ניתוח תולעת ה-Conficker

מאת הרצל לוי ואפיק קסטיאל (cp77fk4r)

(התמונה נלקחה מ- slate.com)

תולעת הקונפיקר (Conficker), הידועה גם בשמות Downup, Downadup ו-Kido, היא תולעת שהתגלתה לראשונה בנובמבר 2008 והתפשטה מאז במידה רחבה כל כך, שרבים הכתירו אותה בתור התולעת המסוכנת ביותר עד היום. נכון להיום, מעריכים שיותר מ-12 מליון מחשבים נדבקו בתולעת. מאז החשיפה הראשונה של התולעת נמצאו 5 וריאציות שלה (E,D,C,B,A). התולעת פוגעת רק במחשבים שעליהם מותקנות מערכות ההפעלה Windows למיניהן, כולל את Windows 7.

התולעת לא פסחה אף על אתרי ממשלה, רשתות צבאיות, בתי חולים, משטרות ברחבי העולם ואפילו רשת צהלנט נפגעה. התולעת הצליחה לעצבן את מיקרוסופט עד כדי כך שגרמה להם להציע סכום של $250,000 למי שיצליח לאתר את יוצריה (דרך אגב , הצעה זו עדיין בתוקף למי שתוהה).

התולעת קונפיקר משתמשת בהרבה שיטות מתקדמות ומעניינות להדבקה, הפצה ופגיעה במשתמשי Windows. במאמר זה נתאר וננתח חלק מהן.

אז מה הופך את התולעת הזאת לכל כך נפוצה ומסוכנת?

חדירה

1. קונפיקר מדביקה מחשבים על ידי ניצול חולשה (MS08-067) ב-Windows Server service (SVCHOST.EXE) של מערכת ההפעלה, שמאפשרת הפעלת פקודות מרחוק (RPC) כאשר שיתוף קבצים מאופשר. כותבי קונפיקר השתמשו במודול של Metasploit לאקספלויט שנקרא ms08_067_netapi שנכתב ע"י HD Moore ושמנצל חולשה זו.
2. גילוי כל המשתמשים (למשל על ידי שימוש בפקודה: net user) והתקפת Brute Force עם שימוש במילון סיסמאות על כל משתמש (בעצם התקפה על סיסמאות חלשות ומוכרות).
3. דרך התקנים ניידים כמו דיסק און קי – על ידי יצירת קבצי autorun.inf שיגרמו להפעלה אוטומטית של הזרקת קובץ ה-DLL המכיל את הקוד הזדוני.

הדבקה

לאחר שלב החדירה, הקונפיקר מנסה להעתיק את עצמה לתיקיית המערכת (%SysDir%) של מחשבים אחרים על ידי אפשרות שיתוף הקבצים. הניסיון הראשון הוא לחדור דרך השיתוף של מנהל המערכת (ADMIN$). אם ניסיון ההעתקה לשיתוף זה נכשל, התולעת תשתמש בהתקפת ה-Brute Force שתוארה לפני כן ואז שוב תנסה להעתיק את עצמה לתיקיית המערכת או לתיקיות של תוכנות שמגיעות עם מערכת ההפעלה כמו IE או Windows Movie Maker. הקונפיקר מעתיקה את עצמה בצורת קובץ DLL חבוי בעל שם רנדומאלי (אי שמירה על תבנית אחידה מוסיפה על הקושי באיתור התולעת) ומכיוון שקובץ DLL הוא לא קובץ הרצה, אופן ההטמעה שלו היא על ידי הזרקה של ה-DLL לתהליך אחר שכבר רץ במערכת (DLL Injection). כדי שקונפיקר תשרוד חסימות של Firewall והרשאות היא מזריקה עצמה לתהליכי מערכת כמו rundll32.exe. ההזרקה נעשית בצורה הבאה:

(התמונה המקורית נלקחה מ- "Threat Experts Blog")

