temp\ethereXXXXa03968
zpskon_128684...	QueryOpen	C:\Program Files\CuteFTP
zpskon_128684...	RegOpenKey	HKCU\Software\GlobalSCAPE\CuteFTP 6 Home\QCToolbar
zpskon_128684...	RegOpenKey	HKCU\Software\GlobalSCAPE\CuteFTP 6 Professional\QCToolbar
zpskon_128684...	RegOpenKey	HKCU\Software\GlobalSCAPE\CuteFTP 7 Home\QCToolbar
zpskon_128684...	RegOpenKey	HKCU\Software\GlobalSCAPE\CuteFTP 7 Professional\QCToolbar
zpskon_128684...	RegOpenKey	HKCU\Software\FlashFXP
zpskon_128684...	RegOpenKey	HKCU\Software\FlashFXP\3
zpskon_128684...	RegOpenKey	HKCU\Software\FlashFXP\3
zpskon_128684...	RegOpenKey	HKLM\Software\FlashFXP
zpskon_128684...	RegOpenKey	HKLM\Software\FlashFXP\3
zpskon_128684...	RegOpenKey	HKLM\Software\FlashFXP\3
zpskon_128684...	Load Image	C:\WINDOWS\system32\shell32.dll
zpskon_128684...	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\shell32.dll
zpskon_128684...	RegOpenKey	HKLM\SYSTEM\Setup
zpskon_128684...	RegQueryValue	HKLM\SYSTEM\Setup\SystemSetupInProgress

חיפוש אחר התוכנות "FlashFXP" ו-"CuteFTP" של GlobalSCAPE.

- דוגמה שלישית:

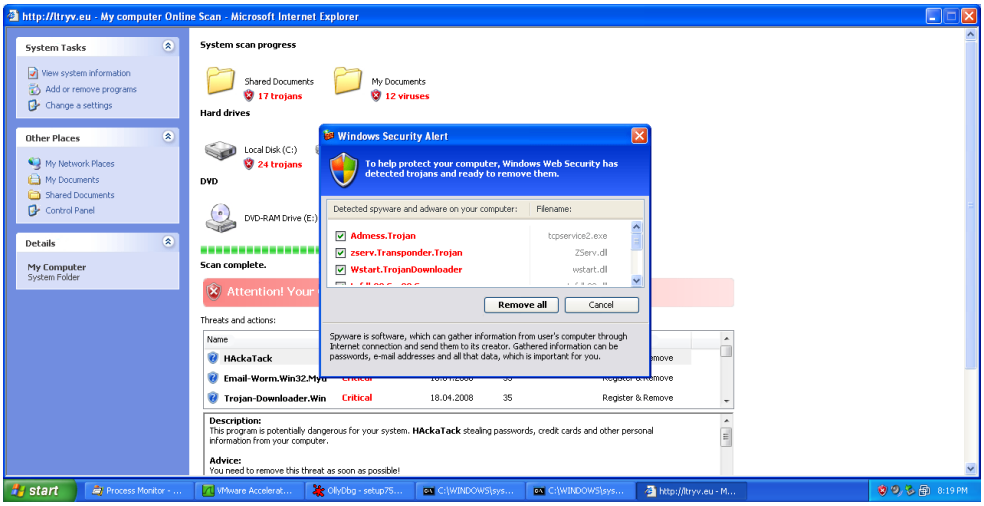


zpskon_128684...	RegCloseKey	HKCU\Volatile Environment
zpskon_128684...	CreateFile	C:\Documents and Settings\Administrator\Application Data\FileZilla
zpskon_128684...	CreateFile	C:\Documents and Settings\Administrator\Application Data\FileZilla
zpskon_128684...	RegOpenKey	HKCU\Software\FileZilla
zpskon_128684...	RegOpenKey	HKCU\Software\FileZilla Client
zpskon_128684...	RegOpenKey	HKCU\Software\FileZilla\Recent Servers
zpskon_128684...	RegOpenKey	HKCU\Software\FileZilla\Site Manager
zpskon_128684...	RegOpenKey	HKCU\Software\FileZilla Client\Recent Servers
zpskon_128684...	RegOpenKey	HKCU\Software\FileZilla Client\Site Manager
zpskon_128684...	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\FTP Commander Pro
zpskon_128684...	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\FTP Navigator
zpskon_128684...	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\FTP Commander
zpskon_128684...	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\FTP Commander Deluxe
zpskon_128684...	RegOpenKey	HKCU\Software\BPFTP\Bullet Proof FTP\Main
zpskon_128684...	RegOpenKey	HKCU\Software\BulletProof Software\BulletProof FTP Client\Main
zpskon_128684...	RegOpenKey	HKCU\Software\BPFTP\Bullet Proof FTP\Options
zpskon_128684...	RegOpenKey	HKCU\Software\BulletProof Software\BulletProof FTP Client\Options
zpskon_128684...	RegOpenKey	HKCU\Software\BPFTP
zpskon_128684...	RegOpenKey	HKCU\Software\BPFTP\Bullet Proof FTP\Main
zpskon_128684...	Load Image	C:\WINDOWS\system32\shell32.dll
zpskon_128684...	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\shell32.dll
zpskon_128684...	RegOpenKey	HKLM\SYSTEM\Setup
zpskon_128684...	RegQueryValue	HKLM\SYSTEM\Setup\SystemSetupInProgress

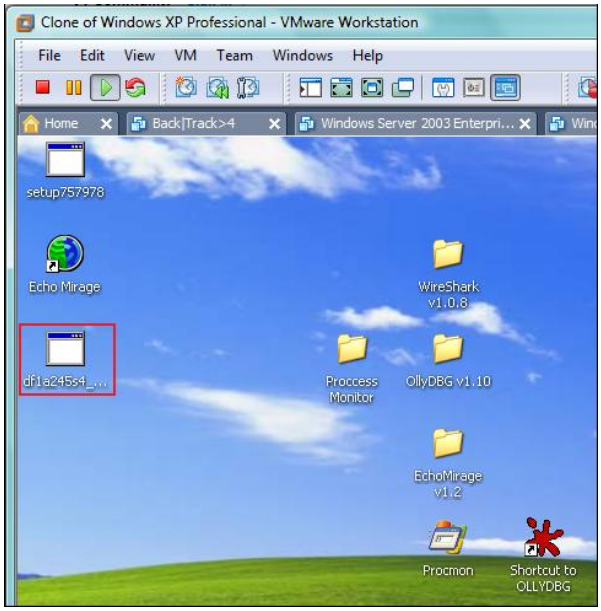
חיפוש אחר "FileZilla" (שגם ל-Password Manager שלה לא חסר), חיפוש אחר " FTP Commander Deluxe/Pro", חיפוש אחר "Bullet Proof FTP".

ושלל תוכנות FTP נוספות...

בקשר ל-fd1a245s4_868.exe, לא ניתן להגיע איתו כל כך רחוק, שלא לדבר על להבין מה הוא עושה. ככל הנראה הוא התהליך שאחראי להקפיץ את החלונות:

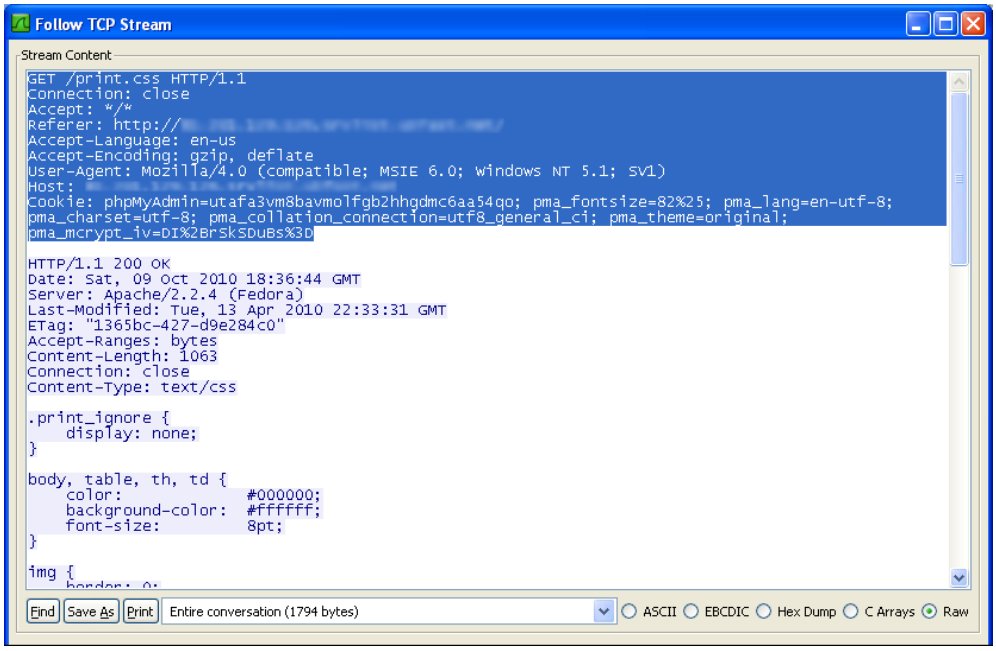


חוסר מקצועיות נוסף שהתגלה הוא שמיקום יצירת קובץ זה לאחר הורדתו נקבע ב-CWD (קיצור של Current Working Directory) ומשם הוא גם מורץ בניגוד לשאר הקבצים (שנוצרים בתיקיות "נשכחות" כגון %Temp% וכו'), דבר המאפשר למשתמש- אפילו התמים ביותר לזהות פעילות חשודה. תחת הגדרות ברירת המחדל של הדפדפן - הקובץ פשוט יווצר על שולחן העבודה של המשתמש:

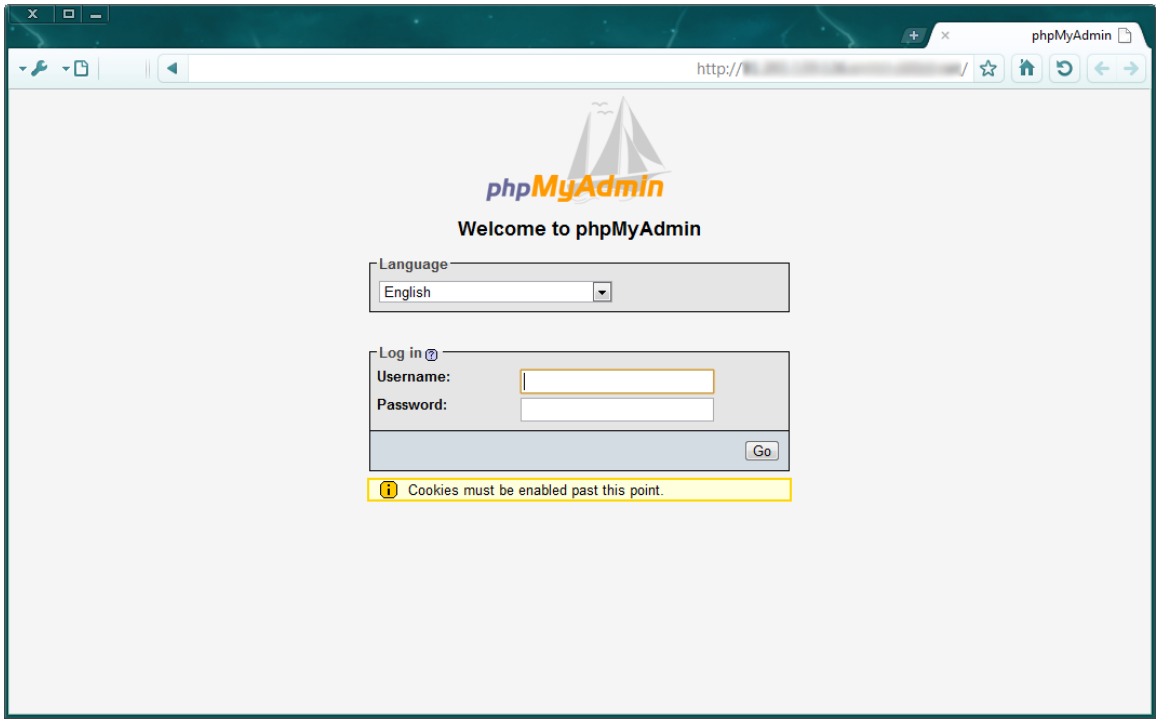


לאחר כל הניתוח הגיע הזמן לחלק הרציני יותר- איתור שרת הניהול של התולעת והשתלטות עליו.

