digital whisper
Technologic Papers

טכניקות התרבות בקרב תולעים חברותיות

מאת: אפיק קסטיאל (cp77fk4r)

הקדמה

במסגרת מאמר זה אני מעוניין להציג סקירה על מספר מנגנוני התפשטות של תולעי-אינטרנט שונות שפקדו ופוקדות אותנו בעבר ובזמן האחרון. מטרת המאמר הינה להציג לכם, הקוראים, איך עולם תולעי-האינטרנט בכלל, ומנגנוני ההתפשטות שלהן בפרט הולך וצובר תאוצה בשנים האחרונות.

קיימים מספר רב של וקטורי הפצה בהם תולעי-אינטרנט מבצעות שימוש בכדי להגיע לתפוצה נרחבת, וקטורי הפצה כגון:

- ניצול חולשות במערכת ההפעלה.
- הדבקת התקני אחסון ניידים (USB).
- שליחת אימיילים (Mass-Mailing).
- הדבקת קבצי ברי-הרצה
- הנדסה חברתית.
- רשתות Peer 2 Peer.
- ועוד...

אך במאמר זה אני מעוניין לגעת רק בוקטורי הפצה בהם התולעים מבצעות שימוש בהנדסה חברתית.
מצד אחד, הגיוני מאוד להניח כי מנגנוני הפצה אשר אינן דורשים אינטרקציה של המשתמש ומנצלים חולשות במערכת ההפעלה / דפדפן הם מנגנוני ההפצה הטובים ביותר. אך מצד שני- ברגע שהתולעת נתפסה, נחקרה והובן מהו כשל האבטחה בו היא עושה שימוש בכדי להתפשט, חיי התולעת יהיו קצרים ביותר. אותה החברה שאחראית על המנגנון בו נמצא כשל האבטחה תשחרר טלאי שיסגור אותו, וכאן בערך תמו חייה של התולעת.

מהסתכלות אחורה בזמן, נתן לראות כי דווקא התולעים שלא נצלו כשלי אבטחה אלא עשו שימוש בוקטורי התפשטות אשר כן דורשים אינטרקציה עם המשתמש ומבצעים שימוש בהנדסה חברתית- הן התולעים עם אורך החיים הגדול ביותר.

מדובר בשאלה לא פשוטה, והשאלה האם וקטורים אשר דורשים אינטרקציה עם המשתמש ("user interaction based") הם וקטורי ההפצה הטובים ביותר להפצת תולעים היא שאלה מעניינת בפני עצמה, אך היא אינה תעלה על הפרק במאמר הזה.

ולענייננו, כותב התולעת יכול להשתמש בהנדסה חברתית במספר פלטפורמות שונות, כגון:

- תוכנות מסרים מידיים (ICQ, MSN, Yahoo! Messenger, Skype, ערוצי IRC ועוד).
- משלוח אימיילים (דרך Outlook, שרתי SMTP שונים ו-Webmails)
- רשתות חברתיות (Facebook, Myspace וכו').
- ועוד...

במסגרת המאמר אציג מספר תולעים אשר מבצעות שימוש בפלטפורמות השונות בכדי שנוכל לבצע השוואה.

אני אוהב אותך אנה קורניקובה!

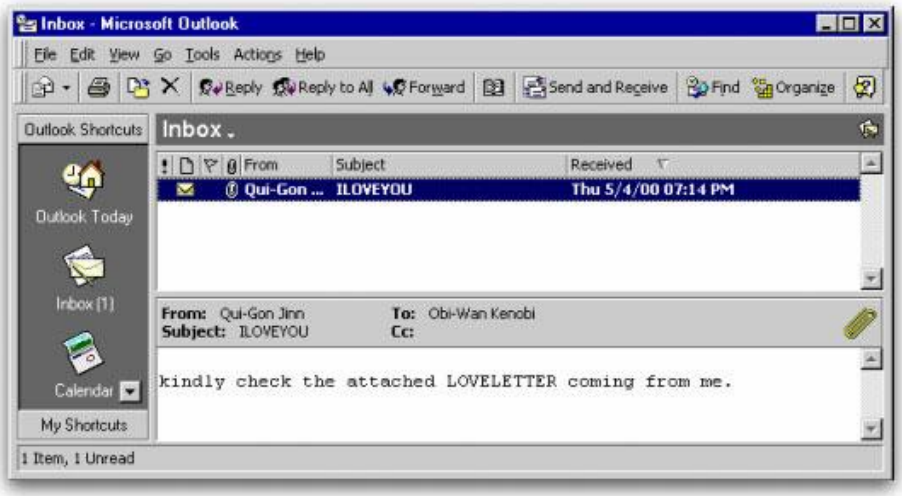
מדובר בשני תולעי-אינטרנט אגדיות (משנת 2000 ו-2001), הראשונה היא ה-"Love Bug" (מוכרת גם כ-"ILOVEYOU" ו-"Love Letter") והשניה היא כמובן התולעת: "VBS.SST@mm", או כמו שכל המדיה באותה התקופה כינתה אותה: "The Anna Kournikova Worm".

