דו"ח סיכום

-

CONFICKER

ממשל זמין – פרויקט תהיל"ה

מאפייני מסמך

מחבר	פולינה חזנוב, יול בהט
מספר גרסה	1.0
סטטוס	סופית
תאריך הוצאה	מאי 2010
שם קובץ אלקטרוני	

תשומות / הערות

שם/תפקיד	הערה (אופציונאלי)	תאריך	חתימה

היסטוריה

מ. גרסה	ת. הוצאה	מחבר	שינויים מרכזיים בגרסה
0.1	18/01/10	פולינה חזנוב	גרסה ראשונה
0.2	01/03/10	פולינה חזנוב, יול בהט	תיקונים
1.0	13/05/10	פולינה חזנוב, יול בהט	גרסה סופית

הפצה

מ. גרסה	נמענים
1.0	רשימת תפוצה SI

www.gov.il
ממשל זמין – פרויקט תהיל"ה

תוכן עניינים

1. כללי 4
1.1 רקע 4
1.2 Concfiker worm 5
2. Conficker בפרוט 6
2.1 רקע 6
2.2 דרכי הפצה 7
2.2.1 MS08-67 7
2.2.2 ניצול סיסמאות חלשות 9
2.2.3 ניצול Autorun 9
2.3 פרטים טכניים נוספים 10
2.3.1 תיאור תהליך ההתפשטות 10
2.3.2 פרוט לפי גרסאות 14
2.3.3 יכולות שונות 17
2.3.4 יצירה של Domain Names 18
2.3.5 הצפנה 19
2.3.6 רשימות שחורות 20
2.4 נזקים אפשריים 20
2.4.1 השחתה של מערכות הגנה 20
2.4.2 יצירת רשת Botnet 20
2.4.3 התקנת תוכנות זדוניות נוספות 21
2.5 היסטוריה וסטטיסטיקות 23
2.5.1 אירועים חריגים 23
2.5.2 סטטיסטיקה 24
2.6 הימנעות מהדבקה 26
2.7 גילוי והסרה 26
2.7.1 סימפטומים 26
2.7.2 גילוי הידבקות 27
3. ביבליוגרפיה וקריאה נוספת 28

1. כללי

1.1 רקע

במסגרת פעילותו של פרויקט תהיל"ה, צוות אבטחת המידע של הפרויקט חוקר מגוון נרחב של איומים אלקטרוניים על תשתיות המחשוב של ממשלת ישראל.

מתוך רצון וכוונה לשמר את הידע הנצבר במסגרת פעילות מחקר זו, וכן על מנת להגביר את המודעות בנושאים שונים באבטחת מידע בקרב אוכלוסיות הממשלה השונות, צוות אבטחת המידע מרכז, מסכם ומפיץ סקירות שונות בנושאים אלו.

1.2 תולעים – כללי

תולעת היא תוכנית מחשב אשר מסוגלת לשכפל את עצמה (בפעולת העתקה) בצורה אוטומטית בין מחשבים שונים. תוכניות מסוג "תולעת" עושות שימוש ברשת המחשבים כדי להעתיק ולשכפל את עצמן לצמתי רשת (מחשב ברשת מהווה צומת), זאת באופן אוטומטי וללא צורך במעורבות של מפעיל. שלא כמו וירוס המחשב, התולעת לא בהכרח נצמדת לתוכנית אחרת כדי לפעול. תוכנות תולעת פוגעות ברשת ובהעברת הנתונים דרכה - בשל צריכת משאבי תקשורת (שימוש ברוחב פס יקר - והקטנת "מהירות העברה") כדי להעביר את עצמן. בחלוקת עבודה זו - הוירוס פוגע בקבצים והתולעת ברשת.

נהוג לחלק את תוכנות התולעת למספר קטגוריות:

- תולעי דוא"ל: מתפשטים בהודעות דוא"ל .
- תולעי הודעות מיידיות: מסנגרים וכד'.
- תולעיIRC : בערוצי צ'אט.
- תולעי רשתות שיתוף קבצים: בתוכנות שיתוף P2P.
- תולעי מכשירים ניידים – המתפשט בעזרת Blue Tooth

עם זאת, רשימה זו בהחלט אינה סופית.

1.3 Concfiker

תולעת ה-Conficker, המוכרת גם בשמות Downup, Downadup ו-Kido, התגלתה בנובמבר 2008. התולעת הצליחה לנצל בהצלחה ובצורה אוטומטית לחלוטין פרצת אבטחת מידע חמורה במערכת ההפעלה Windows של חברת Microsoft. כמו כן התולעת משתמשת במספר טכניקות הסוואה.

מחקרים שונים מראים כי בשיאה, התולעת הדביקה כ-9 מיליון מחשבים שנדבקו ויש אף כאלה הטוענים ל-15 מיליון. נהוג לחלק את התולעת ל-5 גרסאות עיקריות, אבל 3 מהן נפוצות יותר. התולעת מבטלת שירותים חיוניים של מערכת ההפעלה חלונות כגון: Windows Security Center, Windows Defender ,Windows Automatic Update ואף Windows Error Reporting. ביטול שירותים אלה לבדו לא גורם נזק מיידי למחשב אך הופך את המחשב לפגיע יותר וחושף אותו למתקפות שונות שאת חלקן היא עצמה עשויה ליזום בשלב השני של פעילותה.