הפונקציות המתוארות בפיסקה זו הן פונקציות API של מערכת ההפעלה. בתור התחלה התולעת תפתח את תהליך היעד בעזרת OpenProcess, תקצה זיכרון במרחב הכתובות שלו בעזרת VirtualAllocEX ותרשום לתוכו את הנתיב המלא ל-Conficker DLL. לאחר מכן היא תשיג את הכתובת של הפונקציה LoadLibraryA שבעזרתה נתן לטעון DLL לתוך מרחב כתובות של תהליך מסוים על ידי שימוש ב-kernel32.dll (קובץ שמגיע עם מערכת ההפעלה Windows) ותטען את תוכן קובץ ה-DLL על ידי השימוש בפונקציה זו. בעזרת CreateRemoteThread נוצר Theard שרץ במרחב הכתובות של תהליך המערכת ומריץ את ה-Conficker DLL.

הישרדות

כדי לשרוד אתחול, גילוי והסרה, הקונפיקר חייבת לבצע שינויים במערכת ההפעלה:

1. כדי לשרוד אתחול, היא רושמת את עצמה כשירות של המערכת (service) המופעל אוטומטית בעליית המערכת, על ידי הוספת ערכים בעורך הרישום תחת המפתח הבא:

```
HKLM\SYSTEM\CurrentControlSet\Services
```

2. ביטול ה-Firewall של Windows.
3. על מנת לשרוד עדכוני אבטחה של Windows התולעת מבטלת עדכונים אוטומטיים, את Windows Defender ואת האפשרות להרצת המערכת במצב בטוח.
4. דרך הישרדות נוספת היא מחיקה של נקודות השחזור (restore points) של המערכת.
5. יצירת משימות מתוזמנות להזרקת ה-DLL מחדש.
6. חסימת תהליכים שיכולים לגרום להסרתה כגון תוכנות אנטי-וירוס.
7. חסימת גישה לאתרי חברות אנטי-וירוס.

הפצה

הקונפיקר היא תולעת, כלומר, היא יודעת להתרבות ולהפיץ את עצמה. לאחר שתולעת חודרת למערכת ומבצעת את כל הפעולות בכדי להבטיח את ההישרדות שלה, היא תפיץ את עצמה בדרכים הבאות:

1. סריקת כל הרשת הפנימית לחיפוש מחשבים עם פורטים פתוחים ושימוש בטכניקות חדירה והדבקה שתוארו קודם לכן.
   מחשב שנגוע בקונפיקר משמש גם כלקוח וגם כשרת. כדי לאפשר זאת, הקונפיקר פותחת 4 פורטים לשימוש השרת שהם: 2 פורטים של UDP ו-2 של TCP שלהם היא מאזינה ופורט נוסף שישמש כלקוח.

2. לאחר שלב החדירה, הקונפיקר מזהה חיבורים של התקנים ניידים וכוננים ממופים ואז מעתיקה עצמה לשם כפי שתואר בשלב ההדבקה.

שיטות מתקדמות בהן משתמשת התולעת

הפצת ה-Payload

כפי שתואר לפני כן, קונפיקר פותחת 4 פורטים, מאזינה להם ובין היתר מנתחת את תעבורת הנתונים בפורטים אלו. כאשר קונפיקר מפיצה עצמה ברשת הפנימית שבה היא נמצאת, היא משתמשת בתקשורת P2P וחודרת לקורבן באמצעות שליחת האקספלויט שמנצל את החולשה שתוארה קודם לכן וגורמת לכך שלתוקף תהיה אפשרות להפעלת פרוצדורות מרחוק (RPC) על הקורבן.

כאשר מחשב נגוע אחד מנסה לחדור למחשב נגוע אחר (זאת אומרת שהוא שולח לו את האקספלויט), או שמחשב נגוע מזהה ששלחו לו את אותו אקספלויט שבו גם הוא השתמש, הוא מבין שאותו מחשב שניסה לחדור אליו גם הוא נגוע ולכן באותו הרגע הוא שולח למחשב שניסה לחדור אליו את ה-Payload שיש אצלו, כך שה-Payload מופץ בין כל מחשבי הרשת הנגועים.