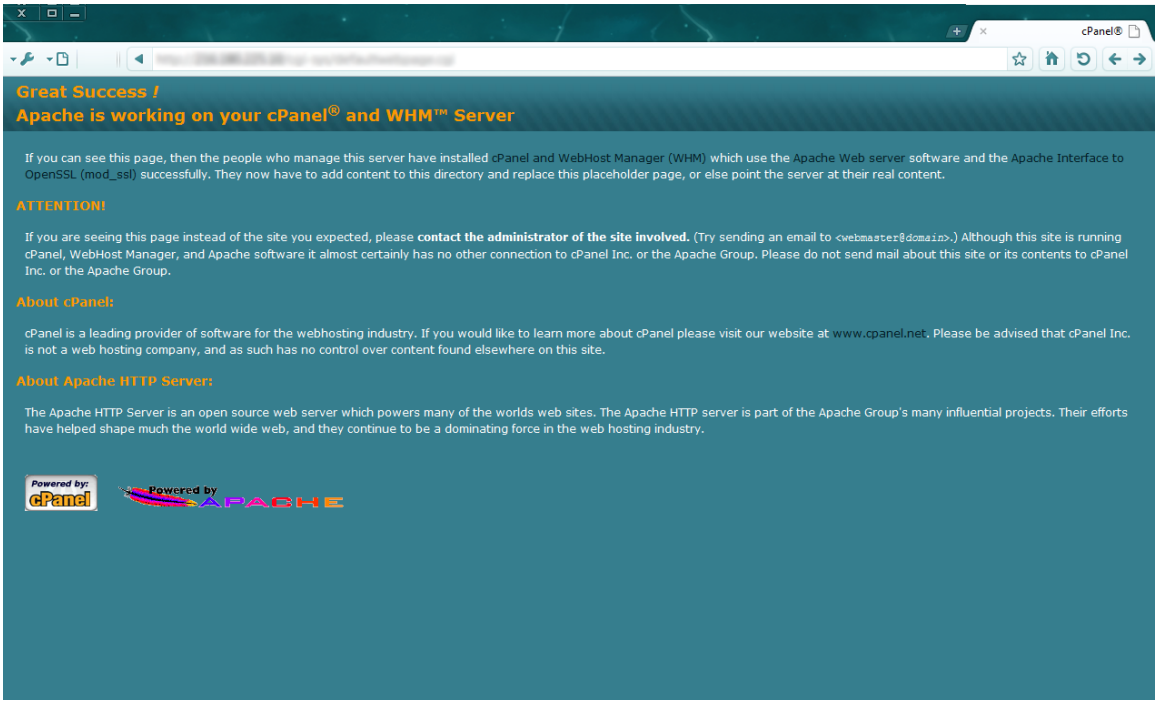
בין פאקטים לפאקטים, הודעות בפייסבוק, הורדה של קבצים בינארים, ושאר Stream של מידע חסר משמעות- נגלה מספר פאקטים מעניינים במיוחד, לדוגמה:



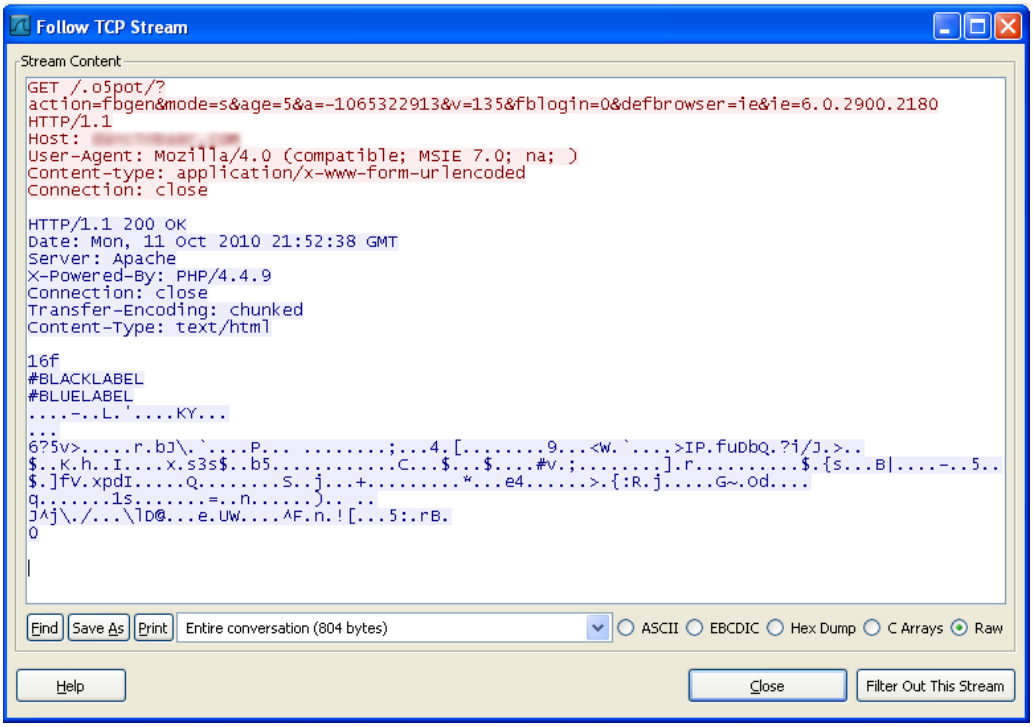
כאשר נכנסתי לאותו עמוד דרך הדפדפן הגעתי, באופן מעניין למדי, לעמוד ההזדהות של מערכת ניהול מסדי הנתונים החופשית- phpMyAdmin:



על אותו שרת מצאתי גם cPanel:



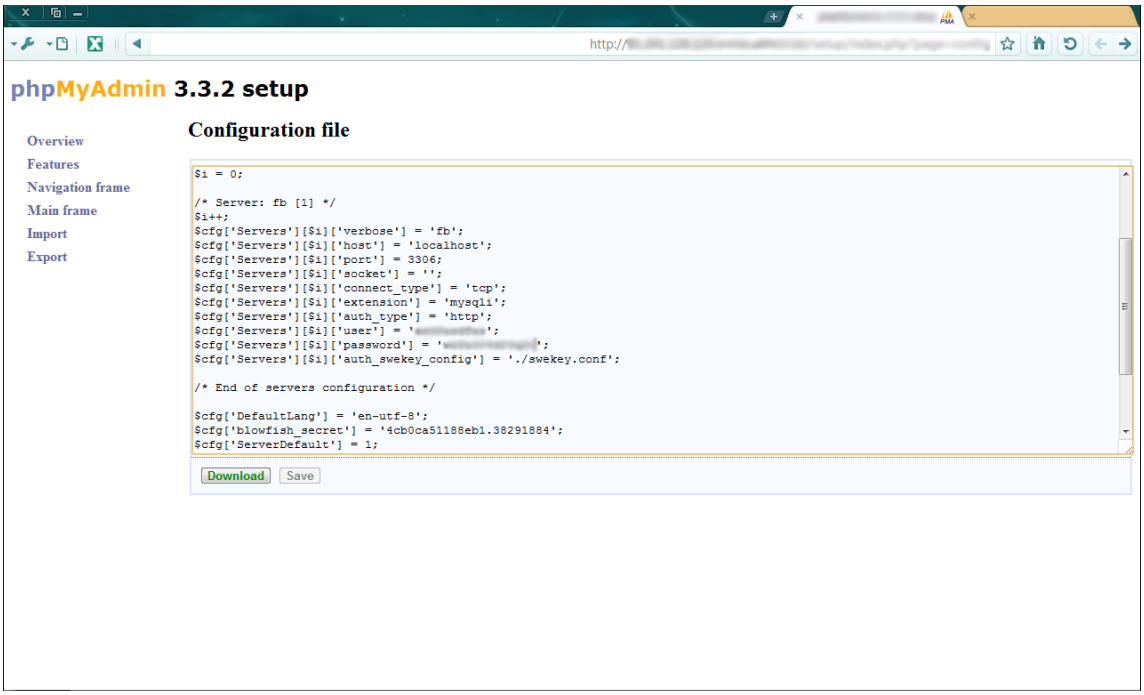
ואל השרת הזה נשלחו גם הנתונים שהתולעת אספה. לדוגמה:



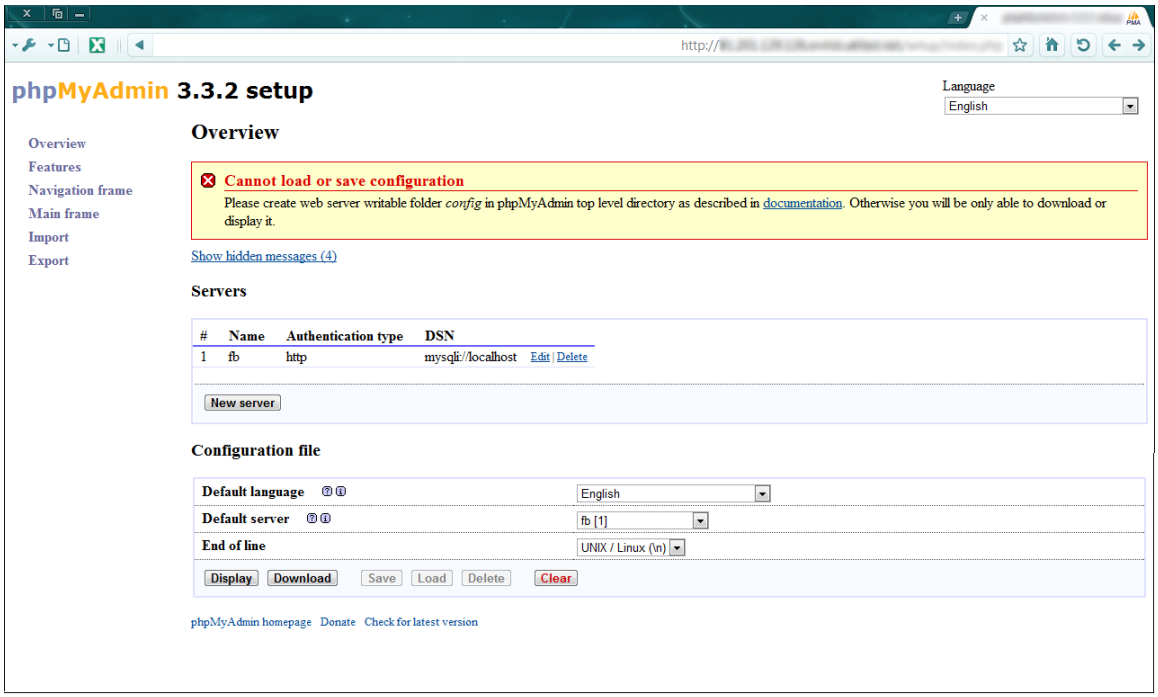
לפי ההגיון הראשוני- פרטי ההזדהות של המערכת אמורים להיות Hard-Coded בתולעת, ובניתוח תחת דיבאגר אני אמור למצוא אותם. כמו כן, פשוט על ידי הסתכלות בלוגים של WireShark אנו אמורים לזהות את הפאקט בו נשלחים פרטי ההזדהות לממשק- וכך לגנוב אותם.