לבסוף, התולעת פותחת דלת אחורית לקבלת הוראות נוספות משרת מרוחק. היא עשויה לקבל מהשרת אחת או יותר מההוראות הבאות:

- הוראה להתרבות ולהפיץ את עצמה
- הוראה לאסוף מידע אישי על המחשב ועל המשתמש
- הוראה להוריד מהשרת או ממקור אחר תוכנות זדוניות נוספות למחשב בו הופעלה.

2. Conficker בפרוט

2.1 רקע

הגרסא הראשונה (A) של התולעת התגלתה בנובמבר 2008, והשתמשה בפגיעות של Network Service במערכת הפעלה Windows. בסוף אוקטובר חברת Microsoft הוציאה טלאי (Patch) שתיקן את החור האבטחתי. למרות זאת, מכיוון שאחוז מתקיני טלאי אבטחת המידע בעולם עומד על כ-70%, מחשבים רבים נשארו פגיעים ואכן הותקפו.

בדצמבר 2009 יוצרי Conficker הוציאו גרסא חדשה של התולעת (B), והוסיפו לתולעת יכולות להתפשטות דרך רשתות LAN, והתקנים חיצוניים. גרסה זו הייתה הרסנית במיוחד במגזר העסקי, ובינואר 2009 היו בין 9 ל 15 מיליון מחשבים שנדבקו. בין חודש פברואר של אותה שנה ועד לחודש אפריל, כל חודש יצאה גרסה חדשה, עד לגרסה E, אשר נחשבת לגרסה האחרונה הידועה.

קיימות שתי תיאוריות עיקריות לגבי מקור השם קונפיקר. האופציה הראשונה היא מהמילה האנגלית Configuration והמילה הגרמנית ficker [1]. האופציה השניה היא סידור מחדש של אותיות של דומיין traf**ficcon**vert**er**.biz, האתר המקורי ממנו הורדו עדכוני התוכנה של התולעת (Fic)(Con)(Er) => (Con) (Fic) (+K) (Er) => CONFIKER.

[1] משמעות המילה הינה גסה מכדי לעלות על גבי מסמך זה. למעוניינים ניתן ללחוץ על הלינק הבא : http://translate.google.com/#de|iw|ficker

2.2 דרכי הפצה

נהוג לומר כי קיימות שלוש דרכי הפצה עיקריות לתולעת ה Conflicker:

1. דרך ניצול פרצת אבטחה מידע במערכת ההפעלה Windows הידועה בכינוי ms08-67 [2].

2. מנגנון ה-Autorun – כלומר ניצול התכונה של מערכת ההפעלה להפעיל בצורה אוטומטית קבצים הנמצאים על תקליטורים ו\או התקנים ניידים אחרים.

3. ניצול סיסמאות חלשות – מחקרים רבים מראים כי אחת הסיבות העיקריות להתפשטותה המהירה של קונפיקר נבעה מהעובדה כי ברשתות עסקיות רבות משתמשים עשו שימוש בסיסמאות פשוטות למדי, אשר התולעת הצליחה לנחש, או אפילו פתחו תיקיות משותפות ללא סיסמה כלל.

4. בנוסף לתולעת קיים מנגנון עדכון אשר מטרתו לעדכן את הגרסא החדשה יותר של התולעת.

להלן הסברים טכניים לגבי אופי ניצול דרכי הפצה אלו:

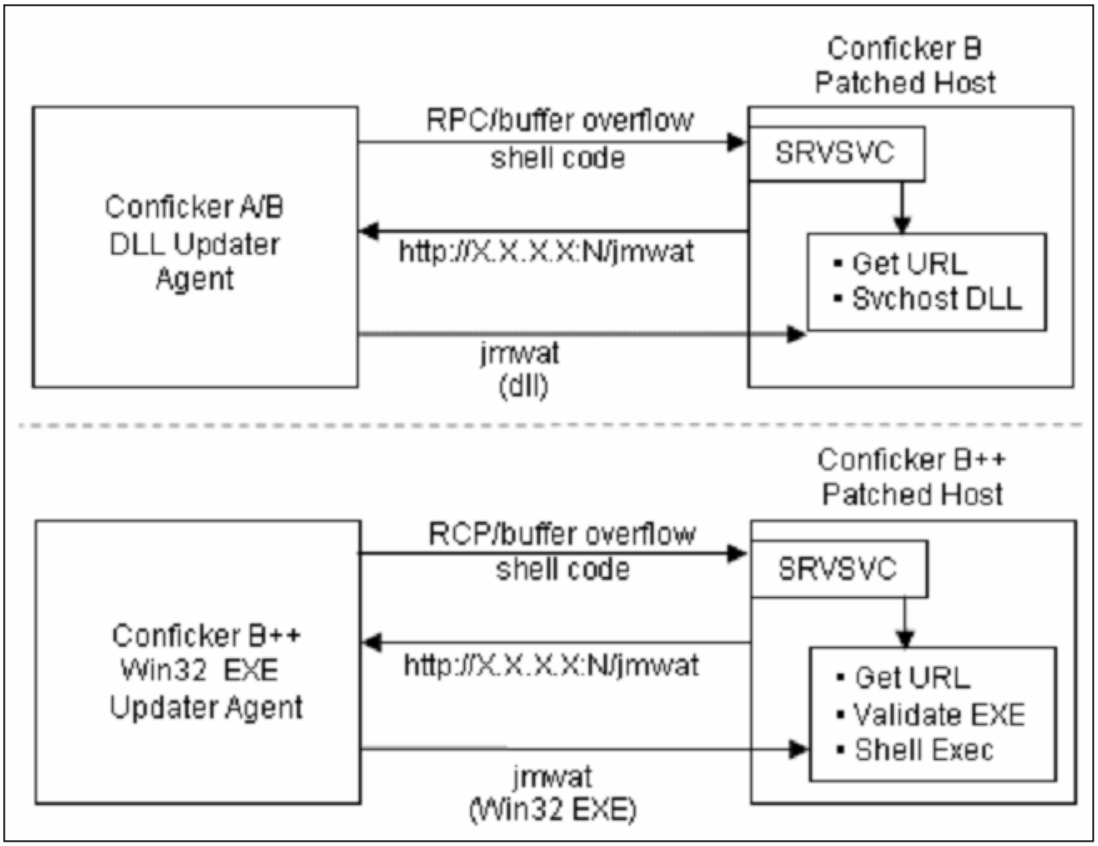
2.2.1 MS08-67

כאמור, הדרך המקורית והראשית דרכה הופצה התולעת למחשבים ורשתות חדשים, היא באמצעות ניצול פרצת אבטחת המידע MS08-067, אשר התגלתה ברכיב ה- Network Remote Procedure Call Service (RPC), אשר נועד כדי לאפשר הרצת פקודות מורשות בצורה מרוחקת. בעת ריצה, התולעת סורקת את הרשת המקומית ומחפשת קורבנות, כלומר מחשבים בהם עדיין לא הותקן טלאי אבטחת המידע. כתוצאה מניצול מוצלח של הפרצה, לתוקף (במקרה זה התולעת) יש אפשרות להרצת קוד מרחוק בהרשאות גבוהות מאוד.

[2] http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx

ברמה הטכנית, ה-Service נחשף ע"י התהליך Services.exe או Svhost.exe (תלוי בגרסת הWindows). ה-Service מתקשר עם DLL בשם 'srvsvc.dll', אשר מייצא פונקציה '_NetprPathCanonicalize' שנועדה לבדוק ולאחסן את הכתובת של מי שקראה לה. פונקציה זו בתורה קוראת ל-netapi32.dll, המייצאת פונקציה נוספת בשם 'sub_5B86A51B ' (השם תלוי בגרסת מערכת ההפעלה). מטרתה של פונקציה זו היא לבדוק אם כתובת מסויימת היא חוקית וגם להחליף ביטויים כגון \..\ לכתובות מלאות של תיקיות. לדוגמא הנתיב c://aa/../cc/bb יתורגם ל c://aa/bb.

הניצול מתאפיין בכך שתולעת הקונפיקר מעבירה מחרוזת ספציפית לפונקציה, כך שהתרגום של הכתובת בפונקציה sub_5B86A51B רושם את הנתונים מחוץ למחסנית (Buffer Overflow), מה שגורם למכונה להריץ את הקוד הזדוני. בקוד הזדוני ישנה טעינה של urlmon.dll הקורא לפונקציה URLDownloadToFile, שכשמו כן הוא מתחבר לשרת, להוריד ממנו קובץ ולשמור אותו בדיסק הקשיח.