Anti-Analyzing

על מנת להגיע למצב בו חברות האנטי-וירוסים יוכלו לכלול כלים להסרת התולעת מהמחשב בתוכנות שלהן, על חוקרי הוירוסים להצליח לנתח את התולעת. ניתוח התולעת יכול לכלול אלמנטים ממספר תחומים, אם זה ביצוע Debugging על התהליך שהתולעת הוזרקה אליו או על קובץ ה-Deploy שלה, אם זה ביצוע Sniffing וניתוח תעבורת המידע היוצאת והנכנסת מעמדה הנגועה באחת מגרסאות התולעת או אם זה ניתוח השינויים בסביבת התולעת.

ברוב המקרים שלב הניתוח מבוצע במעבדות המכונות "Security-lab" - רשתות מחשבים המדמות את רשת האינטרנט הנמצאות תחת מעקב של אין ספור כלים, החל מכלים המבצעים Sniffing לכלל תעבורת הרשת וכלה בכלים המבצעים האזנה וניתוח השינויים בתהליכים פנימיים במחשב בזמן ריצת התולעת.

יוצרי התולעת יישמו מספר מנגנונים בכדי להקשות על חוקרי הוירוסים מלבצע את אותן הפעולות שציינו כאן. שלב ניתוח התולעת הוא מאוד קריטי, חומרת וכמות הנזק שהתולעת תעשה ברשת האינטרנט הן כמעט תמיד נגזרת של המהירות בה ניתוח התולעת יעשה וברמת הדיוק שאליה יגיעו חוקרי התולעת.

המנגנונים <u>העיקריים</u> בהם השתמש יוצר הווירוס להקשות על נסיונות המחקר הם:

- שינוי הרשאות כתיבה/צפייה של ערכים שונים בעורך הרישום של מערכת ההפעלה.
- שינוי הרשאות קריאה ומחיקה של הקבצים הנמצאים בשימוש של התולעת.
- ביצוע Hooking לפונקציות מערכת ותהליכים שונים במערכת ההפעלה.
- ביצוע Hooking ל-Dll הספציפי שבו קיימת החולשה אותה מנצלת התולעת.

- ביטול שירותי אבטחה עדכון גיבוי ושחזור של מערכת ההפעלה.
- שימוש במידה רבה של Obfuscation לקוד התולעת.
- זיהוי האם התולעת רצה בסביבה וירטואלית או לא ויישום שני מנגנוני ריצה שונים בהתאם.
- שימוש בערוץ תקשורת מוצפן תחת אלגוריתמי הצפנה "כבדים" (כגון ה-RSA) ושימוש במפתחות הצפנה גבוהים.
- ניטור התהליכים הרצים במערכת ההפעלה ובדיקה האם הינם "כלי ניתוח".
- קינפוג מחדש של כלים כגון תוכנת ה-Firewall של מערכת ההפעלה.

שינוי ערכים קריטיים בעורך הרישום

כחלק מהשינויים שהתולעת הייתה מבצעת בעורך הרישום של מערכת ההפעלה היא הייתה מוחקת/משנה את הערכים תחת המפתחות הבאים:

- מחיקת המפתח:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot
```

בכדי למנוע מהמשתמש לבצע אתחול מחדש של המחשב במצב "Safemode". (השימוש הנצפה הראשון בטכניקה הזאת היה של הווירוס "W32/Bagle.fb@MM" בשנת 2006)

- שינוי הערכים במפתח:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\A
dvanced\Folder\Hidden\
```

(זהו הערך האחראי על אפשרות ה-show hidden files and folders) כך שגם אם המשתמש יבחר להציג את הקבצים המוסתרים (ATTRIB +H) במערכת- המערכת לא תציג אותם.