אך מסתבר כי יוצרי התולעת אינם כאלה טפשים- התולעת כלל לא צריכה להזדהות למערכת בכדי להכניס פרטים ומידע על התחנה הנגועה, היא פשוט מאוד ניגשת לקובץ php שמורץ על השרת, טוענת לתוכו את המידע בבקשות GET והקובץ כבר יודע איך לאחסן אותם במסד. זאת אומרת שיש לתולעת אפשרות לכתוב מידע חדש, אך בשום אופן לא לקרוא מידע קיים, שלא לדבר על למחוק או לערוך.

למרות האכזבה, לא אפרט כאן יותר מדי מסיבות השמורות במערכת, אלא רק אגיד שלאחר חקירת המערכת הספציפית על שרת מקומי ובדיקת מספר נתונים עליו, הצלחתי להכנס אל תוך המערכת ולהשיג אליה גישת ניהול. החולשה הייתה בקינפוג מזוויע של תהליך התקנת המערכת, שאיפשר לי לצפות ולהוריד את קובץ הקונפיגורציה שבעזרתו התקינו מסד נתונים בשם "fb" (כנראה קיצור של FaceBook) יחיד שמצאתי במערכת.



השלב השני היה להתפלל שפרטי ההזדהות במסד הנתונים הם הסיסמה של ממשק הניהול... מה שהסתבר כנכון.



☺ GAME OVER!

סיכום

השורה התחתונה של מאמר זה היא שמחקתי את כל מסד הנתונים שנאגר עד כה, שיניתי את הגדרות ההזדהות ודיווחתי לחברת האיחסון על הפעילות שנמצאה בשרתים שלה (עם צילומי מסך וכן הלאה). נכון לכתיבת שורות אלו החשבון אליו שוייך שטח האיחסון + דומיין נסגר והשרת אינו פעיל.

הבעיה היא שלכותבי התולעת אין שום בעיה לשנות קוד התולעת לתקשר עם שרתים חדשים, לקמפל וליצור גל נוסף של מתקפות כאלה בפייסבוק.

זהו מאמר ראשון מסוגו שאני מפרסם במגזין Digital Whisper ואני מקווה שלמדתם ממנו רבות. ניתוח תולעים הוא נושא מעניין ורחב מאוד, דעתי האישית היא שוירוסים ותולעים מתקדמים עושים כיום שימוש בשיא הטכנולוגיה הידועה כעת בעולם המחשבים. במקרה הספציפי שלנו לא היה מדובר בתולעת מסובכת מדי ואפשר לראות שכותביה כמעט ולא ניסו להסתיר אותה- אין כאן שום שימוש בטכנולוגיות שמאפיינות את ה-Rootkits הפשוטים ביותר. במקרים מסויימים נתקלנו בחוסר מקצועיות מפתיע ונראה כי למרות כל הרעש שהתולעת מצליחה לעשות (והיא מצליחה), לא מדובר במצב מתוחכם יתר על המידה. למרות כל הפרסומים, אין מדובר בתולעת מסוג Bot-Net (לפחות לא בגרסא שאני חקרתי) היות ולא בוצעו כלל התקשרויות חשודות מחוץ למערכת ההפעלה (וחבל כי יכול היה להיות מעניין לנתח מקרה שכזה). דבר נוסף הוא, שלדעתי אהפוך את המאמר הזה לסידרת מאמרים-בכל מאמר אחקור ואנתח תולעת אחרת, כך שנוכל לבצע השוואות ולהבין טוב יותר את העולם המעניין הזה.

אין סודות בחברה

מאת אריק פרידמן

הקדמה – על סודות בהצפנה

אחד העקרונות הבסיסיים בתורת הקריפטוגרפיה הוא עקרון קרכהופס (Kerckheoffs's principle), שנקרא על שם אוגוסט קרכהופס, בלשן וקריפטוגרף הולנדי שחי במאה ה-19. קרכהופס מוכר כיום בעיקר הודות לשני מאמרים שפרסם בשנת 1883 (בצרפתית) בנושא קריפטוגרפיה צבאית. עקרון קרכהופס הוא העקרון הידוע ביותר מבין שישה עקרונות של תכנון צפנים צבאיים, שפירסם במאמרים אלה. לפי עקרון זה, סודיות הצפנים נשענת על סודיות של מחרוזת המכונה מפתח ההצפנה, בעוד אלגוריתם ההצפנה עצמו לא דורש כל סודיות. חשיפה של המערכת לא צריכה לגרום לטרחה גדולה מדי (למשל, במקרה שמכונת הצפנה נופלת לידי האויב). במידה והמפתח נחשף, ניתן להחליפו במפתח אחר, בעוד החומרה והתוכנה המממשות את אלגוריתם ההצפנה נשארות על כנן. תקורת החלפת המפתח נמוכה משמעותית מזו של החלפת מערכות הצפנה במלואן. האנטי-תזה לעקרון קרכהופס היא הגנה על ידי הסתרה – מצב בו בטיחות המערכת כולה נשענת על שמירת סוד, אלגוריתם ההצפנה עצמו נחשב סודי; במידה והסוד נחשף המערכת עלולה להישבר.

לדוגמה, סטנדרט ההצפנה הסימטרית המקובל כיום – אלגוריתם AES, נבחר ב-2001 בעקבות תהליך בן 5 שנים, בו נבדקו אלגוריתמים מועמדים בעיניהם הבוחנות של מומחי קריפטוגרפיה מרחבי העולם. אין שום חלק סודי באלגוריתם – הסתרת המידע המוצפן נשענת אך ורק על סודיות המפתח המשמש להצפנה. הדוגמה הנגדית היא צופן סקיפג'ק (Skipjack) שפותח על-ידי הסוכנות לבטחון לאומי (NSA) בארה"ב. התכנון היה לשלב את הצופן במעבד ההצפנה Clipper שהוכרז ב-1993. הצופן סווג כסודי ולכן לא היה חשוף לבחינה של הקהילה הקריפטוגרפית. ב-1998 הורד הסיווג של הצופן, ותוך יום כבר פורסמה התקפה על גרסה מוחלשת של האלגוריתם, שבוצעה על-ידי אלי ביהם, עדי שמיר וחוקרים נוספים.

היחס לסודיות בתהליך ההצפנה הוא אחד מהבדלי הגישה המשמעותיים בין אנשי קריפטוגרפיה לבין האדם מהרחוב (שני ההבדלים המשמעותיים האחרים הם, כמובן, הנטייה הקלה לציניות שמאפיינת אנשי

קריפטוגרפיה, וכן שאם תשאלו אותם לשם הנעורים של אמא שלהם הם יטענו בתוקף שהוא F^sl42!Vsz). כל בוגר קורס קריפטוגרפיה 101 לומד להתייחס בחשדנות לשיטות קריפטוגרפיות סודיות – תכנון צופן הוא משימה קשה ואם עוסק בה רק מספר מצומצם של אנשים תחת מעטה של סודיות, יש סיכוי סביר שפגמים בתכנון יחמקו תחת ידם. לעומת זאת, האינטואיציה של אנשים ללא רקע בתחום, מנחה אותם לראות בסודיות של שיטת ההצפנה גורם חיובי שמעלה את הרף עבור התוקף הפוטנציאלי.

מתברר כי פער זה אינו מוגבל רק לתחום ההצפנה. עוד ב-1993, ציין ג'ון גילמור (אקטיביסט וחלוץ אינטרנט הידוע בין השאר כאחד המייסדים של Electronic Frontier Foundation – EFF) כי רשת האינטרנט מפרשת צנזורה כנזק ומנתבת את דרכה סביב הצנזורה. למרות תכונה מובהקת זו של הרשת, נראה כי ארגונים ומשתמשים רבים שבויים בתפיסה שסודיות וצנזורה מהוות כלים יעילים וניתנים לשליטה. כפי שנראה, גישה בעייתית זו מסתיימת לרוב בעוגמת נפש עבור אותם גורמים.

הבית של ברברה

ב-2002 פתח קנת אדלמן, מתכנת (ומולטי מיליונר) בן 39 ממחוז סנטה קרוז בקליפורניה, בפרוייקט שאפתני: צילום קו החוף של קליפורניה. מטרת הפרוייקט הייתה ועודנה לצלם את קו החוף, על מנת שיהיה ניתן להשתמש בתיעוד זה כנגד פעילויות בלתי חוקית הפוגעות בקו החוף. הפרוייקט התקדם בהצלחה, ועד תחילת 2003 כבר הצטברו באתר מעל ל-12,000 צילומים. אחד מהם (תמונה 3850) היה הצילום הבא ממאליבו, שצולם בשעות הצהריים ב-23 בספטמבר 2002:

הצילום הופיע באתר כשתחתיו הכיתוב "אחוזת סטרייסנד". למי שעדיין לא זיהה, הבית המגודל התופס כ-3% משטח הצילום הינו אחוזתה של ברברה סטרייסנד. עקב הפרסום התברר כי סטרייסנד אינה שבעת רצון מכך שביתה נלכד בעדשת המצלמה ומופיע באתר האינטרנט של הפרוייקט. סטרייסנד פנתה לאתר בדרישה להסיר את התמונה, בטענה כי פרסומה מהווה פגיעה בפרטיות ואיום לבטחונה האישי, מה גם שהתמונה מפרה את חוק "אנטי-פאפארצי" הקליפורני ומטרתה רק להרוויח כסף משמה של סטרייסנד. קנת, שהאמין בצדקת הפרוייקט ולא ראה סיבה לנקוט באפליה לטובת בעלות אדמות חוף עשירות, סרב להיענות לפנייתה. תגובתה של סטרייסנד לא איחרה לבוא בדמות מכתבי אזהרה מטעם עורכי דינה, ובעקבותיהם אף תביעה משפטית בסך של 10 מליון דולר. בסופו של דבר התביעה נדחתה וסטרייסנד נאלצה לשלם לאדלמן הוצאות משפטיות בסך למעלה מ-$150,000.

לכל התהליך הייתה תופעת לוואי מעניינת: התביעה המשפטית משכה תשומת לב ציבורית לא מעטה וסוקרה בעשרות כתבות עיתונות (באתר של אדלמן מוקדש דף מיוחד לנושא). אם עד אז תמונת האחוזה הייתה טמונה עלומה בין 12,000 ויותר תמונות אחרות, הרי שתשומת הלב התקשורתית הבטיחה כי כל מי שלא שם לב לתמונה עד לשלב זה, ידע בדיוק איפה ברברה סטרייסנד גרה ואיך האחוזה שלה נראית. למעשה, בחודש שלאחר הגשת התביעה גלשו לאתר של אדלמן למעלה מ-420,000 מבקרים כדי להעיף מבט בתמונה המדוברת. הפער העצום בין כוונתה של סטרייסנד למנוע את פרסום התמונה לבין התוצאה בפועל, הביא לטביעת המונח תוצא סטרייסנד (Streisand effect) כשם כללי לנסיון צנזורה של פיסת מידע באינטרנט, המביא לתוצאה ההפוכה – תפוצה רחבה של המידע. בהשראת המקרה הוקם גם אתר בשם תוצא סטרייסנד ששם לו למטרה לתעד מקרים דומים של צנזורת מידע כושלת.