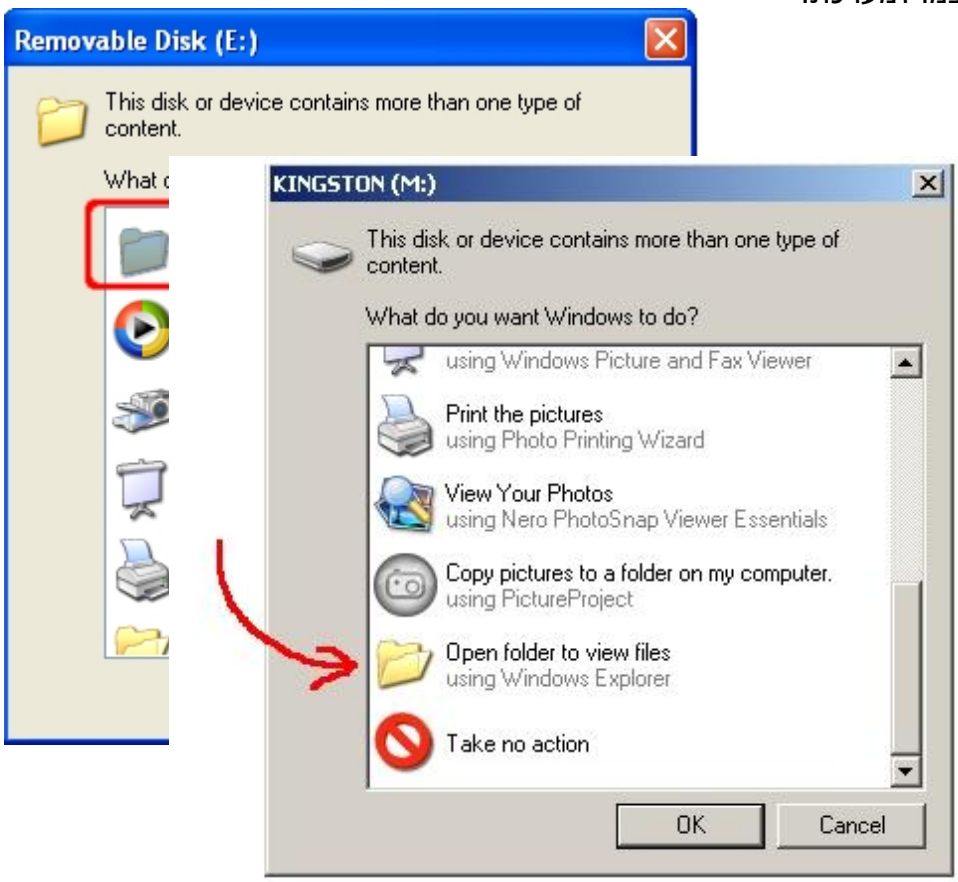


2.2.2 ניצול סיסמאות חלשות

מחשב אשר נדבק בתולעת מחפש ברשת המקומית שלו תיקיות משותפות, ומנסה לנחש את הסיסמא. במידה והארגון לא אוכף מדיניות סיסמאות קשיחה, בסופו של דבר התולעת תצליח לנחש את הסיסמה. לאחר שתולעת חודרת לתיקיה משותפת היא מעתיקה קבצים לתיקיית המערכת - בדר"כ היא שמה קובץ בתיקיה של ה-Tasks תחת השם at#.job וכן קובץ DLL בתיקיה System32. בצורה זו היא גורמת להרצה של Task מתוזמן שגורם לתהליך rundll32.exe להריץ אותו וליצור Service קבוע במערכת המותקפת עם הרשאות גבוהות.

2.2.3 ניצול Autorun

כאשר הקונפיקר נמצא במחשב, הוא יוצר 2 קבצים בתיקיית ה-Root של כל מדיה ניידת שהוא מזהה (לדוגמה Disk On Key). הקבצים שהוא יוצר הם xxxxxxx.inf (xxxxxxx - שם אקראי), וקובץ Autorun תואם. כאשר אותה מדיה מחוברת למחשב נוסף, מוצגת למשתמש האופציה של '**Open folder to view files**'. עם זאת, אופציה זו היא אופציה מזוייפת, מכיוון שכאשר המשתמש בוחר בה, הקובץ של aoutorun.inf נפתח, והקוד הזדוני טוען את עצמו למערכת.



2.3 פרטים טכניים נוספים

2.3.1 תיאור תהליך ההתפשטות

2.3.1.1 התבססות

לאחר התקנה מוצלחת, התולעת מעתיקה את עצמה בשם אקראי לתיקיה של %Sysdir%, כלומר תיקיית המערכת. לדוגמא: C:/windows/system32 - תלוי באיזו גרסא של Windows מדובר.

קיימות גרסאות של התולעת שמשתמשות במיקום חילופי:

ProgramFiles\Internet Explorer%

ProgramFiles\Movie Maker%

%temp%

C:\documents and settings\all users\application data

בנוסף, התולעת משנה Registry key על מנת להוסיף service אקראי על המכונה המותקפת:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\{random} \Parameters \"ServiceDll" = "Path to worm"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\{random} \ "ImagePath" = %SystemRoot%\system32\svchost.exe -k netsvcs

לרוב ניתן לראות רק את ה:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\{random}

(תלוי בגרסא של ה windows).

2.3.1.2 הכנת התשתית

בשלב הבא, התולעת מנסה להתחבר למספר אתרים כדי לבדוק את כתובת ה ip של המכונה:

- http://www.getmyip.org
- http://getmyip.co.uk
- http://checkip.dyndns.org
- http://whatsmyipaddress.com

לאחר מכן מורידה קובץ מהכתובת (בגרסא הראשונה)

http://trafficconverter.biz/4vir/antispyware/loada[REMOVED]

התולעת פותחת שרת HTTP במחשב הפגוע בפורט אקראי מ1024 עד 10000. שרת זה מכיל עותק של התולעת.

2.3.1.3 מציאת קורבנות

השרת עם התולעת סורק באופן קבוע את הרשת (בפורט 445) המקומית על מנת למצוא קורבנות חדשים (על פי פרצה MS08-67). ברגע שהשרת מוצא מכונה שניתן להדביק אותה בתולעת, הוא מנסה להדביק אותה – כלומר, אין נסיון להסוות את התהליך.