שתי התולעים אללו התפשטו בעזרת משלוח הודעות דוא"ל. שתי התולעים הפיצו את עצמן בעזרת התממשקות לתוכנת ה-Outlook שעל המחשב בו הן נפתחו ושלחו את עצמן כקובץ מצורף לאימייל אשר נשלח לכלל רשימת אנשי הקשר של הקורבן.

בשתי התולעים לא נוצלה אף חולשה בקוד של אף אחד מהמנגנונים שליוו את השליחה (כגון חולשות לוגיות או חולשות מבוססות זכרון כמו שנצפה בתולעים אחרות), אלא פשוט התממשקות לתוכנת ה-Outlook בעזרת שורות סקריפט לפקדי מאקרו של התוכנה (אובייקטים כגון Outlook.Application ב-WSH ו-VBS עושים את העבודה יופי).

התולעת "ILOVEYOU" הפיצה אימייל עם הכותרת "ILOVEYOU" ובתוכנו היה רשום המשפט:

```
Kindly check the attached LOVELETTER coming from me"
```



(במקור: http://iamjenessa.wordpress.com/2011/06/28/memories-of-the-love-bug-worm-by-graham-cluley-on-may-4-2009/)

לאותו האימייל היה מצורף קובץ- "מכתב אהבה" בשם: "LOVELETTER.TXT.VBS" או "LOVE-LETTER-FOR-YOU.TXT.VBS". הרעיון הוא שאז, במערכת ההפעלה Windows, ברירת המחדל הייתה לא להציג את סיומות הקבצים, כך שהקובץ הוצג כ-"LOVELETTER.TXT". כמובן שכאשר הקורבן היה לוחץ על הקובץ במחשבה שהוא הולך לקרוא מכתב אהבה- הוא בעצם הריץ את אותו קובץ VBS שהכיל את התולעת שהייתה מדביקה לו את המחשב ומפיצה עצמה לכלל רשימת אנשי הקשר שלו.

התולעת השניה, על שם שחקנית הטניס הרוסיה אנה קורניקובה, הרעיון הוא אותו רעיון. המימוש זהה כמעט לחלוטין, אך במקום לקבל מכתב אהבה, התולעת הפיצה את עצמה באימיילים שהתיימרו להכיל תמונה של השחקנית. נושא ההודעה היה: "Here you have, ;o)" והתוכן היה פשוט: "Check This!". שמו של הקובץ המצורף היה "AnnaKournikova.jpg.vbs", ושוב- עקב הגדרות ברירת המחדל של מערכת ההפעלה Windows, הסיומת ".vbs" הייתה נשמטת.

בכדי שהתולעת לא תרוץ על אותו משתמש מספר פעמים, לאחר הרצה ראשונה, היא הייתה כותבת ערך לעורך הרישום של מערכת ההפעלה, במיקום:

```
HKEY_CURRENT_USER\Software\OnTheFly\mailed
```

וכך, בכדי לא לשלוח לאותה רשימת אנשי קשר את עצמה שנית- הייתה מתבצעת בדיקה לפני כל שליחה- האם אותו מפתח קיים. במידה והיא הייתה מוצאת אותו- לא הייתה מתבצעת השליחה.

ושוב, כאשר הקורבן היה לוחץ על ה"תמונה", התולעת הייתה מורצת ושולחת את עצמה לכלל רשימת אנשי הקשר שלו.

(במקור: http://www.f-secure.com/v-descs/onthefly.shtml)

כשחושבים על שתי התולעים כיום, מפתיע לחשוב שהן הצליחו להתפשט לכל כך הרבה מחשבים. הרי לא נעשה כאן כמעט שימוש בהנדסה חברתית, ואפשר להצביע כאן על מספר נקודות די בעייתיות, כגון זה שהסיומת של הקובץ כאשר הוא מצורף למייל מופיע כ-"TXT.VBS" או "jpg.vbs", או זה שהאייקון של הקובץ נשאר כאייקון של קובץ סקריפט ולא מופיע האייקון של הקובץ שהוא מתיימר להיות.

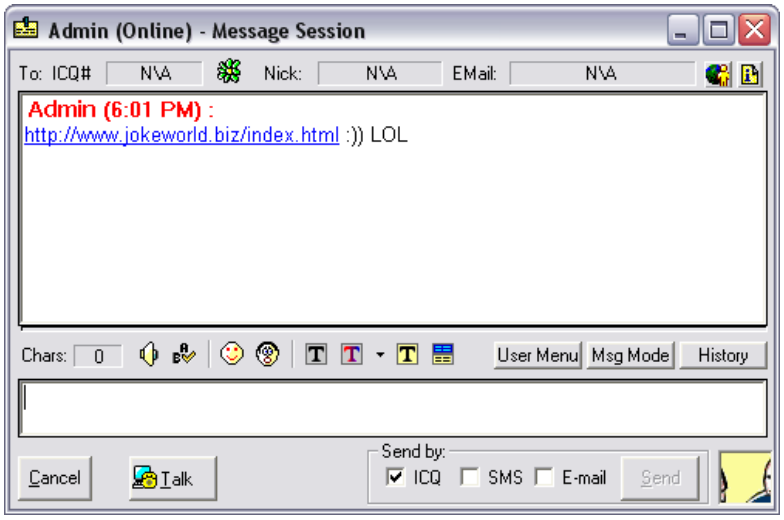
בכדי להבין למה אותן התולעים הצליחו כל כך, אנו צריכים לזכור כי מדובר בתחילת שנות ה-2000, וכמו שכולנו יודעים, קשה להאשים את אותה התקופה במודעות יתר לסיכונים הכרוכים בגלישה באינטרנט. כיום, המודעות לאבטחת מידע ולסיכונים כגון אלו גבוהה יותר. ולכן לתולעים כגון אלו, כיום, כמעט ואין סיכוי ליצור את ההד אותו הן הצליחו ליצור בתחילת העשור הקודם.