09-f9-11-02-9d-74-e3-5b-d8-41-56-c5-63-56-88-c0

דוגמה מאלפת לתוצא סטרייסנד התרחשה במאי 2007, המהומה נסובה סביב מחרוזת בת 128 סיביות אותה ניסתה חברה מסויימת למחות מדפי הרשת. הנסיון הסתיים כמובן בכשלון חרוץ.

כדי להבין מה היה מיוחד כל כך במחרוזת זו נדון בקצרה על DRM (Digital Rights Managaement) – ניהול זכויות דיגיטליות. באופן כללי, מדובר בטכנולוגיה שתפקידה להגן על זכויות יוצרים, או במילים אחרות – למנוע מצב בו כל אחד יכול להוריד מהאינטרנט את הדיסק האחרון של ברברה סטרייסנד מבלי לשלם אגורה. אחד מהאמצעים למימוש DRM הוא סטנדרט מ-2005 שנקרא AACS (Advanced Access

Control System). סטנדרט זה אומץ להגנה על דיסקים של Blu-Ray ו-HD-DVD, והחל מ-2006 כבר נעשה בו שימוש במכשירים ששווקו לציבור הרחב. ב-11 בפברואר 2007 "פוצח" ופורסם מפתח העיבוד של AACS. ניהול המפתחות של AACS אינו הנושא שעל הפרק (הסבר קצר על איך המפתח שנחשף משתלב ב-AACS ניתן למצוא כאן) אך עם זאת, כדאי להבין את המשמעות של חשיפת המפתח: לא מדובר בשבירה כוללת של AACS, מאחר והמפתח ניתן להחלפה וכל הצפנה עתידית של מדיה יכולה להתבסס על מפתח חדש (עקרון קרכהופס!). עם זאת, המפתח שנחשף איפשר לפענח כל כותר HD-DVD שיצא עד אותו זמן. מיותר לציין כי אולפני הסרטים לא אהבו את ההתפתחות הזאת.

לאחר שנחשף המפתח, והסתובב מספר שבועות בפורומים ואתרים שונים, החליטו אולפני הסרטים ו-AACS LA (גוף הרישוי של AACS) לנקוט בפעולה, והחלו לשגר מכתבי אזהרה המורים להסיר מופעים של המפתח מהפורומים והאתרים השונים בהם פורסם, תוך איומים בנקיטת צעדים משפטיים. אחד מהאתרים שזכו לאיומים אלו היה אתר Digg – אתר בו הגולשים יכולים לפרסם לינקים לכתבות באינטרנט ולהמליץ על כתבות שאחרים פרסמו, כאשר הכתבות הפופולריות ביותר מוצגות בדף הראשי של האתר. גולשים באתר Digg פרסמו בו כתבות על המפתח שנחשף, ולכן גם בעלי האתר זכו לקבל מכתב אזהרה. כדי להימנע מהסיכון שיאלצו לסגור את האתר, החליטו ב-Digg לשתף פעולה – הכתבות בהן פורסם המפתח הוסרו וגולשים שהתעקשו לפרסם כתבות נוספות בנושא נחסמו בפני האתר.

עבור הגולשים באתר, זו הייתה הכרזת מלחמה.

האתר הוצף במאות כתבות ואלפי הערות של הגולשים, בהם לקחה המחרוזת האסורה מקום מרכזי – נחשול של יצירתיות שטף את האינטרנט כאשר אנשים התחרו ביניהם על הפצת המחרוזת. למערכה גויסו תמונות, חתולים, חידונים, חולצות, ישו, והיה גם שיר שהוקדש במיוחד לענין (Oh Nine, Eff Nine). לא רק הצנזורה הכעיסה את גולשי האינטרנט, אלא גם עצם הרעיון שגוף כלשהו יכול לקחת מספר שהוא אקראי ביסודו ולהכריז עליו כלא חוקי ואסור להפצה. אתר Freedom to Tinker החל בתגובה לחלק בעלות על מספרים אקראיים בני 128 סיביות.

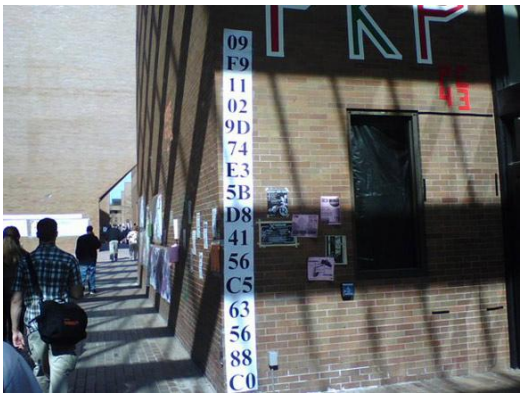
הנה כמה דוגמאות הממחישות את היצירתיות שהופגנה במערכה זו:

The best riddle you will hear today. Period.

1. Directory assistance service number in Moscow, Russia...?
2. A function key on a computer keyboard following F8 and preceding F10...?
3. Yao Ming's (Houston Rockets) jersey number...?
4. Scientific symbol for molecular oxygen also known as dioxygen...?
5. Number of New York state route also known as a Rear Mountain-Beacon Highway...?
6. Number of U.S. interstate that runs from Iowa to Ohio...?
7. Non immigrant visa allowing Australian citizens to live and work in the United States...?
8. Number of vertebrate animal form, required for all research involving vertebrate animals that is conducted in a regulated research institution...?
9. The eight-sided die is also known as...?
10. The international direct dialing code for Switzerland...?
11. The number of consecutive games in which Joe DiMaggio had a base hit in 1941 (still a record)...?
12. The fifth generation of the Chevrolet Corvette sports car is known as...?
13. NBA playoff record for most points scored in a playoff game, achieved by Michael Jordan in 1986, is...?
14. The number of men who signed the United States declaration of independence in 1776...?
15. Atomic number of radium...?
16. IATA code for Centralwings Airline...?

ANSWERS:

1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.
09	**F9**	**11**	**02**	**9D**	**74**	**E3**	**5B**	**D8**	**41**	**56**	**c5**	**63**	**56**	**88**	**c0**



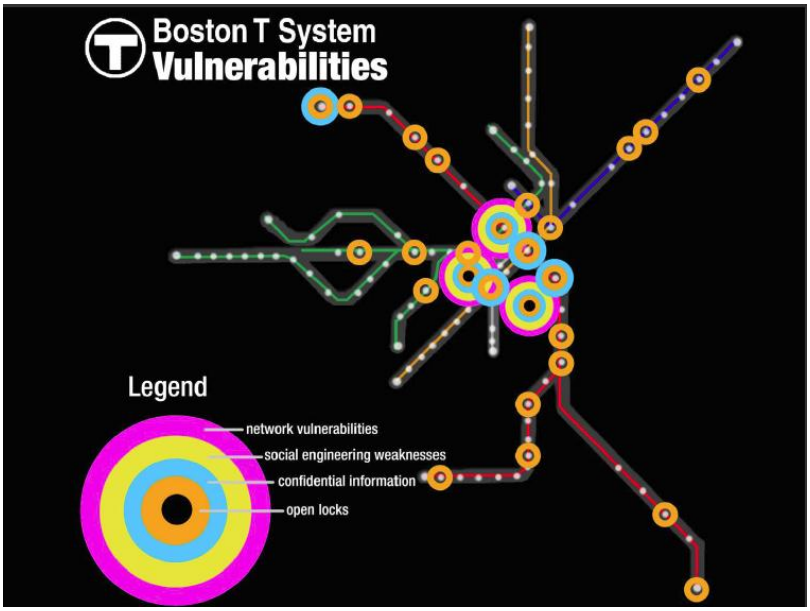
בשלב זה, היה כבר ברור לאנשי AACS LA כי העניינים יצאו מכלל שליטה. אחד ממנהלי AACS LA התייחס להתפתחויות במילים "interesting new twist". לאור התגובה החריפה של הגולשים באתר, מפעילי Digg הבינו כי המשתמשים מעדיפים לראות את Digg נלחם עד לאבדון ולא מתקפל מול הלחץ המשפטי, ובתגובה שינו את החלטתם הקודמת ולקחו את הצד של המשתמשים.

נכון להיום, חיפוש מחרוזת המפתח באינטרנט מניב למעלה ממליון וחצי תוצאות.

רשות התחבורה מנסה להשתיק ביקורת

לאור הנסיון העגום והפומבי של AACS LA עם צנזורה ברשת, היה מקום לצפות שהתקרית תהווה תמרור אזהרה לגורמים אחרים המנסים להעלים מידע בעל עניין הציבור מהאינטרנט. למרות זאת, לא עבר זמן רב ותוצא סטרייסנד היכה שוב.

ב-2008 העביר פרופ' רון ריבסט (ה-R של RSA) ב-MIT את הקורס 6.857, שנושאו אבטחת מחשבים ורשתות. כחלק מדרישות הקורס, הסטודנטים נדרשו להגיש פרוייקט סיכום. שלושה סטודנטים, זאק אנדרסון, ראסל ריאן ואלסנדרו צ'זה, בחרו כנושא עבודה את ה-MBTA (Massachusetts Bay Transportation Authority), מערכת התחבורה הציבורית של בוסטון רבתי. במסגרת הפרוייקט, בחנו הסטודנטים שלל כשלונות אבטחת מחשבים ורשתות ב-MBTA: כשלונות בהגנה פיסית (מנעולים פתוחים ועמדות בקרה ללא השגחה), זיוף כרטיסי נסיעה מגנטיים, האזנה לתקשורת RFID של כרטיסי נסיעה חכמים וחשיפת המפתח, או התחברות לא מורשית לרשת המחשבים של המערכת.



הסטודנטים תכננו להציג את העבודה שלהם בכנס ההאקרים DEFCON באוגוסט 2008, אך MBTA חששו מהחשיפה השלילית ובמקום לאמץ את הביקורת ולבחון כיצד לתקן את הכשלים, בחרה המערכת להתקיף והגישה תביעה נגד הסטודנטים ו-MIT. בטווח הקצר, הטקטיקה של MBTA הצליחה: השופט אישר צו איסור פרסום זמני אשר מנע מהסטודנטים להציג את העבודה בכנס. אף על פי כן, התוצאה של צו איסור הפרסום הייתה, באופן בלתי נמנע, שהזרקור הציבורי הופנה מייד לסיקור הפרשה. צו איסור הפרסום התברר כלא יעיל; באי הכנס קיבלו דיסקים הכוללים עותק של המצגת שיועדה להצגה בכנס (זו נשלחה למארגני הכנס עוד לפני שהצו יצא) ועותק של המצגת הוצמד בשוגג כראייה לתיק התביעה, שפורסם באתר בית המשפט המחוזי, כך שלמעשה המצגת עם הפרטים הבעייתיים הייתה זמינה לכל. אם במקור מטרת הפרוייקט היתה להגיע לעיני קהילה מצומצמת של באי הכנס, הרי שה-MBTA במו-ידיהם הביאו לכך שהביקורת החריפה תגיע לציבור הרחב. יתר על כן, עקב צו איסור הפרסום, אחד-עשר מומחי אבטחה התגייסו וכתבו לבית המשפט מכתב התוקף את החלטתו לצדד ב-MBTA, בו הדגישו את חשיבות הדיון הפתוח למחקר בתחום מדעי המחשב ולשיפור בטיחות הציבור באמצעות חשיפת הכשלים והפעלת לחץ לתיקונם.

מילות סיכום – זווית ישראלית

אף על פי שהוכח שוב ושוב כי קיים קושי לצנזר מידע בעידן האינטרנט מרגע שיצא לחופשי, נראה כי עדיין ישנם גורמים השבויים בתפיסה הארכאית, שביכולתם להשתמש בכלים משפטיים כדי לשלוט על הפצת המידע. עמוד הויקיפדיה על תוצא סטרייסנד מתעדכן מדי פעם בדוגמאות מסוג זה.