2.3.1.4 שכפול

לאחר מציאת קורבן מתאים, התולעת מעתיקה את עצמה למקומות הבאים:

% • Sysdir%\[Random].dll

% •Program Files%\Internet Explorer\[Random].dll

% •Program Files%\Movie Maker\[Random].dll

% •Program Files%\Windows Media Player\[Random].dll

% •Program Files%\Windows NT\[Random].dll

ומפסיקה את ה Services הבאים:

•WerSvc (Microsoft Vista Windows Error Service)

•ERSvc (Microsoft XP Windows Error Service)

•BITS (Microsoft Background Intelligent Transfer Service – Updates)

•wuauserv (Microsoft Windows Update)

•WinDefend (Microsoft AV)

•Wscsvc (Microsoft Windows Security Centre)

2.3.1.5 הסוואה

התולעת מחפשת תהליכים שיכולים להיות מסוכנים בשבילה, ומנסה לסיים אותם:

•wireshark (Network packet tool)
• unlocker (Rootkit detection tool)
• tcpview (Network packet tool)
• sysclean (Trend Micro AV tool)
• scct_ (Splinter Cell)
• regmon (Sys internals registry monitoring tool)
•procmon (Sys internals registry monitoring tool)
•procexp (Sys internals registry monitoring tool)
•ms08-06 (Privilege escalation HotFix)
•mrtstub (Microsoft Malicious Software Removal Tool)
•mrt. (Microsoft Malicious Software Removal Tool)
•Mbsa. (Microsoft Malicious Software Removal Tool)
•klwk (Kaspersky AV Tool)
•kido (Less common name for W32/Conficker.worm or W32/downad.worm)
•kb958 (Blocks MS08-067, KB958644)
•kb890 (Microsoft Malicious Software Removal Tool)
•hotfix (Microsoft hot fixes)
•gmer (Rootkit detection tool)
•filemon (Sys internals registry monitoring tool)
•downad (Common names for Conficker.worm or downad.worm)
•confick (Common names for Conficker.worm or downad.worm)
•avenger (Rootkit detection tool)
•autoruns (Hooking point detection tool)

בגרסאות חדשות התווספו גם המחרוזות הבאות:

• activescan
• adware
• av-sc
• bd_rem
• bdtools
• cfremo
• enigma
• kill
• mitre.
• ms-mvp
• precisesecurity
• stinger

2.3.2 פרוט לפי גרסאות

2.3.2.1 Conficker A

תאריך גילוי ראשוני: 21.11.08

צורת הפצה:

- דרך חור אבטחתי MS08-67 של Service של Microsoft.

מנגנון עדכון:

- התחברות לשרת `trafficconverter.biz`
- יצירה של 250 שמות Domain אקראיים ו-5 סיומות ומתעדכן דרכן.

הפעולה הסופית:

- מעדכן לגרסא B,C או D

2.3.2.2 Conficker B

תאריך גילוי ראשוני: 29.12.08

צורת הפצה:

- דרך חור אבטחתי MS08-67 של Service של Microsoft.
- מנסה לנחש סיסמאות לתיקיות שיתוף והעתקת התולעת לתיקיה.
- דרך מדיה ניידת.

מנגנון עדכון:

- יצירה של 250 שמות Domain אקראיים ו-8 סיומות ועדכון דרכן.
- פתיחת דלת אחורית לעדכון דרך חור אבטחתי MS08-67.

דרכי התגוננות:

- חוסם psDNS looku
- מבטל עדכון אוטומטי של מערכת ההפעלה

הפעולה הסופית:

- מעדכן לגרסא C או D

2.3.2.3 Conficker C\B++

תאריך גילוי ראשוני: 20.02.09

צורת הפצה: כמו בגרסה הקודמת

מנגנון עדכון:

- יצירה של 250 שמות Domain אקראיים ו-8 סיומות ומתעדכן דרכן.
- פותח דלת אחורית לעדכון דרך חור אבטחתי MS08-67.
- פותח ערוץ תקשורת עם שרת שליטה מרוחק ומוריד ממנו כתובת שרת לעידכון.

דרכי התגוננות: כמו בגרסה הקודמת

הפעולה הסופית: מעדכן לגרסא D

2.3.2.4 Conficker D\C

תאריך גילוי ראשוני: 04.03.09

צורת הפצה: כמו בגרסה הקודמת

מנגנון עדכון:

- יצירה של 50000 שמות Domain אקראיים ו-116 סיומות ומתעדכן דרכן.
- עדכון דרך רשת P2P ייעודית - סורק את הרשת בפרוטוקול תקשורת שבוני התולעת יצרו על מנת למצוא מכונות שנדבקו, ומעביר למכונות שהוא מצא עדכונים בפרוטוקול TCP.