- שינוי הערך: TcpNumConnections

תחת המפתח:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\
```

ל-00FFFFFE (הערך המקסימאלי) בכדי לאפשר את הכמות המירבית של חיבורי TCP/IP בתחנה.

- הוספת ערכים למפתח:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
```

בכדי להיכנס לרשימת ה-Services של המערכת ולהטען מיד עם הפעלתה

- הוספת ערכים למפתח:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Svchost
```

בכדי להטען בהפעלת המערכת דרך תהליך ה-Svchost.exe. (ריצה של מספר תהליכי ה-Svchost.exe במערכת ההפעלה היא דרך נורמלית) התהליך אחראי על "אירוח" של מספר תהליכים במערכת ההפעלה והוא טוען אותם בזמן טעינת מערכת ההפעלה.

בנוסף, ע"י השימוש בפונקציה "RegSetKeySecurity" (תחת ADVAPI32.dll) התולעת הייתה מורידה את ההרשאות לכלל המשתמשים משינוי ערכים ספציפיים בעורך הרישום (ערכים כגון רשימת ה-Services) ומותירה הרשאה מיוחדת רק למשתמש System – כך שגם למשתמשים מקבוצת "Administrators" לא הייתה גישה לשנות/לצפות בהם.

גרסאות שונות של תולעת ה-Conficker מבצעות שינויים שונים בעורך הרישום, אלה השינויים שלרוב יתרחשו כחלק ממנגנון פריסת התולעת.

Hooking לפונקציות מערכת/ תהליכי מערכת

כפי שנכתב בעמודים הקודמים, כחלק מהפעולות שהתולעת עושה היא גם מבצעת Hooking לכל מיני פונקציות מערכת ותהליכי מערכת שונים, לדוגמא:

- פעולת ה-Hook המרכזית שהתולעת מבצעת היא לפונקציה NetpwPathCanonicalize

הפונקציה NetpwPathCanonicalize מאוחסנת תחת הקובץ netapi32.dll, והיא ה-API האחראי על ה-RPC שבו קיימת החולשה שאותה מנצלת התולעת (MS08-067).

התולעת מחליפה את חמשת הבייטים הראשונים של הפונקציה בפקודת JMP המעבירה את המעבד לקוד האחראי על הרצת התולעת.

תחילת הקוד של NetpwPathCanonicalize לאחר עריכת התולעת

```
5B86A259 E9 A0B028A6   JMP 01AF52FE
5B86A25E 53            PUSH EBX
5B86A25F 8B5D 14       MOV EBX,DWORD PTR SS:[EBP+14]
5B86A262 56            PUSH ESI
5B86A263 57            PUSH EDI
5B86A264 33FF          XOR EDI,EDI
5B86A266 3BDF          CMP EBX,EDI
5B86A268 0F85 8EDE0000 JNZ NETAPI32.5B8780FC
```

תחילת הקוד המקורי של NetpwPathCanonicalize