דברי אלי בפרחים

סוג התולעים השני עליו נדבר היום הוא ה-"Instant Messenge Worms". מדובר בתולעים שיודעות להתממשק לפרוטוקול של תוכנות המסרים המידיים השונות (כגון ICQ או MSN Messenger) באופן כזה או אחר, ובעזרת גניבת פרטי ההזדהות של בעלי החשבונות השונים שלחו בשמם הודעות לחבריהם עם קישורים לקבצים / אתרים זדוניים אשר הכילו את התולעים עצמן.

לדוגמא, כאשר תולעים כגון "Bizex" או "Stration" היו מורצות במחשב אשר עליו מותקנת תוכנת המסרים המידיים "ICQ" הן היו שולפות את פרטי ההזדהות של המשתמש מאחד מקבצי ה-DAT של התוכנה (הקובץ בו נשמרים פרטי ההזדהות כאשר המשתמש מסמן "Remember Me" בעת ההזדהות לצורכי הזדהויות עתידיות), מפענחות אותם, ומשתמשות בהם בכדי להזדהות בשמו של המשתמש לשרת ה-ICQ ולהוריד את רשימת אנשי הקשר שלו. זאת כמובן בכדי לשלוח בשמו את עצמן לשאר לחבריו. בדרך כלל הן היו שולחות לחברי הקורבן (בשמו כמובן) קישור לאתר אשר דרש מהקורבן להתקין קובץ EXE במסווה של משחק קטן או שומר-מסך נחמד.

דוגמא להודעה שנשלחה על ידי התולעת "Bizex":



(במקור: http://www.kaspersky.co.in/news?id=4277566)

בגרסאות מתקדמות של התולעת, אף נעשה שימוש בחולשה שנמצאה במנוע לפענוח DHTML בדפדפן Internet Explorer (MS03-040) כך שמספיק שהמשתמש היה לוחץ על הלינק, ומבלי להוריד את קובץ Exe הוא היה נדבק.

ICQ אינה תוכנת המסרים המידיים היחידה שכותבי וירוסים ותולעים השתמשו ומשתמשים בה גם היום בתור פלטפורמה להפצת המוצרים שלהם. תולעים אחרות, כגון "Bropia" ו-"Yimfoca" (שמוטציות שונות שלה עדיין רצות בשטח) בחרו להפיץ עצמן דרך תוכנות כגון Msn Messenger ו-Yahoo! Messenger (בהתאמה). הפלטפורמה אולי שונה- אך הקונספט זהה לחלוטין. המשתמש מקבל הודעה ממכר / אדם רנדומלי ומתבקש ללחוץ על קישור באינטרנט. קישור זה בדרך כלל מפנה לקובץ Exe או במקרים אחרים - עמוד המנצל חולשת 0day בדפדפן אשר מריץ קוד ומדביק את המשתמש התמים בתולעת. כאן אציין כי במקרים מסויימים, במידה ולא נשמרו פרטי ההזדהות בקבצים המיועדים לכך, נעשה שימוש ב- Keyboard Sniffing בכדי לדלות את סיסמת החשבון.

עד היום פורסמו לא מעט חולשות בתוכנות מסרים מידיים או בגורמים שונים שניתן היה לנצל באופן מרוחק בכדי לגרום להרצת קוד דרך תוכנות מסוג זה, כגון המקרה הבא, אך בסופו של דבר נצפו מספר קטן מאוד של תולעים שנצלו חולשות אלו. מספר התולעים שניצלו חולשות בפרוטוקול התקשורת, או במנגנון שאחראי על פרסור ההודעות של תוכנת המסרים המידיים בכדי להריץ את עצמן- מאוד נדירות. במקרים שונים, כמו במקרה של התולעת Witty, נעשה שימוש בחולשת Buffer Overflow שנמצאה במנגנון פענוח פרוטוקול ה-ICQ בתוכנות אבטחה שונות, כגון: BlackICE ו-RealSecure (שתיהן של ISS) בכדי להריץ קוד על הקורבן.

תולעי IRC

IRC הינו פרוטוקול המשמש לביצוע שיחות צ'אט רב משתתפים בזמן אמת. שרתי וערוצי IRC קיימים כבר מסוף שנות התשעים, וכותבי הוירוסים לא פסחו עליהם. חשוב להבין את ההבדל בין Botnets שבמספר רב מהמקרים **ארכיטקטורת השליטה עליהם מתבצעת על-גבי שרתי IRC** לבין תולעי IRC שמנצלות את פרוטוקול ה-IRC **לטובת הפצתן**. למידע בנוגע ל-Botnets ניתן לקרוא במאמר: "Botnet - מה זאת החיה הזאת?" שפורסם בגליון השלישי של Digital Whisper.