גם בארץ ניתן מדי פעם להתקל במקרה אבסורדי, בו צו איסור פרסום מונע כיסוי עיתונאי של ידיעות הזמינות ברשת לכל המעוניין. ב-2008 בית המשפט התעלם מהאינטרנט והטיל צו פרסום על פרשייה שנגעה לאולמרט, ראש הממשלה דאז, למרות שכל הפרטים היו נגישים בניו-יורק פוסט. מקרה מופרך יותר היה המעצר של ענת קם, שלמרות צו איסור הפרסום זכה לחשיפה רבה (אתר העין השביעית נקט בדרך יצירתית לעקוף את הצו ולעודד את הקורא לחפש את המידע לבד). כמו כן, בבלוג של אורי ברייטמן יש מספר פוסטים ("מדינת ישראל נגד גוגל") המסקרים את הגישה הלא יעילה שגופים ממשלתיים נוקטים כדי להשיג ערפול תקשורתי.

בעולם אבטחת המידע יש מקום לקוות כי הקושי בשמירת סודות יאלץ את הארגונים לנקוט בגישה אוהדת לדיון פתוח באבטחה של מערכות ממוחשבות, ומנגד יעודד תהליכים מסודרים יותר של חשיפת פרצות אבטחה. ואולי גם בעולם ה"אמיתי" יבוא יום בו הגופים הממשלתיים ובית המשפט בישראל יכירו בקיום האינטרנט ובנגישות לאתרים זרים, וינקטו בגישה שפויה יותר ביחס לזכות הציבור לדעת.

מתי אפשר לתפוס שרתים, מחשבים ודיסקים

מאת עו"ד יהונתן קלינגר

הקדמה

בהליך משפטי נדרש לעיתים "לתפוס" חומרי מחשב המצויים אצל הצד השני, בין אם מדובר בהליך פלילי בו החומר הוא של נאשם, או בהליך אזרחי בו החומר מוחזק על ידי צד נתבע או תובע, ויש צורך להוכיח את קיומו או שימוש בו. מאמר קצר זה סוקר את הדרכים בהן ניתן לבקש תפיסה של חומר מחשב וכיצד מבוצעת התפיסה בפועל. כמו כן, המאמר מעלה מספר שאלות הנוגעות לשינויים שחלים כיום בעולם המחשוב והשפעתם על תהליך התפיסה בעתיד. לרוב, בדרך כלל הנתפס הוא דיסקים קשיחים (לדוגמא בש 16886/08 מדינת ישראל נ' משה הלוי, ה"ת 23495-01-10 דני סימנדיוב נ' משטרת ישראל - ימ"ר גליל), אולם לעיתים יתפסו גם שרתים או שרתים המוחזקים על ידי מי שאינו צד לצו התפיסה (בש"א 9455/09 תום קפלן ואח' נ' קבוצת פי.סי.אי.סי בע"מ).

אם כן מתי ניתן לתפוס חומר מחשב?

בהליך פלילי ניתן לתפוס חומר מחשב כחלק מחקירת המשטרה; הסיבות למתן צו חיפוש הן רחבות למדי וכוללות תנאי רחב לפיו די בכך ש"החיפוש בו [במחשב - י.ק] נחוץ כדי להבטיח הצגת חפץ לצורך **כל** חקירה, משפט או הליך אחר;" (סעיף 23 לפקודת סדר הדין הפלילי (מעצר וחיפוש)).כאמור, מדובר בסיבות רחבות למדי הכוללות מעשי הימורים (ב"ש 3707/01 יגודייב אמלטי נ' מדינת ישראל), עבירות מס (מ 11295/04 מדינת ישראל נ' יהונתן רבינוביץ), אחזקת פורנוגרפית קטינים (ב"ש 2428/08 פ 1235/08 מדינת ישראל נ' עגנון יונאי) ועוד. ההסדר הרחב ביותר קובע כי צווי חיפוש ינתנו כעניין שבשגרה, ולעיתים אף עם יד קלה מדי על ההדק לטעמי.

לאחר מתן הצו, חיפוש זה יבוצע רק על ידי בעל מקצוע מיומן, אלא שכאמור, בעלי המקצוע המיומנים לא גיבשו עד כה פרקטיקת חיפוש ראויה (משה הלוי, "ראיות אלקטרוניות: בדיחה ושמה משטרת ישראל," דואר חשמלי, 22.03.2010). מעבר לכך, בתי המשפט לא היו עקביים בנוגע לדרישת נוכחות העדים בעת החיפוש ; בעוד שדיני החיפוש הכלליים קובעים כי חיפוש יעשה בנוכחות שני עדים (וכך אף נפסק בפרשת בש 1153/02 מדינת ישראל נ' מיכאל אברג'יל) במקרים אחרים (כגון ב"ש 1152/03 מדינת ישראל נ' רבינוביץ יהונתן) נפסק כי העדר העדים מוריד ממשקל הראיות אך לא פוסל אותן ובעניין *סימנדיוב* נפסק כי אי-נוכחות העדים אינה מורידה ואינה מעלה מקיום הצו. בתי המשפט אף אישרו תפיסת שרת המכיל חומרים של אחרים (פרשת *רבינוביץ'*) בהליך פלילי.

הליך התפיסה

תפיסת החומר אמורה להתמצות בהעתקתו (ב"ש 93750/06 הלוי משה נ' יאח"ה, ערעור על ההחלטה, ברע"פ 770/07 משה הלוי נ' היחידה הארצית לחקירות הונאה נדחה), לאחר העתקת החומר יש להשיב את החומר לבעליו (ב"ש 3040/05 זיסקינר ואח' נ' מדינת ישראל). אי החזרת החומר עשויה לפגוע ביכולת של הנאשם להתמודד עם האישומים, אולם לעיתים נאסרה החזרת החומר התפוס- כך לדוגמא, בבש 574/08 שוהם ברוך נ' פרקליטות מחוז ת"א, נפסק כי חומרי מחשב המכילים תמונות עירום של מתלוננות לא ימסרו במלואן, אלא רק תמונת הראש, והעיון בהן יעשה רק בנוכחות עורך דינו של החשוד.

תפיסה בהליך אזרחי מבוססת על הליך בשם אנטון פילר. בשנת 1975 ניתנה החלטה בענין Anton Piller Ors & KG v Manufacturing Processes Ltd [1975] EWCA Civ 12. במקרה זה ביקשה חברת אנטון פילר המייצרת מנועים, לערוך חיפוש בנכסים הנמצאים אצל סוכניה בבריטניה שנחשדים בהעברת מידע סודי למתחרים. בית המשפט, בהחלטה חדשנית, אישר לחברה לחפש אצל סוכניה ופסק כי:

> Let me say at once that **no Court in this land has any power to issue a search warrant to enter a man's house so as to see if there are papers or documents there which are of an incriminating nature,** whether libels or infringements of copyright or anything else of the kind. No constable or bailiff can knock at the door and demand entry so as to inspect papers or documents. The householder can shut the door in his face and say "Get out". That was established in the leading case of Entick v. Carrington, in (1765) 2 Wilson. None of us would wish to whittle down that principle in the slightest.
>
> **But the Order sought in this case is not a search warrant**. It does not authorise the Plaintiffs' Solicitors or anyone else to enter the Defendant's premises against his will. It does not authorise the breaking down of any doors, nor the slipping in by a back door, nor getting in by an open door or window. It only authorises entry and inspection by the permission of the Defendants. The Plaintiff must get the Defendant's permission. But it does do this: It brings pressure on the Defendants to give permission. It does more. It actually orders him to give permission - with, I suppose, the result that if he does not give permission, he is guilty of contempt of Court.

כלומר- הצו המקורי היה צו שאפשר כניסה ובדיקה של חומר שלא בכח. במידה והיה מסרב הנתבע לפתוח את הדלת ולאפשר בחינה של החומרים, היה אשם בבזיון בית המשפט אך לא ניתן היה לחפש בחצריו. צו **אנטון פילר** יובא למשפט הישראלי בתקנה 387א לתקנות סדר הדין האזרחי הקובעת כי "בית המשפט רשאי, בצו, בכפוף להוראות סימן א', למנות אדם לשם ביצוע חיפוש, צילום, העתקה או תפיסה של נכסים המצויים בחצרים (להלן – תופס נכסים) אם שוכנע על בסיס ראיות מהימנות לכאורה כי קיים

חשש ממשי שהמשיב או אדם אחר מטעמו עומד להעלים את הנכסים או להשמידם, וכי הדבר יכביד באופן ממשי על קיום ההליך". בשנת 1999 התווסף צו על פי חוק עוולות מסחריות, המאפשר גם שימוש בכח וכניסה לחצרים כאשר העוולה המתבקשת על פי חוק עוולות מסחריות. במרבית המקרים הצו ניתן במעמד צד אחד, כלומר- ללא ידיעת הצד השני על הבקשה עד לאחר החלטה בבקשה. הסיבה לכך היא שבמקרה בו הצד השני יודע על הבקשה, הוא יכול לפעול להעלמת הנכסים או קבצי המחשב.

ההבדל בין הצווים הוסבר בעניין פלונית (בר"ע 210/08 פלונית נ' פלונית): "היקף היריעה הצר של צו חיפוש ותפיסה בחוק עוולות מסחריות ותקנותיו, לעומת היקף היריעה הרחב של סעד חיפוש ותפיסה, המוקנה למבקש, מכח תקנות סדר הדין האזרחי. (...) **אמת המידה החוקתית למינוי כונס לצורך תפיסת ראיות לפי סעיף 16 לחוק עוולות מסחריות, היא של חשש סביר להעלמתן. בעוד אשר תקנות סדר הדין האזרחי מעלות לדרגה של חשש ממשי, את אמת המידה הנדרשת להוכחת העלמת נכסים, תוך מתן הגנה רחבה יותר לבעל הדין נגדו מכוון הצו**".

מגבלות, בעיות וחסרונות

מאז הפסיקה בעניין אנטון פילר ולפחות בישראל, הורחבו העילות למתן צו והיכולות של מקבל הצו לעשות בו שימוש נרחב. ראשית, הסיבות למתן צו חיפוש במחשבים הורחבו לעובדים המחזיקים חומר של מעביד לשעבר (בשא (ת"א) 10105/07 כלל פנגסים בטוחה ברוקראז' בע"מ נ' בני דקל), הפרת פטנט (בשא (י-ם) 814/05 אורבוטק נ' קמטק), הוכחה כי הועתקו קבצים ומסדי נתונים (רעא 11356/05 דף רץ שירותי הדפסה בע"מ נ' דן אנד ברדסטריט(ישראל) בע"מ) או פגיעה בפרטיות (עניין *קפלן*). בכל המקרים נדרש להראות כי ביצוע הצו נחוץ על מנת למנוע העלמה של נכסים שהיו מצויים בשליטת הנתבע, וכי ללא הצו יש חשש ממשי שאלו יועלמו.

החיפוש והתפיסה מבוצעים על ידי כונס נכסים הנדרש להיות נייטרלי להליך (ע"א 219/07 עמוס חכמון נ' LDI-Licensing Dynamics International Ltd), ובמקרים בהם כונס הנכסים נגוע בניגוד עניינים או מהווה יד ארוכה של אחד הצדדים, ניתן לפסול אותו ואת הראיות שהביא. תקנה 9 לתקנות עוולות מסחריות קובעת כי "כונס נכסים לא יעשה שימוש במידע או במסמכים שהגיעו אליו עקב תפקידו, ולא יגלה אותם לאחר, אלא לצורך ביצוע תפקידו, מכוח חובה על פי דין למסור מידע או אם הורשה לכך על ידי בית המשפט, וינקוט אמצעים, ככל הדרוש, כדי להבטיח שהעובדים בשירותו ישמרו על סודיות כאמור".