דרכי התגוננות:

- חוסם DNS lookups לכתובות השייכות לו
- מבטל עדכון אוטומטי של מערכת ההפעלה
- מבטל Safe mode
- מבטל תהליכים של תוכנות אנטי-וירוס

הפעולה הסופית: מעדכן לגרסא E

2.3.2.5 Conficker E\D

תאריך גילוי ראשוני: 07.04.09

צורת הפצה: כמו בגרסה הקודמת

מנגנון עדכון: כמו בגרסה הקודמת

דרכי התגוננות: כמו בגרסה הקודמת

הפעולה הסופית:

- אם במחשב המותקף הייתה גרסא C מעדכן אותה ל D (בנוסף לE).
- מתקין תוכנת אנטי וירוס מזויפת בשם SpyProtect 2009.
- מתקין סוס טרויאני בשם Waledac – שמטרתו היא הפצה של דואר זבל.
- מסיר את עצמו מהמחשב בתאריך מוגדר מראש (בדר"כ 3.05.09) אבל הגרסא הקודמת נשארת על המחשב.

2.3.3 יכולות שונות

2.3.3.1 Hooking

Conficker מבצע מספר Hooks (תפיסה ושינוי של קריאות מערכת) במחשב הפגוע. התולעת מבצעת Hook לפונקציה NetpwPathCanonicalize. התולעת משנה את מספר הביטים ראשונים של הפונקציה, כך שברגע שקוראים לפונקציה היא מבצעת קפיצה למקום אחר בזיכרון.

בתמונה הבאה ניתן לראות את השינוי של הקוד.

```
5B86A259   8BFF          MOV EDI,EDI                      5B86A259 E9 A0B028A6   JMP 01AF52FE
5B86A25B   55            PUSH EBP
5B86A25C   8BEC          MOV EBP,ESP
5B86A25E   53            PUSH EBX                         5B86A25E 53            PUSH EBX
5B86A25F   8B5D 14       MOV EBX,DWORD PTR SS:[EBP+14]    5B86A25F 8B5D 14       MOV EBX,DWORD PTR SS:[EBP+14]
5B86A262   56            PUSH ESI                         5B86A262 56            PUSH ESI
5B86A263   57            PUSH EDI                         5B86A263 57            PUSH EDI
5B86A264   33FF          XOR EDI,EDI                      5B86A264 33FF          XOR EDI,EDI
5B86A266   3BDF          CMP EBX,EDI                      5B86A266 3BDF          CMP EBX,EDI
5B86A268   0F85 8EDE0000 JNZ NETAPI32.5B8780FC            5B86A268 0F85 8EDE0000 JNZ NETAPI32.5B8780FC
```

התולעת משתמשת בשיטות דומות לביצוע Hooking גם לפונקציות אחרות. למשל היא משבשת את ה-DNS Caching לאפליקציות אחרות על מנת לבצע פילטור על Name Resolutions של אתרי אנטי וירוסים שונים. בטבלה הבאה ניתן לראות את הפונקציות שקונפיקר מבצעה עליהן Hook.

DLL	Function
dnsapi.dll	DnsQuery_A
	DnsQuery_UTF8
	DnsQuery_W
	Query_Main
netapi32.dll	NetpwPathCanonicalize
ntdll.dll	NtQueryInformationProcess
wininet.dll	InetnetGetConnectedState
ws2_32.dll	sendto

ביצוע Hooking לפונקציה NetpwPathCanonicalize בעצם מבצעת גם חסימה של ניסיון של מישהו אחר לבצע ניצול של החור האבטחתי MS08-67, מה שמבטיח מצד אחד שליטה בלעדית על המכונה, וכן לוודא שמכונות אחרות לא ינסו להדביק את המכונה שוב ושוב. התולעת מנתחת את הבקשה של המחשב השני ומחלץ משם הכתובת של השרת שממנו אפשר להוריד גרסא חדשה יותר של התולעת.

2.3.4 יצירה של Domain Names

הגרסא הראשונה של הקונפיקר ייצרה כ-250 שמות של Domain בכל יום ובגרסאות האחרונות התולעת מייצרת 50000 שמות. לאחר יצירה של Domains התולעת מנסה להוריד מהם עדכונים. ההתחברות לשרתים אלו יכולה לגרום ל-Denial of service לשרתים, ולכן בגרסה C יוצרי התולעת ניסו להתגבר על הבעיה ע"י כך שמתוך ה-50000 שמות, מוגרלים רק 500 והמחשב הפגוע מנסה להתחבר אליהם.

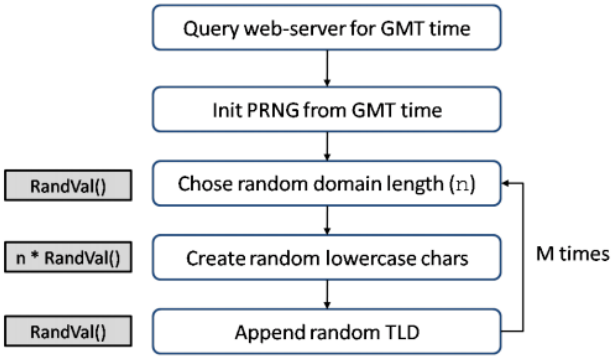
ההגרלה של שמות הDomains תלויה בגורמים רבים במחשב שבו נמצאת התולעת. אם ניסיון ההתחברות לשרת לא הצליח, התולעת ממתינה בין 40 ל 50 שניות ומנסה להתחבר ל-Domain הבא. אם כל ההתחברויות נכשלו התולעת ממתינה 24 שעות ומתחילה את התהליך מהתחלה. אם העידכון הצליח, קונפיקר ממתין 4 ימים לפני הורדה של עדכון נוסף. בגרסאות A ו B קונפיקר היה מנסה להתחבר לשרתים כל 2-3 שעות.