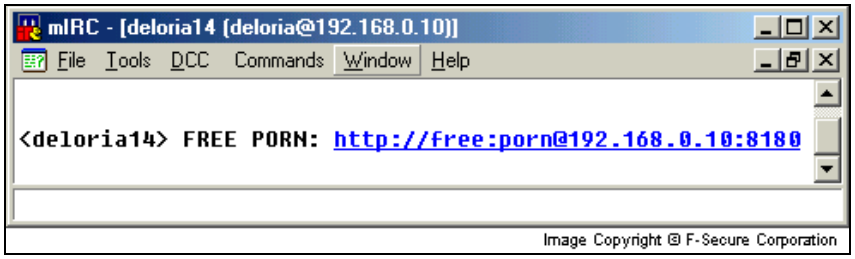
תולעי IRC מתחזות למשתמשי IRC אמיתיים ובעזרת הנדסה חברתית / ניצול חולשות בתוכנות לקוח לפרוטוקול ה-IRC (IRC Clients) מפיצות עצמן. גם בפלטפורמה זאת, המקרים בהם תולעי IRC משתמשות בהנדסה חברתית רבים יותר מתולעים אשר ניצלו חולשות שונות ב-IRC Clients לצרכי הפצה.

אפשר לחלק תולעים מסוג זה לשתי קבוצות:

- תולעים בעלות מנוע IRC מובנה שמאפשר להן להתממשק לערוצי IRC מבלי תלות בתוכנת לקוח ה-IRC שמותקנת על המחשב בו הן רצות.

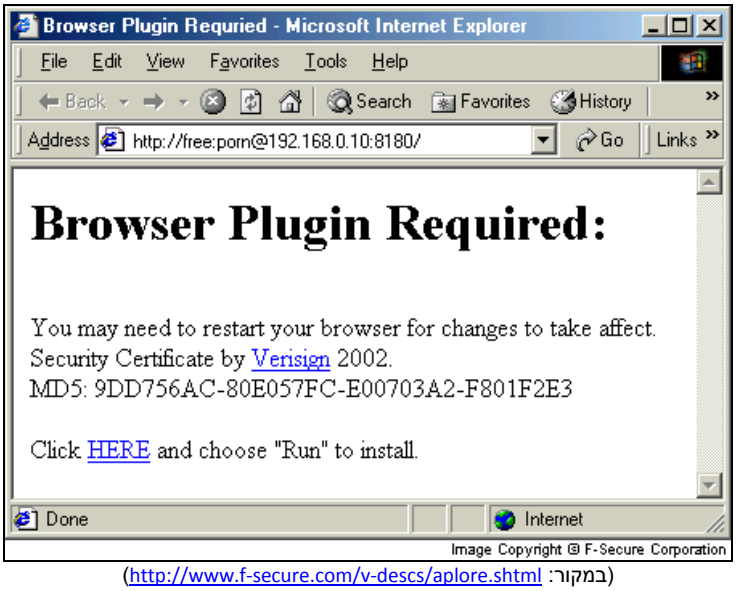
- תולעים חסרות מנוע IRC, אשר מתממשקות לתוכנת הלקוח שמותקנת על המחשב עליו הן רצות ובעזרתן מתקשרות עם שאר משתתפי הערוץ.

נקח לדוגמה את התולעת "Aplore" (מוכרת גם כ-"Aphex") שנצפתה לראשונה בסביבות אמצע שנת 2004. התולעת הפיצה עצמה ע"י מנוע IRC מובנה, שבעזרתו היא הייתה מתחברת לערוצי IRC שונים, ומפיצה הודעה פרטית לכלל המשתמשים הנוכחים בערוץ. תוכן ההודעה הכיל בדרך כלל הודעות בסיגנון "Free Porn" וקישור לכתובת אינטרנט של אתר פורנוגראפי כביכול:



(במקור: http://www.f-secure.com/v-descs/aplore.shtml)

משתמש שהיה נכנס לאתר, היה מתבקש להתקין תוסף לדפדפן הנדרש לצורך צפיה בתוכן האתר:



(במקור: http://www.f-secure.com/v-descs/aplore.shtml)

וכמובן- כל מי שהיה מתקין את התוסף לדפדפן, היה נדבק גם הוא.

לעומת "Aplore", שהכילה מנוע IRC פנימי משלה, תולעים כגון "Momma" ו-"Hellfire" היו תולעים שגם הפיצו עצמן דרך ערוצי IRC אך בשונה מ-"Aplore", הן עשו זאת בעזרת שימוש במנוע הסקריפטינג של התוכנה mIRC (תוכנת לקוח IRC נפוצה). במקרים כאלה יוצר התולעת יכול לבחור בשתי דרכים נוספות להדבקת הקורבן, חוץ מהפניית הקורבן לעמוד עם תוכן זדוני, ניתן לנסות לשכנע את הקורבן להריץ סקריפט (בטענה שמדובר בפקודות הזדהות לערוץ וכו') שיתפקד כ-Backdoor ויאפשר לתוקף שליטה מלאה על תוכנת הצ'אט או שליחת קובץ מדביק על גבי DCC (פרוטוקול נפוץ להעברת מידע Peer to Peer הנתמך במספר רב של לקוחות IRC) שיאפשר גישה למערכת המותקפת. כמובן שלאחר הדבקת המשתמש התולעת אינה נשארת במסגרת ה-mIRC, היא מורידה ומריצה Payloads שונים על המחשב ומקנה לתוקף שליטה מלאה גם על המערכת.