הליך התפיסה יכול לכלול תפיסה של חפצים וחומרי מחשב, אך בתי המשפט נוטים שלא להבהיר האם מדובר בחיפוש גם בתוך קבצי המחשב, או רק העתקה והחזקה של כלל הקבצים. במקרה אחד (עניין *כלל פנגסים בטוחה ברוקראז'*), קבע בית המשפט כי כונס הנכסים יהיה רשאי לתפוס ולחפש "חוזים, תרשומות, טפסים, הזמנות חשבוניות, מצגות, רשימות אנשי קשר של לקוחות ו/או ספקי המבקשת והתכתבויות (לרבות בדוא"ל) של המשיב בינו לבין עצמו ו/או עם החברה המתחרה ואשר קשורים לעסקי

המבקשת בכל מדיה שהיא, לרבות מדיה מגנטית וממוחשבת, ואשר מצויים בחצרו של המשיב. כמו כן הכונס יהיה רשאי לתפוס את המחשבים ואת המדיות המגנטיות המצויים בחצרי המשיב".

אולם לאחר שנתפס החומר, יש להשתמש בו רק למטרה שלשמה ניתן הצו (עניין *פלונית*) ולא לאפשר שימוש אחר הקרוי "דייג ראיות". לדוגמא, אם נתפס מחשב עקב חשש לגזל סוד מסחרי על פי חוק עוולות מסחריות, ולאחר מכן התגלו ראיות המראות כי הופרו גם זכויות יוצרים, הרי שלא ניתן יהיה להשתמש בהן למטרה שונה מהמטרה לה נתפר הצו. בית המשפט פסק כי "מטרת הצו היא תפיסת חומר ספציפי הנמצא בידי המשיב נגדו מכוון הצו, ולא חיפוש כללי של ראיות ו"דייג" שאינם מתיישבים עם אופיו של הצו" וכי "שימוש בצווים אלו לצורך "דייג" של ראיות אינו מתיישב עם אופיים הדרקוני של הצווים הללו, ולאור נוסחה של הבקשה סבורה אני, כי בעניינו החלק הארי של הבקשה מתייחס, לכאורה, לחיפוש כללי של ראיות שאין להתירו, בוודאי לא במסגרת של מתן הצווים המבוקשים, שהינם פולשניים ויש בהם כדי לפגוע בפרטיותו של אדם, ובפרט במעמד צד אחד" (בשא (ת"א) 3792/06 ברונו אינטרנשיונל בע"מ נ' יצחק גור).

גם לאחר התפיסה לא ברור כי לכונס או לצד המבקש את הצו יש את האפשרות לעיין בחומר (בניגוד להליך פלילי). בבשא (חי') 11352/03 קנקדו בע"מ נ' גילה אבן – פז נתבקש צו אנטון פילר, ולאחר שזה ניתן במעמד צד אחד, נמנע בית המשפט להעניק סעד של עיון במסמכים אלא רק אפשר את שמירתם.

אחת הסכנות בצווי אנטון פילר או צווי חיפוש פליליים היא חשיפה כאשר מדובר בשרת שיתופי (Shared Hosting), מצב בומספר אתרי אינטרנט מאוחסנים על שרת אחד של ספק אחסון. במקרה בו מתקבל צו אנטון פילר לתפיסת השרת עקב הפרת זכויות יוצרים על ידי אחד מאתרי האינטרנט, קודם כל יתפסו ויועתקו חומרי השרת ורק לאחר מכן יבררו מבינם מה משויך ומה אינו משויך לעניין הנדון (עניין *קפלן*). כך, במקרה ובו חומר מוגן בחסיון כלשהוא, ינסו להפריד את החומר ולא יעבירו אותו לצדדים, אלא שהעניין עשוי להתרחש במועד מאוחר מדי (ראו עחה"ס 1/81 פלוני נ' מדינת ישראל, לעניין זה); משמעות הדבר היא שבתי המשפט בישראל טרם התייחסו לסוגיה של שירות אחסון שיתופי (למרות שבעניין *רבינוביץ'* היתה החלטה חלקית בנושא). הבעיה היא שמרגע שמידע מאוחסן על שרת שיתופי, ניתן להגיע גם אליו ולתפוס אותו במסגרת תפיסה של חומר המחשב. מהלך זה עשוי לגרום ליצירת עותקים של ארכיוני דואר אלקטרוני של אדם שאינו צד להליך, ואף לגרום לפגיעה מיותרת בצדדים שלישיים.

אם כן, ראוי לפרש את הליך אנטון פילר ככזה שאינו מאפשר אלא העתקה של החומר המתבקש, בהתאם להלכות *ברונו אינטרנשונל* ו*קנקדו*, בצורה בה יפורט בבקשה היקף החומר הנתפס, כאשר החומר מוחזק על ידי צד שלישי (כלומר מי שהצו לא נתבקש נגדו, אלא מחזיק תמים כמו שירותי אירוח); לדוגמא- המשתמש שכנגדו מתבקש צו התפיסה, חשבון הדואר האלקטרוני הנתפס (במקרה שמדובר נניח בשרת דואר אלקטרוני כמו Gmail) או שם המתחם שקבציו מתבקשים. כמו כן, בעת ההעתקה יש לדאוג לכך שהנזק שיגרם לצדדים שלישיים (לדוגמא, הפלת אתרים) או למחזיק השרת, יהיה מזערי ככל הניתן ושהוצאותיו ישולמו.

בעיה נוספת מתעוררת כאשר מדובר באחסון בענן. במצב כזה מדובר בצו תפיסה על שטח וירטואלי ועל נכס וירטואלי, שהגישה אליו לא בהכרח מתאפשרת על ידי ספק השירותים. בעוד שבמקרה בו מתבקשת תפיסה של שרת אמיתי, ניתן להעתיק בצורה פיסית את הדיסק הקשיח ולחלץ ממנו את המידע לאחר מכן, במצב של תשתיות ענן מאובטחות לא אין ערובה שלספק השירות תהיה נגישות לקבצים המאפשרת את אחזור המידע, ללא הסכמת בעל השרת. במצב כזה נראה כי מנהלי אתר עשויים להיות חסינים בפני חיפוש, עד לתיקון החקיקה בנושא. כלומר, אם ינתן צו נגד ספק אחסון המחזיק עותק מאתר אינטרנט המפיץ סודות מסחריים של חברה מסוימת, הספק יכול להסיר את האתר מהרשת, הוא יכול לתת פרטים על בעל החשבון (בכפוף להגבלות ברע"א 4447/07 רמי מור נ' ברק) אך לא תמיד יכול לאפשר גישה לחומר מוצפן שנמצא על השרת.

סיכום

על מבקש צו תפיסה מוטלת אחריות כבדה: עליו למצוא כונס נכסים נייטרלי אשר יעתיק את החומר מבלי לפגוע בו ובצורה מושלמת, כמו גם להחזיר את החומר למקום. על המבקש נאסר להעביר מידע לצד שביקש את הצו, אלא בהוראת בית המשפט והוא עשוי להיות אחראי על נזקים שיגרמו. כמו כן, הוא אמור לברר מה מהמידע רלוונטי להליך ומה אינו, ולהשמיד מהעותקים המצויים אצלו כל מידע חסוי או שאינו רלוונטי. מנגד, מקבל הצו אמור לבחון את המתבקש כנגדו ולדאוג כי הפרוצדורה מתקיימת בצורה מושלמת: שלא מועתק חומר בניגוד לנהלים, שעדים מפקחים על ההעתקה ושהחומר לא משמש למטרות זרות.

אבטחת חבילות תוכנה

מאת ליאור קפלן (kaplanlior@gmail.com)

הקדמה

הרשאות Root הן הגביע הקדוש של הפריצה לשרתים מבוססי לינוקס ומערכות Unix דומות. אנשים רבים משקיעים זמן ומשאבים גדולים בכדי לאבטח את המערכות, וחברות רבות מרוויחות כסף טוב מסיפוק שירותים כאלה.

עם זאת, משתמשי לינוקס רבים שוכחים שכל התקנת חבילת תוכנה (deb, RPM וכו') מהווה בפועל מתן הרשאות root ליוצר החבילה, כך שמומלץ לחשוב פעמיים לפני שאתם מוסיפים מאגרי תוכנה לא רשמיים של ההפצה כגון dotdeb או getdeb.

אולי כבר התחלתם לחשוד במאגרים לא רשמיים, אך לפעמים מאגרים רשמיים יכולים להיות מסוכנים אף יותר, בדיוק בגלל שיש סבירות גבוהה יותר שתסמכו עליהם. הפצות הלינוקס עושות מאמצים רבים בכדי לבצע בקרה על הגישה למאגרי החבילות בצד אחד של התהליך, ובדיקה כי מידע תקין מגיע בצד השני למנהל החבילות.

מאמר זה יתאר את התהליך המתרחש בהפצות הלינוקס הנוגע לנושאי אבטחה של חבילות תוכנה. הדוגמאות מתבססות על הפצת הלינוקס Debian אותה אני מכיר לעומק, ועל הפצת Fedora הנפוצה, כאשר העקרונות דומים ברוב ההפצות. בנוסף, אציג מחקר שנערך בארה"ב העוסק בפרצות אבטחה במאגרי הפצות הלינוקס ושיטת ניהול החבילות.

ניהול מפתחות

במטרה לחתום על הקבצים השונים, מנהלות הפצות לינוקס מספר מפתחות הצפנה, בדביאן מדובר במפתח ראשי אחד לכל גרסה של הפצה ומספר מפתחות יעודיים למאגרים, חלקם מתחלפים באופן תקופתי. המפתחות נחתמים על ידי מספר חברי הפצה ובראשם ה-ftp-master, ניתן לראות כי לאורך הזמן חוזק המפתחות עולה.

```
# apt-key list

pub  1024D/F42584E6 2008-04-06 [expires: 2012-05-15]
uid  Lenny Stable Release Key debian-release@lists.debian.org

pub  4096R/55BE302B 2009-01-27 [expires: 2012-12-31]
uid  Debian Archive Automatic Signing Key (5.0/lenny) <ftpmaster@debian.org>
```

```
pub  2048R/6D849617 2009-01-24 [expires: 2013-01-23]
uid  Debian-Volatile Archive Automatic Signing Key (5.0/lenny)

pub  4096R/B98321F9 2010-08-07 [expires: 2017-08-05]
uid  Squeeze Stable Release Key <debian-release@lists.debian.org>

pub  4096R/473041FA 2010-08-27 [expires: 2018-03-05]
uid  Debian Archive Automatic Signing Key (6.0/squeeze) <ftpmaster@debian.org>
```

מידע נוסף בנושא המפתחות, נהלים לביטול שלהם ומי מורשה לכך, נמצא בדף מידע יעודי בנושא המפתחות.

פדורה, לעומת דביאן, מחזיקה מפתח הצפנה עבור כל גרסה חדשה, זאת במטרה לחתום את החבילות מיד עם סיום הבניה שלהן. כל מפתח חתום על ידי 2-3 אנשים מהפרוייקט, פרטים נוספים זמינים בעמוד המפתחות של פדורה. ב-Red Hat ישנה התנהגות שונה, השותפים בפרוייקט מעדיפים להישאר עם מפתחות קבועים ולא לשנות אותם בכל גרסה, אך עדיין קיימת הפרדה למספר מפתחות עבור שימושים שונים.