```
5B86A259   8BFF          MOV EDI,EDI
5B86A25B   55            PUSH EBP
5B86A25C   8BEC          MOV EBP,ESP
5B86A25E   53            PUSH EBX
5B86A25F   8B5D 14       MOV EBX,DWORD PTR SS:[EBP+14]
5B86A262   56            PUSH ESI
5B86A263   57            PUSH EDI
5B86A264   33FF          XOR EDI,EDI
5B86A266   3BDF          CMP EBX,EDI
5B86A268   0F85 8EDE0000 JNZ NETAPI32.5B8780FC
```

(התמונה המקורית נלקחה מהמאמר המצויין "Know Your Enemy: Containing Conficker" של הפרויקט Honeynet, נכתב במקור ע"י Felix Leder ו-Tillmann Werner)

בנוסף, התולעת מבצעת פעולות Hooking לארבעה (בגרסאות מתקדמות אף יותר) קבצי DLL נוספים:

- פעולת Hooking לפונקציות הבאות:
  - DnsQuery_A
  - DnsQuery_UTF8
  - DnsQuery_W
  - Query_Main

המאוחסנות תחת הקובץ dnsapi.dll. מטרת הפעולה הנ"ל היא ברובה בכדי למנוע מהתחנה המקומית לגשת לשרתי חברות האנטי-וירוסים המשמשים את תוכנות האנטי-וירוס לעדכן את מערך החתימות הקיימות באפליקציות שלהן וכך למנוע מהם לזהותה.

- ועוד פעולות Hooking לפונקציות "קלאסיות", כגון:
  - NtQueryInformationProcess
  - InetnetGetConnectedState
  - Sendto

המאוחסנות בקבצים ntdll.dll, wininet.dll ו- ws2_32.dll (בהתאמה) אשר משמשות את מערכת ההפעלה להשיג מידע על תהליכים ואירועים במערכת:

- NtQueryInformationProcess - אחראית על השגת מידע אודות תהליכים במערכת. (שם, נתוני PEB וכו')
- InetnetGetConnectedState - מאפשרת בדיקה האם בוצעה "Internet dialup".
- Sendto - אחראית על שליחת מידע ליעד ספציפי מהתחנה.

גילוי מכונות וירטואליות ושימוש ב-Obfuscation

השימושים המשמעותים ביותר ב-Obfuscation נצפו בגרסתה השנייה של התולעת ומעליה, גרסתה השנייה התגלתה ע"י החוקרים של חברת Sophos באמצעות Honeypots. אחד הסעיפים המעניינים שעלה בדו"ח של החוקרים מאותה החברה הוא שהתולעת משתמשת במנגנון המכונה "Red Pill" (כן, בהשראת הסצנה ממטריקס) – מנגנון פשוט להפליא אשר נועד לבדוק האם התהליך רץ תחת מכונה וירטואלית. הנתון המעניין הוא שבמידה והתולעת "הבינה" שהיא מורצת בתוך סביבה וירטואלית – כנראה במסגרת ניסיונות לנתח אותה – היא הייתה מתנהגת באופן שונה ממה שהיא הייתה מתנהגת בסביבה טבעית. רעיון ה-Red Pill הוא אלגנטי ופשוט, במקור הוא הוצג בשנת 2004 ע"י Joanna Rutkowska, במאמר:

"Red Pill... or how to detect VMM using (almost) one CPU instruction"

ופותח לאחר מכן ע"י שני חברי קהילת Offensive Computing בשם Danny Quist ו-Val Smith, במאמר:

"Detecting the Presence of Virtual Machines Using the Local Data Table"

על ידי השוואה פשוטה בין ערכים שונים (הידועים מראש) של ה-LDT, התולעת יכלה לדעת היכן היא רצה. באופן כזה אופי התולעת משתנה בזמן ריצתה, במידה וחוקר יפספס את המנגנון הנ"ל- הוא יוכל לבזבז זמן יקר בניתוח הקוד שלא מבצע שום דבר. לא מדובר פה על Code Obfuscation רגיל, אך עדיין מדובר במהלך אשר יקשה על מנתח התולעת. בנוסף, ביצעו יוצרי התולעת פעולות Obfuscation לקריאות ה-API שבהן השתמשה התולעת בכדי להסוות קריאות אלו ולהקשות על חוקרי הוירוסים למצוא את כתובותיהן המקוריות.

מנגנוני הצפנה ומנגנוני אימות

תולעת הקונפיקר מבצעת שימוש בשליחת וקבלת נתונים על גבי רשת האינטרנט למספר מטרות, בין אם מדובר בעדכון Payload התקיפה של התולעת, בפקודות לביצוע (כמו התקפת שרת מסוים וכו') או בסריקת הרשת למציאת קורבנות נוספים.

כפי שניתן היה להבין עד כה- תולעת הקונפיקר פותחת על העמדה הנגועה ערוצי תקשורת, אשר דרכם היא בודקת כל פרק זמן מסוים האם יוצרי התולעת שחררו עדכונים, כמו למשל- עדכון וקטור התקיפה

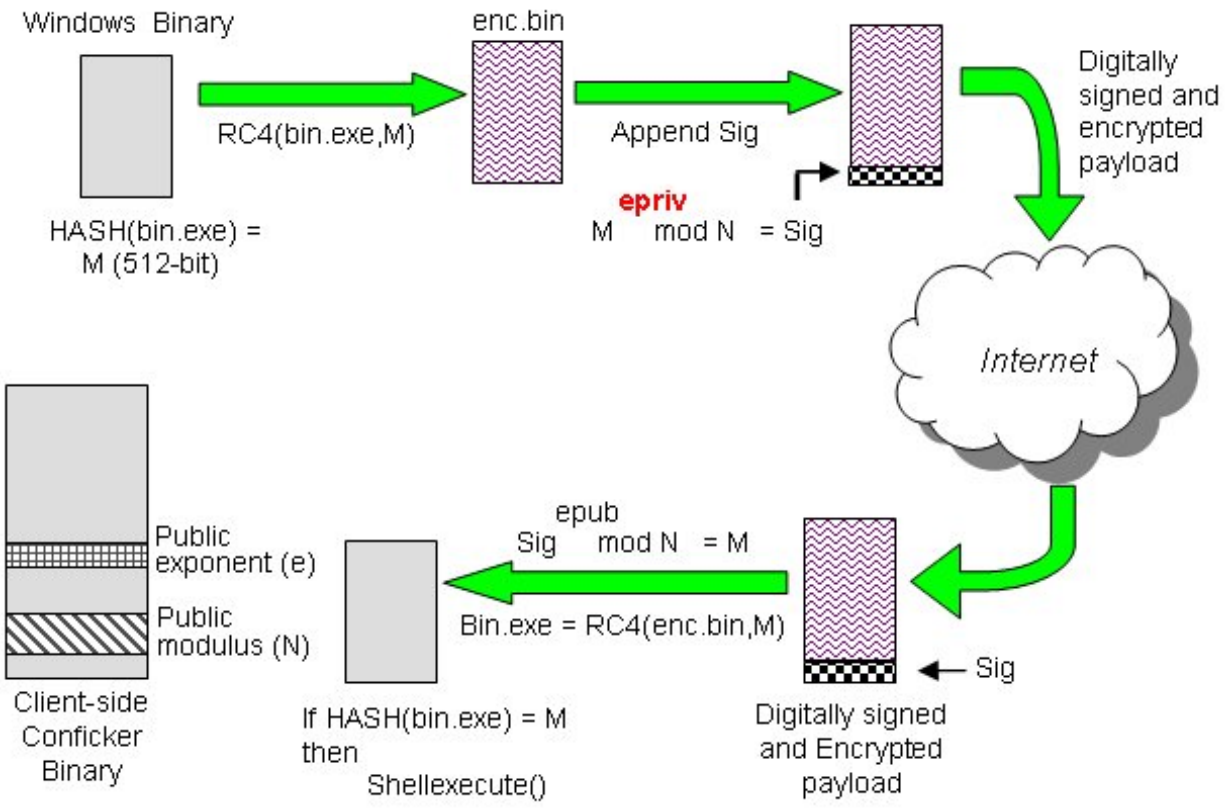
שבה התולעת תשתמש בכדי לתקוף מחשבים חדשים, וכך, גם במידה ומיקרוסופט ישחררו טלאי אבטחה לאותו RPC חשוף- על יוצרי התולעת לשלוח עדכון חדש שכולל בתוכו וקטור תקיפה לחולשה חדשה במערכת, וכך להדביק גם עמדות מעודכנות.

יוצרי הקונפיקר מימשו מנגנון אימות Hashing המבוסס על האלגוריתם MD6 (גם כיום, יותר משנה לאחר התקפת התולעת, אלגוריתם ה-Hashing ממשפחת MD הנפוץ ביותר הוא: 5 – כך שהדבר נחשב אז לפריצת דרך). המידע היה עובר תחת אלגוריתם ה-Stream Cipher המוכר-RC4 בשימוש של מפתח הצפנה בגודל 512-bit ומימוש של אלגוריתם ה-RSA בכדי לייצר חתימה דיגיטלית בעזרת מפתח ציבורי המשותף לכלל תולעי הקונפיקר. החתימה הדיגיטלית הייתה נשלחת ביחד עם קובץ העדכון המוצפן.

כאשר תולעת הקונפיקר הייתה רואה כי פורסם עדכון חדש- היא הייתה נגשת לאחד מהשרתים שהוקצו לפעולה זו, מורידה אותו למחשב ומוודאת כי המידע לא שונה בדרך ושום גורם ביניים לא החליף או ערך את תוכנו. במידה והקובץ נבדק ונמצא כי שום גורם לא ערך את המידע בדרך והקובץ אכן אותנטי - התולעת הייתה מריצה אותו ומעדכנת את עצמה בעזרתו.

הסבר ויזואלי של כלל התהליך פורסם בדיוק לפני שנה, בפברואר 2009, במסגרת מאמר של הארגון SRI INTERNATIONAL המפעיל מערכות / רשתות Honeypots ומפרסם Infection Logs יומיים בנוגע להתקפות/ניסיונות להתקפות אשר בוצעו עליהם:

"AN ANALYSIS OF CONFICKER'S LOGIC AND RENDEZVOUS POINTS"