מנוע הסקריפטינג של mIRC (ושאר תוכנות הצ'אט אשר תומכות באוטומציה) מאפשר למשתמש, בין היתר, להגדיר מאקרו- רצף פעולות שיבוצע בכל פעם שאירוע מסויים מתרחש בערוץ IRC בו המשתמש פעיל.

אירועים לדוגמה:

- הרצה ישירה של המאקרו
- הצטרפות לערוץ / שרת
- התנתקות מערוץ / שרת
- הצטרפות משתמש חדש לערוץ
- הופעה של מילה או משפט מסויים בערוץ
- ועוד אירועים רבים...

הפעולות שניתן לבצע הן אינסופיות: מפעולות שניתן לבצע במסגרת ה-IRC (כתיבת הודעה בערוץ, שליחת הודעה פרטית למשתמש, שליחת קובץ למשתמש על גבי DCC, נתינת או לקיחת הרשאות למשתמשים וכו') ועד עבודה על המחשב המקומי (עבודה עם קבצים, הרצת פקודות מערכת, הורדת קבצים מהאינטרנט והרצתם וכו').

שכתוב של קובץ יחיד אשר אחראי על מימוש המאקרו המקושר לאירועים וסיימנו, המשתמש מודבק, אין צורך לבצע Hook לשום פונקציה, ואין צורך לפתוח סוקטים ולפרסר את הצ'אט. תוכנות צ'אט המאפשרות אוטומציה הן מכרה זהב, גם מפני שהן נפוצות וגם מפני שבקלות מאוד ניתן להתממשק אליהן. מסיבות אלו ודומות כמות התולעים מסוג זה היא/הייתה רבה מאוד- כל משתמש ממוצע עם כוונות זדוניות יכול לממש תולעת כזאת גם מבלי להכיר יותר מדי את עולם התכנות.

דוגמאות מעולות לפשטות שבדבר ניתן לראות במאמרים הבאים:

http://users.telenet.be/ahmadi/mircworm.htm

http://vxheavens.com/lib/vsp21.html

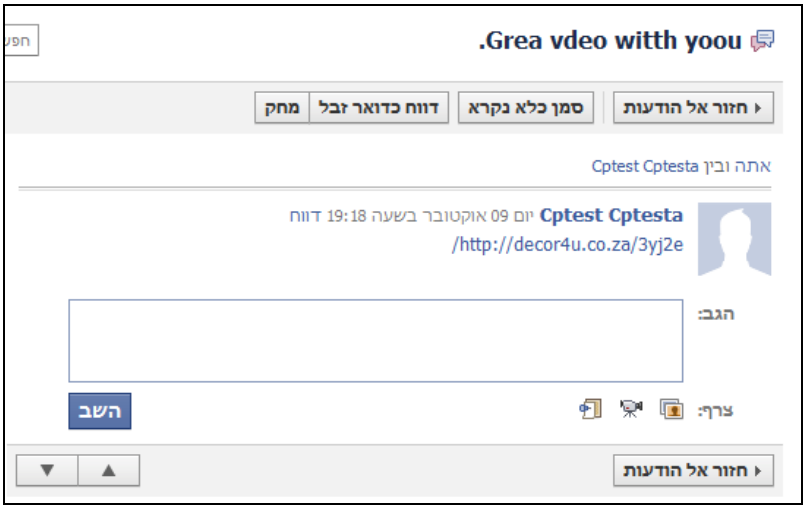
תולעים חברתיות

רשתות חברתיות הן אחת הפלטפורמות הפופולריות כיום בקרב כותבי התולעים, דוגמה טובה לכך אפשר למצוא בחלק הראשון של סדרת המאמרים "Chasing Worms" שפורסם בגליון ה-14 של המגזין, בו הוצג ניתוח של התולעת "Koobface".