הבדל נוסף בין ההפצות השונות הוא העובדה שהעדכונים של דביאן 5 כבר מכילים את המפתח המיועד לדביאן 6, כך שניתן יהיה לשדרג את ההפצה באופן מאובטח מבלי לייבא מפתח חדש. באופן זה, נשמרת רציפות מבחינת אבטחה גם כאשר משלבים חבילות משתי ההפצות (באופן שוטף או כחלק משדרוג).

מעבר לכך, המפתחות של דביאן נוצרים עם תאריך תפוגה (~3 שנים), כך שחייבים להחליף אותם בשלב כלשהו, בעוד שפדורה אינה מציבה הגבלה למפתחות.

מאגר החבילות

בקרת גישה / זכויות העלאה

השלב הראשון בתהליך האבטחה הוא בקרת הגישה והגבלת זכויות העלאה למאגר החבילות של ההפצה. ההרשאות להעלות חבילות מותרת רק למפתחי דביאן, מעמד הדורש מעבר מבחנים טכניים מסויימים. החלק העיקרי בתהליך מבחינתנו הוא ההזדהות באמצעות מפתח GPG. בעוד שכל אחד יכול ליצור מפתח GPG ולהציג את עצמו כבעל המפתח, דביאן דורשת כי המפתח יהיה חתום ע"י כמה מפתחי דביאן קיימים, וזאת במטרה לאמת את זהות בעלי המפתח. באופן זה מפותחת רשת אמון בין חברי הפרוייקט.

החתימה על המפתח ההצפנה נעשית לאחר פגישה פנים מול פנים ובדיקה של מסמכים מזהים המאמתים את זהות האדם. כמו כן, נהוג לבדוק את כתובת הדואר האלקטרוני המופיע במפתח ההצפנה על ידי שליחת החתימה בדואר לבעל המפתח ולא באמצעות העלאתה לשרת מפתחות ציבורי. נוהג זה אינו מוקפד תמיד ולכן בזמן הקבלה לפרוייקט, נבדק כי כתובת הדואר אליה נשלחים פרטים טכניים בזמן הרישום היא זאת הרשומה במפתח.

כהערה יש לציין כי קיימת דרישה להזדהות בשמך המלא מול הפרוייקט, וזאת בכדי למנוע גישה עם כינויים או שמות לא רשמיים (שלא ניתן לאמת ברוב המקרים). נתקלתי כבר במספר חברי פרוייקט עם שמות לא סטנדרטיים, אך הם דאגו כי אלה יהיו גם השמות הרשמיים שלהם (המופיעים בדרכון או בתעודת הזהות).

בסיום שלבים אלה נוצר אמון בין הפרוייקט לבין החבר בו, ומוענקות לו הרשאות העלאה למאגר החבילות. ההרשאות מחולקות בפועל לגישה לשרת באמצעות מפתח SSH ולבדיקה כי החבילות חתומות על ידי מפתח ה-GPG של החבר בפרוייקט. מכאן, כל קובץ המתווסף למאגר החבילות נבדק לגבי מקורו באופן אוטומטי.

אין ספק כי אדם זדוני שעבר את תהליך הקבלה לפרוייקט יכול להעלות קוד לא מאובטח, בין אם באופן תמים או באופן מכוון. אך מעבר למנהגים מסויימים המצמצים את התופעה, הדרך היחידה למנוע את הבעיה היא לבצע סקרי קוד- דבר שצוותי האבטחה של ההפצות עושים באופן קבוע (אם כי ברור שהם לא יכולים לכסות את כל החבילות).

תהליך העלאת החבילה

במהלך יצירתה של חבילת deb חדשה נוצר קובץ changes המכיל את ה-hash של הקבצים אותם ארוצה להעלות על בסיס שלושה אלגוריתמים (sha1, sha256 ו-md5). הקובץ עצמו נחתם לאחר מכן על ידי המפתח הפרטי שלי על מנת לאמת את מקורם. ניתן לראות דוגמה לקובץ כזה כחלק מהתיעוד של תהליך העלאת גרסה 0.110 של חבילת culmus לדביאן חשוב לשים לב כי בדביאן, החבילה עצמה (קובץ ה-deb) אינה חתומה ישירות, אלא בעקיפין דרך קובץ ה-changes. קבצי המקור חתומים באמצעות קובץ נוסף (קובץ dsc) המשמש לאחר מכן גם במאגר החבילות (עבור apt-get source). נוהג זה שונה בהפצות מבוססות RPM, שם החתימה היא על קובץ ה-RPM עצמו (וגם על ה-source RPM).

```
$ rpm -K -p hspell-1.1-3.fc13.src.rpm
hspell-1.1-3.fc13.src.rpm: RSA sha1 ((MD5) PGP) md5 NOT OK (MISSING KEYS:(MD5)
PGP#e8e40fde)

$ rpm -K -p hunspell-he-1.1-3.fc13.x86_64.rpm
hunspell-he-1.1-3.fc13.x86_64.rpm: RSA sha1 ((MD5) PGP) md5 NOT OK (MISSING
KEYS:(MD5) PGP#e8e40fde)
```

מפתח מספר E8E40FDE זמין כחלק מפדורה ופרטיו:

```
pub  4096R/E8E40FDE 2010-01-19
uid  Fedora (13) <fedora@fedoraproject.org>
```

לפני שהחבילה נכנסת למאגר, מבוצעות בדיקות של חתימת ה-GPG וה-hash של הקבצים השונים. לאחר מכן חבילת מקור נשלחת לשרתי הבניה (build server) על מנת ליצור מקוד המקור את החבילות הבינאריות (deb) לארכיטקטורות נוספות. בסיום התהליך, כאשר שהחבילות מוכנות הן נכנסות למאגר ואליהן מצטרפים קבצי המקור, חתומים על ידי קובץ ה-dsc.

בשלב זה ניתן לראות כי התקנה ישירה של קובץ deb בודד אינה מאובטחת, מאחר והקובץ אינו חתום ואין אימות על מקורו. לעומתו, קובץ rpm בודד הוא חתום ואפשר לסמוך עליו כפי הנראה, ההבדלים נובעים מכך שדביאן היא הפצה המתבססת על מאגרים עוד מתחילת דרכה, בעוד שב-Red Hat הנושא הגיע בפיגור משמעותי של יותר מ-10 שנים ביחס לדביאן (yum נכנס ל-RHEL באופן רשמי רק בגרסה 5). הבדל אפשרי נוסף הוא האופי של שני הפרוייקטים – מסחרי לעומת קהילתי, מכאן נגזרים הדגשים השונים על אמצעי האבטחה.

לסיום, יש לקחת בחשבון גם את גודל המאגר שאותו רוצים לחתום. חתימה על כל קובץ בנפרד היא תהליך "יקר" מאוד, ועדיף במקרים רבים לחתום על ה-hash של הקבצים מאשר על הקבצים עצמם. בצורה זאת גודל המידע הנחתם תלוי במספר הקבצים ולא בגודל של כל קובץ (חתימה על hash של קובץ ISO בגודל DVD זהה לחתימה על hash של קובץ בגודל מגה).

האינדקס

עד כה התייחסנו למאגר החבילות כאוסף גדול של קבצי deb ו-RPM (וגם חבילות מקור), אך למאגר החבילות ישנם מספר תפקידים חשובים נוספים. הראשון שבהם הוא גישה מהירה לקבצים ואילו השני הוא אפשרות לחפש אחר החבילה המתאימה לנו ולבסוף גם לעזור לנו לוודא כי החבילה שהורדנו תקינה.

באינדקס מופיע מידע רב על כל חבילה, אך מבחינתנו מה שחשוב הוא ריכוז המידע לגבי שמות הקבצים וה-hash שלהם למקום מרכזי. הפורמט שונה בין ההפצות, כאשר בדביאן מדובר בקובץ טקסט פשוט, בעוד בפדורה והפצות מובססות yum מדובר בקובץ XML. המידע די דומה בסופו של דבר, ומשמש לאותן מטרות.

דוגמאות למידע מתוך האינדקסים:

דביאן:

```
Package: hspell
Priority: optional
Section: text
Installed-Size: 784
Maintainer: Debian Hebrew Packaging Team <debian-hebrew-
package@lists.alioth.debian.org>
Architecture: amd64
Version: 1.0-4
Depends: libc6 (>= 2.7-1), zlib1g (>= 1:1.1.4-1)
Filename: pool/main/h/hspell/hspell_1.0-4_amd64.deb
Size: 570366
MD5sum: 3f280438e2bf263f4ad7665428050a38
SHA1: 7c9da649a727339ed91f5d981922ebb1e40e51ae
SHA256: 083ed6fee0da479c00c9dff355e4ca04f7d5a56b56a93a70d2d698f24ec9f801
```

פדורה:

```
<package type="rpm">
  <name>hunspell-he</name>
  <arch>x86_64</arch>
  <version epoch="0" ver="1.1" rel="3.fc13"/>
  <checksum type="sha256"
pkgid="YES">8eaaa7bcf6e336b29f24d154705559299e0b616a4bbd321fa257af9486ca1e7f</c
hecksum>
  <summary>Hebrew hunspell dictionaries</summary>
  <description>Hebrew hunspell dictionaries.</description>
  <packager>Fedora Project</packager>
  <url>http://hspell.ivrix.org.il</url>
  <time file="1265400182" build="1263071839"/>
  <size package="467644" installed="3541365" archive="3542068"/>
<location href="Packages/hunspell-he-1.1-3.fc13.x86_64.rpm"/>
```

איך נדע שהאינדקס תקין ולא הוכנסו אליו חבילות שלא אמורות להיות בו? עניין זה כבר תלוי בהפצה. בדביאן, בה קבצי ה-deb אינם חתומים, יש חשיבות לחתימה על האינדקס והדבר נעשה באופן מדורג שיוצג בהמשך. בפדורה ו- Red Hat, קובץ האינדקס אינו חתום ואבטחת החבילות מתבססת על העובדה שקובץ ה-RPM עצמו חתום. openSUSE, שמבנה האינדקס שלו דומה מאוד לזה של פדורה משתמש באפשרויות החתימה על האינדקס.

בהמשך המאמר ננתח את המשמעות של כל אחת מהשיטות של ההפצות השונות, אך תחילה נסקור את השיטה בה מנוהל האינדקס. בדביאן המאגר מחולק למספר חלקים (main, contrib, non-free), כך שבכל גרסה (או "טעם") יש לא מעט קבצים. לשם כך נוצר קובץ ה-Release, שמגדיר את כל הקבצים הרלוונטים ואת ה-hash שלהם.

ה-hash מחושב על פי שלושה אלגוריתמים, וכדי שנדע את המקור של המידע, קיים קובץ Release.gpg המכיל את החתימה על הקובץ באמצעות המפתחות של הגרסה הרלוונטית.

בדוגמה הבאה ניתן לראות את הפלט של בדיקת אימות ידנית (נערכה מול Debian 5.0.2):

```
$ gpg -d Release.gpg
Detached signature.
Please enter name of data file: Release
gpg: Signature made Sat 15 Aug 2009 05:41:08 PM IDT using RSA key ID 55BE302B
gpg: Good signature from "Debian Archive Automatic Signing Key (5.0/lenny)
<ftpmaster@debian.org>"
Primary key fingerprint: 150C 8614 919D 8446 E01E  83AF 9AA3 8DCD 55BE 302B
gpg: Signature made Sat 15 Aug 2009 05:45:22 PM IDT using DSA key ID F42584E6
gpg: Good signature from "Lenny Stable Release Key <debian-
release@lists.debian.org>"
Primary key fingerprint: 7F5A 4445 4C72 4A65 CBCD  4FB1 4D27 0D06 F425 84E6
```

קובץ ה-hash מפנה אותנו לאינדקסים השונים של החבילות, על פי חלקי המאגר ועל פי הארכיטקטורה אליה מיועדים קבצי ה-deb, קבצים אלה מכווצים מטעמי חסכון ברוחב פס. אינדקסים אלו מכילים את המידע על החבילות וכפי שהודגם מקודם, מבחינת אבטחה מדובר בהפניה לקובץ מסויים וה-hash שלו. קבצים נוספים בשם Contents מכילים את רשימת הקבצים בתוך כל החבילות של ארכיטקטורה מסויימת.