האלגוריתם של יצירת השמות מתבסס על התאריך הנוכחי, אבל התאריך לא נלקח מהמחשב המקומי אלא התולעת מבצעת בקשת Http רגילה לאחד מהאתרים הבאים:

- Baidu.com
- imageshack.us
- rapidshare.com
- w3.org
- ask.com
- msn.com
- yahoo.com
- google.com
- facebook.com

ומהתשובה שולף את התאריך. התולעת משתמשת בתאריך כבסיס לשם של ה-Domain. לאחר חישוב של שם הדומיין, התולעת מוסיפה אחת מהסופיות שיש אצלה במאגר.

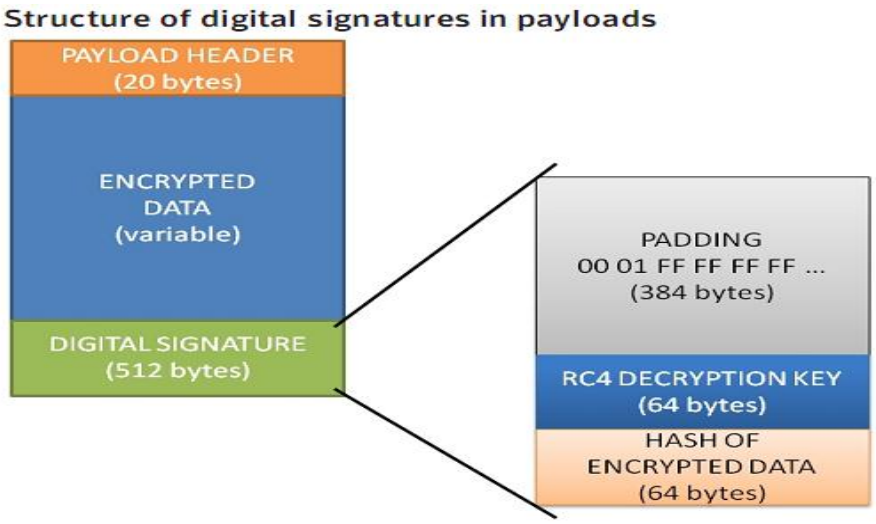
בתמונה הבאה ניתן לראות כיצד תהליך זה עובד:



ארגוני אבטחת מידע רבים ניצלו שיטה זו על מנת לרשום את ה-Domains המוגרלים כדי למנוע עדכון של התולעת ולנסות להעריך את כמות המחשבים המודבקים.

2.3.5 הצפנה

קונפיקר משתמש בהצפנה ותחימה על הקבצים. כל העדכונים מהשרת לקורבן מגיעים חתומים, ומחשב הקורבן מוודא שהחתימה תקינה, ורק לאחר מכן פותח את הקובץ המוצפן. במידה ומישהו מנסה להתחזות לשרת Conficker ושולח עדכון למכונה אחרת, המכונה לא תפתח את הקובץ כי החתימה לא תהיה תקינה.



2.3.6 רשימות שחורות

לתולעת ישנן גם רשימות שחורות עם כתובות שחברות אבטחת המידע מפרסמות. בכל פעם שהתולעת מנסה לעדכן את הגרסה, היא בודקת את הכתובת של הדומיין, ואם היא נמצאת ברשימה השחורה, או אם זו כתובת פנימית התולעת לא מבצעת את הקישור.

2.4 נזקים אפשריים

2.4.1 השחתה של מערכות הגנה

מרגע התקנתו, קונפיקר פועל לניטרול מערכות ההגנה של המחשב בו הוא יושב, על פי רשימה מתעדכנת. כלומר, המחשב שבו נמצא התולעת פתוח לניצול בכל זמן נתון וכותבי התולעת יכולים לעשות בו כרצונם בכל זמן נתון, ללא שום התרעה ממערכות הגנה.