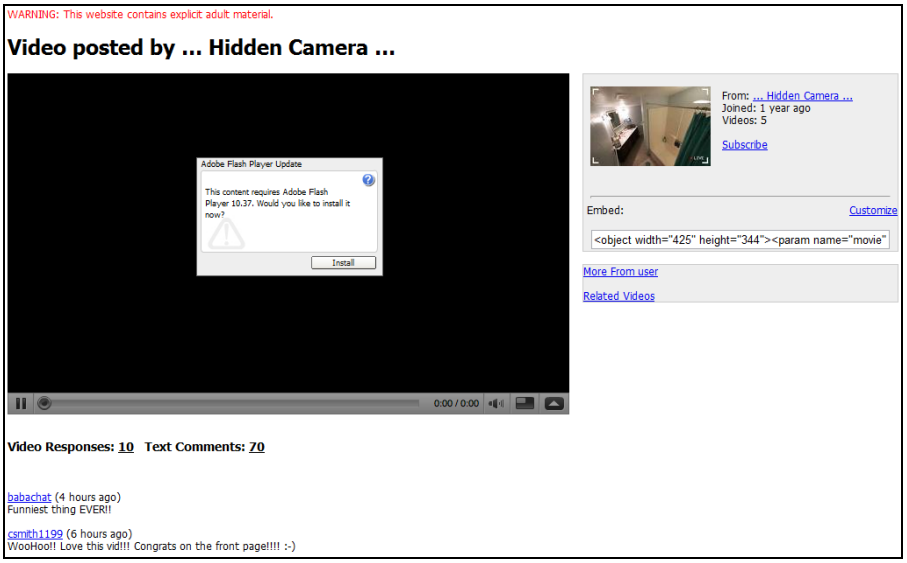
כיום יש מספר רב של רשתות חברתיות, ישנן רשתות בעלות נושאים ספציפיים (LinkedIn, Digg וכו') וישנן רשתות כלליות יותר (Facebook, Google+ וכו'), בשני המקרים, עובר מידע רב בין המשתמשים, וכותבי תולעים הבינו את הפוטנציאל שבדבר.

במקרים הקלאסים, תולעת שמצליחה לגנוב את פרטי ההזדהות של המשתמש פשוט שולחת מהחשבון שנפרץ הודעה פרטית לחבריו ובו קישור לעמוד בעל תוכן זדוני, אך במקרים קצת יותר נדירים נעשה שימוש יפהפה בהנדסה חברתית.

דוגמה למקרה קלאסי הינה Koobface- באופן פשוט יחסית, לאחר השגת גישה לחשבון המשתמש מתבצעת שליחת הודעה פרטית + כתיבה על עמוד הפרופיל של כלל חברי המשתמש עם קישור:



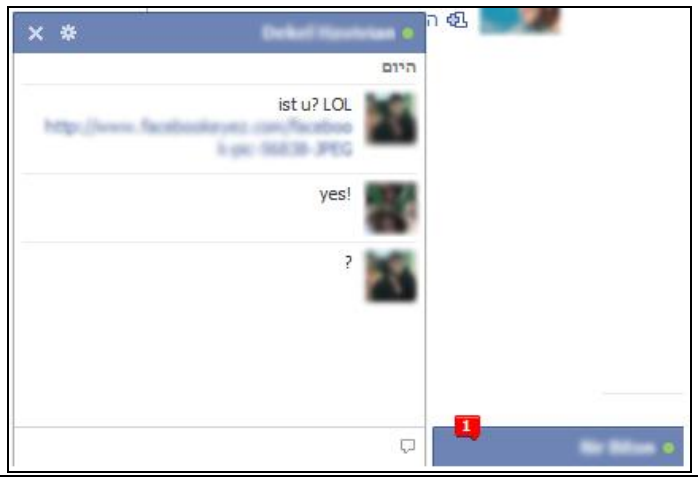
הקישור מפנה לעמוד Youtube פיקטיבי אשר דורש מהמשתמש להתקין עדכון לתוכנת הפלאש שלהם בכדי לצפות בסרטון:



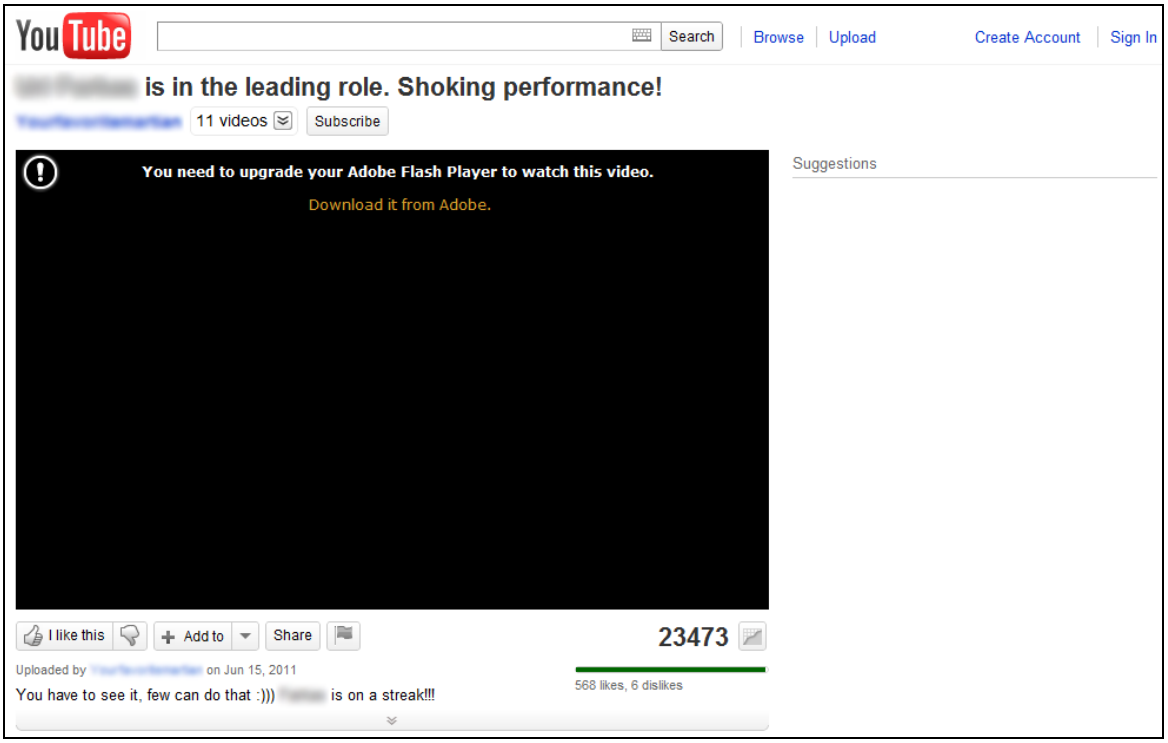
עמוד ה-Youtube סטטי, ומתחתיו יש תגובות של "משתמשי Youtube" פיקטיביים. ולמרות זאת, הדבר הספיק בכדי להפיל אנשים רבים בפח.