לעומת זאת, בפדורה וב- Red Hat מדובר בקובץ XML בשם repomd.xml, המקטלג את החלקים הנוספים של האינדקס במספר קטגוריות כגון מידע על חבילות, רשימת קבצים ומידע נוסף. הקבצים נוספים אף הם קבצי XML, אך הם מכווצים לשם חסכון בתעבורה.

בנוסף, בפדורה הלכו צעד אחד קדימה ושמות החלקים הנוספים מכילים hash כלשהו בשמם זאת על מנת ליצור שמות ייחודיים יותר או פחות צפויים. אף על פי כן, אף אחד מהקבצים אינו חתום על ידי מפתח GPG. openSUSE, לעומת זאת, דאגו לחתימה על הקובץ, הם מספקים את החתימה בקובץ נפרד ואת המפתח עצמו (החלק הציבורי כמובן) בקובץ שלישי. שמות הקבצים ב-openSUSE אינם מכילים את ה-hash, והם מסתפקים בשם הסטנדרטי כמו ב-Red Hat.

אם נשווה את דביאן לפדורה, נבחין כי בדביאן המאגר חתום והחבילות אינן חתומות, בעוד בפדורה החבילות חתומות והמאגר אינו חתום, חשוב לזכור ההבדלים אלו בהמשך הקריאה.

אתרי מראה

במרבית המקרים, בעולם התוכנה החופשית, איננו מקבלים את התוכנה באופן ישיר מההפצה, אלא משתמשים ברשת של אתרי מראה של ההפצה כדי לפזר את עומס ההורדה (קבצי ISO וחבילות). בעוד שאתרי מראה אפקטיביים מאוד לפיזור עומסים, הם מהווים גורם נוסף בו מישהו שולט בקבצים שאנחנו מקבלים.

במקרה האידאלי, בעל אתר המראה מבצע סנכרון (rsync לרוב) המוודא כי הקבצים אצלו עדכניים וזהים לאלה הקיימים בשרת המקור. בעל אתר מראה זדוני תמיד יכול להתערב בקבצים שאצלו ולנסות לספק לכם קבצים שמתפקדים אחרת מאלה שסופקו במסגרת ההפצה.בהמשך המאמר נדגים כיצד ניתן להתערב באתרי המראה בשילוב עם שינוי האינדקס כדי להשפיע על התכנים השונים שהמשתמש מקבל.

מנהל החבילות

APT

APT, מנהל החבילות של דביאן (ואובונטו) מבצע תהליך אימות של האינדקס והורדתו כאשר מורצת הפקודה apt-get update. הקבצים נשמרים כעותק מקומי עד לעדכון הבא:

```
# apt-get update
Get:1 http://mirror.isoc.org.il unstable Release.gpg [835 B]
Get:2 http://mirror.isoc.org.il experimental Release.gpg [835 B]
Get:3 http://mirror.isoc.org.il unstable Release [104 kB]
Get:4 http://mirror.isoc.org.il experimental Release [103 kB]
Get:5 http://mirror.isoc.org.il unstable/main Sources [4,005 kB]
Get:6 http://mirror.isoc.org.il unstable/contrib Sources [38.7 kB]
Get:7 http://mirror.isoc.org.il unstable/main amd64 Packages [6,851 kB]
Get:8 http://mirror.isoc.org.il unstable/contrib amd64 Packages [59.3 kB]
Get:9 http://mirror.isoc.org.il experimental/main amd64 Packages [488 kB]
Get:10 http://mirror.isoc.org.il experimental/contrib amd64 Packages [4,437 B]
```

קובץ ה-Release.gpg מורד ונבדקת החתימה שלו, לאחריו מורדים שאר קבצי האינדקס על פי המוגדר ברשימת המקורות של apt, בדוגמה זו מדובר באינדקס חבילות וחבילות מקור של unstable עבור שני חלקים במאגר (main, contrib), ועבור experimental מדובר באינדקס חבילות (ללא חבילות מקור) עבור אותם שני חלקים של המאגר. חתימות ה-md5sum נבדקות לאורך הדרך.

בשלב ההתקנה, נבדק ה-md5sum של קובץ ה-deb עצמו. אם המצב אינו תקין תתקבל הודעת שגיאה:

```
Failed to fetch
http://mirror.isoc.org.il/pub/debian/pool/main/c/culmus/culmus_0.110-
1_all.deb Hash Sum mismatch
```

הודעות שגיאה דומות קיימות גם עבור כל אחד מרכיבי האינדקס במקרה וה-hash אינו תקין. הפתרון המומלץ הוא הרצה חוזרת של apt-get update, או החלפת אתר מראה בהנחה שהוא שבור או פגום באופן כלשהו.

YUM

Yum מבצע תהליך דומה לזה של apt-get, אך בפדורה ו-Red Hat אין חתימה עליו, כך שאימות האינדקס לא מבוצע מעבר לרמת ה-hash של הקבצים. עבור openSUSE, מבוצע גם אימות של החתימות. במידת הצורך ישנה הודעה המאפשרת ייבוא של המפתח המסופק באותה ספריה. אפשרות ייבוא המפתח תוך כדי ההתקנה, עשויה לאפשר לאתר מראה זדוני ליצור מפתח חלופי, איתו יחתם האינדקס לאחר עריכה, בתקווה כי המשתמש יאשר את השאלה מתוך הנחה כי מדובר בפעולה תקינה. משלב זה והלאה, הדרך כמובן פתוחה.

אבטחת מאגרים

בפברואר 2009, Justin Samuel ו- Justin Cappos ערכו מחקר העוסק בפגיעות של מנהלי חבילות. המחקר מציין שתי התקפות הקשורות למנהלי חבילות, הפשוטה יותר היא עריכה של קבצי האינדקס (meta data) שמטרתה להטעות את מנהל החבילות לגבי תקינות הקבצים, או באמצעות הוספת הפניה לקובץ חדש במאגר כדי "להכשיר" אותו. תקנה זו רלוונטית רק למנהלי החבילות שאינם מסתמכים על חתימות GPG בשלב כלשהו של התהליך (האינדקס או החבילות עצמן).

במידה והמאגרים אכן מסתמכים על חתימות, זיהו החוקרים אפשרות לבצע מתקפות Reply and Freeze, בהן מנהל החבילות מקבל אינדקס תקין וחתום על ידי ההפצה, אך כזה שנוצר בעבר, וידוע כי הוא מפנה לחבילות עם בעיות אבטחה שונות אותן ניתן לנצל.

פתרון אפשרי לבעיה הוא יישום הגבלת זמן על האינדקס, כך שלאחר תקופה מסויימת מנהל החבילות ידרוש לבצע רענון של האינדקס. אולם יישום הרעיון בעייתי במיוחד עבור הפצות בעלות גרסאות יציבות שאינן משתנות לאורך זמן, ולכן לא נוצר להם אינדקס חדש. כמו כן, ישנה בעיה בהפצת האינדקס על גבי CD/DVD בשיטה זאת, מאחר והאינדקס שנצרב לא יהיה תקף.

יש לזכור כי אותה בעיה קיימת גם במנגנון ה-cache המקומי של המרבית מנהלי החבילות, מאחר וגם הוא לרוב אינו מוגבל בזמן. משמעות הדבר שלפעמים לא צריך אפילו לבצע התקפה דרך אתרי המראה, אלא מספיק לבצע בדיקה מתי עודכן ה-cache בפעם האחרונה ואילו חבילות מותקנות/יותקנו. ההמלצה לפתאון בעיה זאת היא כמובן עדכון ה-cache המקומי לפני כל רצף פעולות של עדכון חבילות, זאת במטרה לוודא כי מדובר בגרסה עדכנית ואף בכדי לקבל עדכוני אבטחה שונים. עוד בסוף 2008 דביאן התחילה להגדיר את קבצי ה-Release שלה עם תאריך תפוגה של כשבוע, אך ככול הידוע לי, נושא הבדיקה שלהם לא מומש ב-APT עצמו.

לגבי פדורה ו-Red Hat, לא ברור לי למה המאגרים לא נחתמים על ידי GPG, במיוחד כאשר התמיכה בכך קיימת ב-yum. העובדה הנתונה היא שרק החבילות חתומות, כך שניתן להשתמש בחבילות ישנות יותר המכילות בעיות ידועות, ולהציב אותן במאגרים בצורה ישירה. החבילות יעברו את הבדיקה, מאחר ומדובר בחבילות מקוריות. מחקר זה מציין גם כי ישנם מנהלי חבילות שאינם מתיימרים לספק אבטחה כלשהי, וממצבים כאלו מומלץ להזהר.

סיכום

לסיכום, אפשר לראות כי בהפצות העיקריות ישנם מנגנוני אבטחה לנושא התקנת החבילות. המנגנונים הקיימים אינם מושלמים וקיימות בהם בעיות, אך במקרים רבים מדובר בפשרה בין אבטחה לנוחות שימוש, או ליכולות מסויימות המתנגשות עם פתרונות האבטחה החסרים. למעוניינים במידע נוסף, מומלץ לקרוא על Apt-secure, פרוייקט שמוזג לתוך apt ב-2005- http://wiki.debian.org/SecureApt

על המחבר

ליאור קפלן משתמש בתוכנה חופשית למעלה מ-10 שנים, במהלכן הצטרף לפרוייקט דביאן כמתחזק חבילות ותרם לנושא התמיכה בעברית באופן אופיס. בנוסף, הוא מתחזק ב-6 השנים האחרונות את אתרי המראה של עמותת המקור ואיגוד האינטרנט. השנה (2010) ליאור הצטרף לועד עמותת המקור העוסקת בקידום קוד פתוח ותוכנה חופשית בישראל.

רישיון

דברי סיום

בזאת אנחנו סוגרים את הגליון ה-14 של Digital Whisper. אנו מאוד מקווים כי נהנתם מהגליון והכי חשוב- למדתם ממנו. כמו בגליונות הקודמים, גם הפעם הושקעו הרבה מחשבה, יצירתיות, עבודה קשה ושעות שינה אבודות כדי להביא לכם את הגליון. אפיק אפילו לא עשה הכנות לחתונה שלו ועשה לילה לבן ביום החתונה כדי שהגליון בזמן!

אנחנו מחפשים כתבים, מאיירים, עורכים (או בעצם - כל יצור חי עם טמפרטורת גוף בסביבת ה-37 שיש לו קצת זמן פנוי [אנו מוכנים להתפשר גם על חום גוף 37.5]) ואנשים המעוניינים לעזור ולתרום לגליונות הבאים. אם אתם רוצים לעזור לנו ולהשתתף במגזין Digital Whisper – צרו קשר!

ניתן לשלוח כתבות וכל פניה אחרת דרך עמוד "צור קשר" באתר שלנו, או לשלוח אותן לדואר האלקטרוני שלנו, בכתובת editor@digitalwhisper.co.il

על מנת לקרוא גליונות נוספים, ליצור עימנו קשר ולהצטרף לקהילה שלנו, אנא בקרו באתר המגזין:

www.DigitalWhisper.co.il

הגליון הבא ייצא ביום האחרון של נובמבר 2010.

אפיק קסטיאל,

ניר אדר,

30.10.2010