בעזרת מימוש של מנגנוני אימות אלו הצליחו יוצרי התולעת למנוע מחוקרי הוירוסים להרוס אותה על ידי הזרקת "עדכונים" פיקטיביים שנועדו לעצור אותה. עקב שימוש בדרכים אלו ואחרות, ניסו יוצרי תולעת הקונפיקר, בין היתר, למנוע מחוקרי הוירוסים לעצור את התולעת.

אז מה עושים עם 12 מליון בוטים?

התשובה היא כמובן- הרבה מאוד כסף.
המטרה העיקרית של יוצרי קונפיקר היא כנראה הקמת רשת בוטים שעליהם יוכלו לשלוט בעיקר לצרכים כספיים כמו הפצת ספאם, סחיטות להתקפות DDOS (מפחיד לחשוב על DDOS עם כמות כזאת של בוטים), סחיטות למחיקות קבצים על שרתים וכן הלאה.

פשעי רשת או Cyber Crime הוא מושג המתאר את כל סוגי הפשעים המבוצעים באמצעות או דרך המחשב. בעשור האחרון הפך סוג פשיעה זה למקצועי ומאורגן באופן מדאיג. ארגוני פרסום ספאם או ארגונים שעוסקים בפשעים אלו (נקראים גם Cyber-Mafia) מוכנים לשלם הרבה מאוד כסף תמורת רשתות בוטים, כתיבת תולעים או אפילו מידע מסוים הרלוונטי לצרכיהם. קחו לדוגמה את ה-RBN (Russian Business Network), אחד מארגוני ה-Cyber-mafia הגדולים בעולם. ההתמחות שלהם היא גניבת זהויות ובין היתר מעריכים כי הם אלו ששולטים ברשת הבוטים העצומה Storm. ארגון זה עודד את הוגי התולעת Storm ליצור את אותה תולעת שהכניסה להם הרבה מאוד כסף. ולנו? הרבה מאוד נזק.

אנו מצרפים מחירון לדוגמה ליחידה:

Rank	Item	Percentage	Range of prices
1	Credit cards	22	$0.50 - $5
2	Bank accounts	21	$30 - $400
3	email passwords	8	$1 - $350
4	Mailers	8	$8 - $10
5	Email addresses	8	$2/MB - $4/MB
6	Proxies	6	$0.50 - $3
7	Full identity	6	$10 - $150
8	Scams	6	$10/week
9	Social Security Numbers	3	$5 - $7
10	Compromised Unix shells	2	$2 - $10

Breakdown of goods available for sale on underground economy servers.
(Source: Symantec Corporation, 2007)

(נלקח מ- newcriminologist.com)

לסיכום

אי אפשר שלא להתרשם מהדרך המתוחכמת בה פועלת תולעת הקונפיקר. כותבי קונפיקר השקיעו המון ידע ותכננו תולעת ברמה מאוד גבוהה, השתמשו בשיטות מתקדמות, מימשו אלגוריתמים חדשניים כמו ה-MD6 של רון ריווסט (למי שלא מכיר, ה-R ב-RSA מייצג את רון ריווסט) ואפילו דאגו להתעדכן ולשפר את מנגנוני התולעת שאותם הצליחו לעצור.

התולעת קונפיקר הופעלה בראשון באפריל 2008 והייתה אמורה לטרוף את דרכה ברשת. אבל לא קיימת הוכחה שיוצריה הפעילו אותה בצורה כלשהי. אולי עצם העובדה שהיא הופעלה ב-1 באפריל (April Fools' day) נותנת את התשובה שזאת סתם הייתה מתיחה של כמה גאונים, למרות שקשה להאמין כי השקעה בתולעת מתוחכמת כל כך נעשתה לשם מתיחה.