דוגמה הרבה פחות קלאסית, והרבה יותר מרשימה, אפשר לזקוף לתולעת חדשה יחסית, עדיין חסרת שם, אך לפי מחקר קצר שעשיתי (ותודה ל-Zerith) שעזר כאן, נראה שהיא עוזרת להפיץ כלי לריקון חשבונות BitCoin.

ברגע שהתולעת מורצת על מחשב ועליו יש חשבון Facebook, היא מתממשקת לחשבון ושולחת הודעת צ'אט לחבר שנמצא כרגע On-Line (גם עם בעל החשבון הפרוץ כרגע מחובר לפייסבוק הוא אינו יראה את שיחת הצ'אט אלא עם החשבון המותקף יכתוב לתולעת בחזרה) עם הודעה וקישור:



הקישור מפנה גם הוא לעמוד Youtube שכמובן דורש מהקורבן להתקין עדכון "תמים" לדפדפן:



מה שכל כך יפה בעמוד הזה הוא שהוא דינאמי. מה זאת אומרת? זאת אומרת שהוא נוצר On The Fly, על ידי התולעת, שניות מספר לפני שליחת הודעת הצ'אט.

מה דינאמי בעמוד?

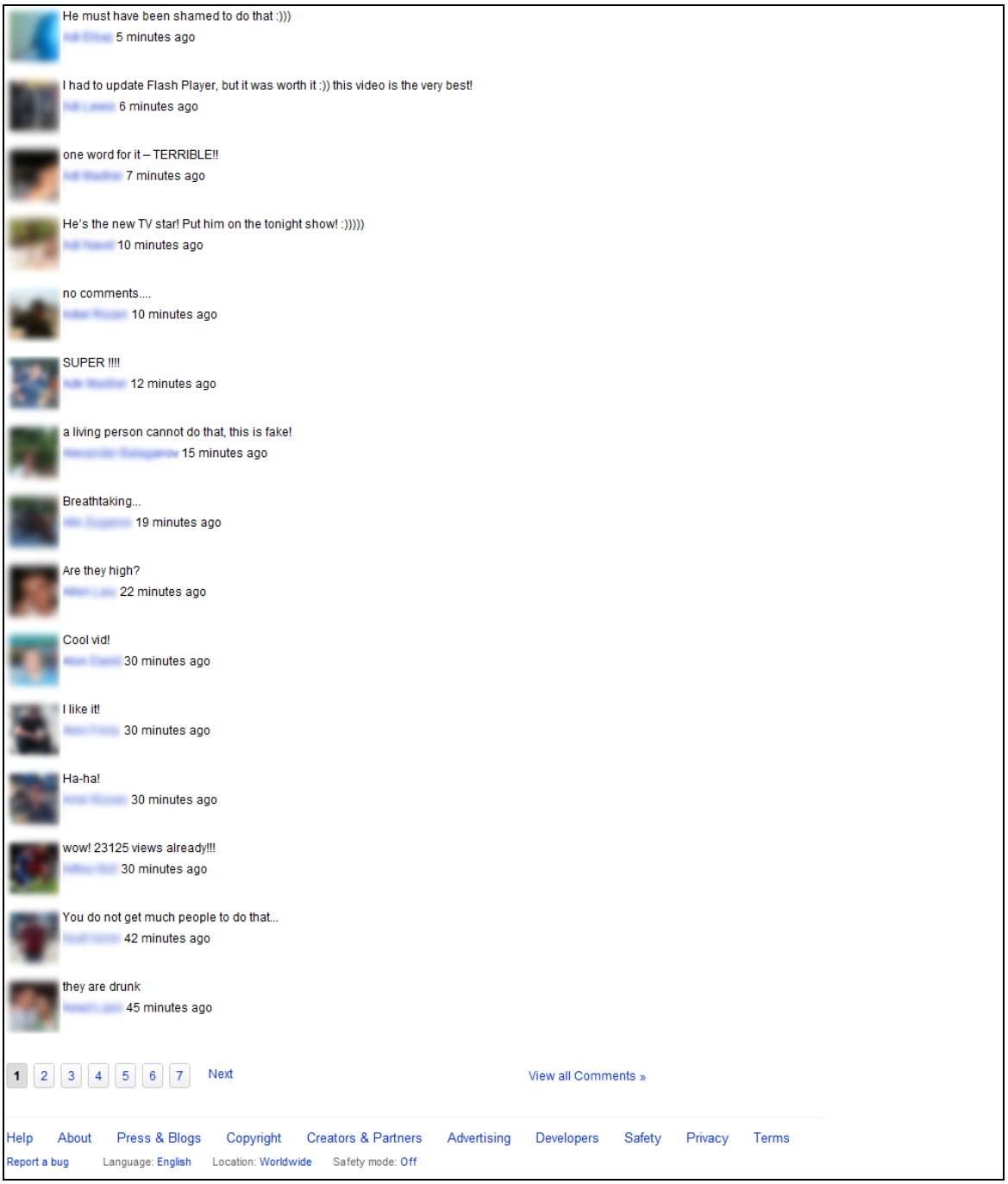
- **הכותרת של הסרטון מרמזת על כך שמדובר בסרטון על הקורבן**
- **התגובות על הסרטון מדברות על הקורבן עצמו.**
- **שמות המגיבי התגובות נלקחו מרשימת החברים של הקורבן.**
- **תמונות המגיבים לקוחות מתמונות פרופיל הפייסבוק האמיתיים של חברי הקורבן.**

שכלול של כלל הנתונים הנ"ל לא רק גורמות לקורבן להאמין כי מדובר בעמוד אמיתי, אלא גם גורמות לו להוריד את העדכון, שאגב, נראה כך:

Flash-Player.exe

בהחלט עושה רושם שבוצעה כאן עבודה מקצועית ביותר.

מספר תגובות על הסרטון הפקטיבי:


He must have been shamed to do that :)))
5 minutes ago

I had to update Flash Player, but it was worth it :)) this video is the very best!
6 minutes ago

one word for it – TERRIBLE!!
7 minutes ago

He's the new TV star! Put him on the tonight show! :)))))
10 minutes ago

no comments....
10 minutes ago

SUPER !!!!
12 minutes ago

a living person cannot do that, this is fake!
15 minutes ago

Breathtaking...
19 minutes ago

Are they high?
22 minutes ago

Cool vid!
30 minutes ago

I like it!
30 minutes ago

Ha-ha!
30 minutes ago

wow! 23125 views already!!!
30 minutes ago

You do not get much people to do that...
42 minutes ago

they are drunk
45 minutes ago

1 2 3 4 5 6 7 Next View all Comments »

Help About Press & Blogs Copyright Creators & Partners Advertising Developers Safety Privacy Terms
Report a bug Language: English Location: Worldwide Safety mode: Off

לאחר הרצת ההעדכון, המשתמש מקבל הודעת שגיאה שאין לו הרשאה להתקין את הקובץ, אך בשלב זה התולעת כבר הדביקה את המחשב...

סיכום

לא נגעתי בכלל הפלטפורמות בהן כותבי התולעים משתמשים, אבל עדיין, מהמידע שהוצג במאמר זה בהחלט ניתן לראות את התפתחות הנושא בשנים החולפות. אם בעבר כותבי התולעים הרשו לעצמם "לעגל פינות", היום, כאשר המודעות לאבטחת מידע גבוהה יותר- נראה כי הם עובדים קשה יותר ויותר בכדי לקנות את אמון הקורבנות. בדרך כלל, משתמש חשדן יוכל לזהות את התרמית, אך במקרים רבים (כגון הדוגמה האחרונה במאמר) נראה כי הסיכויים שגם משתמשים אלו יפלו לפח גבוהים.

נראה כי תולעים אשר מבצעות שימוש בחולשות 0day שונות בעלות עקומת תפוצה נרחבת יותר, אך כאשר מתגלה התולעת ונסגרת אותה החולשה, חיי התולעת קצרים ביותר. לעומת זאת, וקטור הפצה המשתמש בהנדסה חברתית אומנם מאפשר לתולעת להפיץ עצמה בקצב איטי יותר, אך כאן, אין באג שצריך לסגור, והדרך היחידה לעצור את התולעת מלהתפשט היא לעדכן את תוכנת האנטי-וירוס ולהגביר את המודעות הסביבתית לאבטחת מידע.

מקורות

- http://www.wormblog.com/im_worms/
- http://ftp.erm.tu-cottbus.de/security/witty-analysis.html
- http://digitalwhisper.co.il/files/Zines/0x0E/DW14-1-KoobfacePwning.pdf
- http://vx.netlux.org/29a
- http://www.symantec.com/security_response/writeup.jsp?docid=2001-021219-1830-99
- http://en.wikipedia.org/wiki/Anna_Kournikova_(computer_virus)
- http://en.wikipedia.org/wiki/ILOVEYOU
- http://iamjenessa.wordpress.com/2011/06/28/memories-of-the-love-bug-worm-by-graham-cluley-on-may-4-2009
- http://www.f-secure.com/v-descs/onthefly.shtml
- http://www.spywareguide.com/product_show.php?id=3108
- http://www.kaspersky.co.in/news?id=4277566