2.4.2 יצירת רשת Botnet

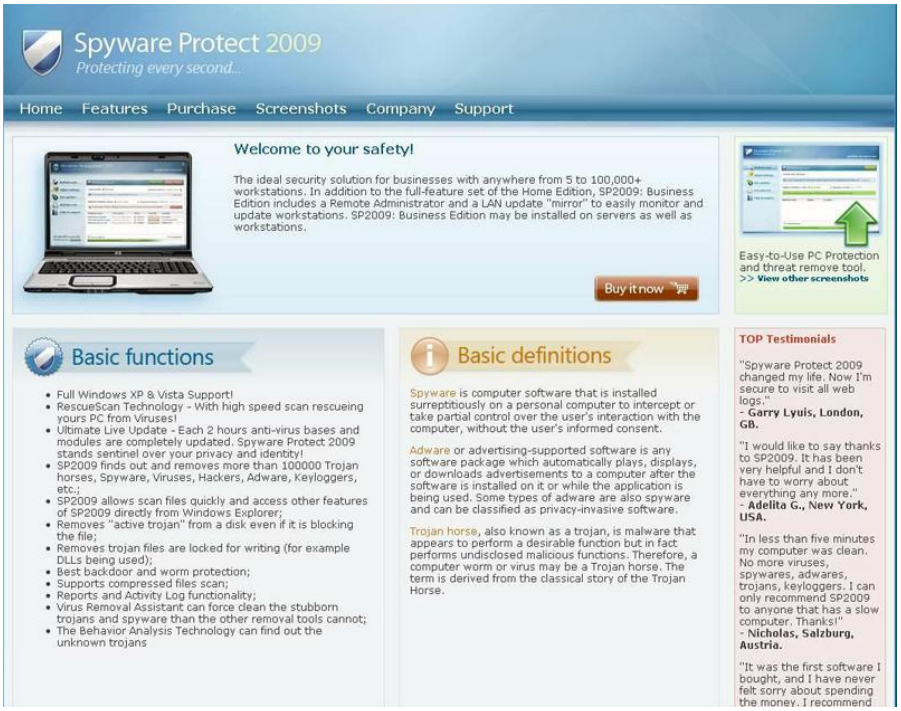
Conficker בעצם יוצר רשת של Botnets, אשר בשיא כוחה הגיעה למליוני מחשבים. על הסכנות האפשריות של רשתות בוטנט נכתב כבר בעבר, וניתן אף לקרוא במסמכים אחרים של הצוות.

החל מאמצע שנת 2009 תשתיות ממשל זמין נמצאות תחת מתקפת נסיונות SQL Injection ללא הפסקה. תקיפות אלו מאופיינות על ידי מספר מצומצם של User Agents, הקשורות לרשת בוטים הידועה בעולם תחת השם nv32ts. למרות שהנושא לא הוכח בצורה מוחלטת, ההשערה המקובלת כיום היא שרשת זו מבוססת על גבי תשתית הבוטים של תולעת הקונפיקר.

2.4.3 התקנת תוכנות זדוניות נוספות

לאחר שקונפיקר מתחיל לרוץ במחשב הנגוע מתחילים לקפוץ Pop-up עם פרסומת לתוכנת אנטי וירוס מזויפת. אם משתמש במערכת מתפתה ונכנס לאתר של האנטי וירוס, באתר מוצעת לגולש סריקה חינם. לאחר הסריקה האנטי וירוס מודיע שבמחשב ישנם תוכנות זדוניות (שלא באמת קיימות) ומציע ללקוח לרכוש את התוכנה תמורת $49.95 על מנת להסיר את התוכנות הזדוניות.

לחילופין יכולות פשוט להתחיל להופיע התראות על תוכנות זדוניות שנמצאות על המחשב ועל מנת להסירן צריך להתקין את התוכנה המזויפת.



ממשק התוכנה דומה לממשקים של מערכות ההגנה של Microsoft, ולכן משתמש יכול בקלות לחשוב שזו התראה לגיטימית של חברת Microsoft ולרכוש את המוצר. בגרסא האחרונה קונפיקר מתקין גם וירוס נוסף בשם Waledac אשר מטרתו העיקרית היא הפצת דואר זבל, גניבת מידע פיננסי ומצרף את המחשב הנגוע לרשת Bot נוספת.

Spyware Protect 2009
Protecting every second...

Perform scan
Adjust settings
Get updates
Activate now
Help & support

Performing scan
Start scan

Current state: Scan complete

Warning
There are serious threats detected on your computer. Your privacy and personal data may not be safe. Do you want to Clean and Protect your PC?
Yes, remove threats
No, continue unprotected

LdPinch V	Critical	A variant of the Key Logger that captures passwords as t
Advanced Stealth Email	Critical	Advanced Stealth Email Redirector (Advanced SER) is a pr
VMalum AWS	High	Trojan: Any program with a hidden intent. Trojans are one
CNNIC Update U	Very high	A program that downloads and may execute or install soft
Bancos DMD		

Your PC is currently unprotected and may be exposed to spyware adware, trojans and viruses
Get full real-time protection

Spyware alert!
Vulnerabilities found
Your computer is infected by spyware - 34 serious threats have been found while scanning your files and registry. It is strongly recommended that you disinfect your computer and activate Realtime secure protection against future intrusions.
Why do you need Spyware Protection?
Upgrade to full version of Spyware Protect 2009 security kit to clean your computer and prevent new security and privacy attacks. You will be able to download daily updates and get online protection against internet attacks.
Activate Spyware Protect 2009
Stay unprotected

Windows Security alert
Windows reports that computer is infected. Antivirus software helps to protect your computer against viruses and other security threats. Click here for the scan you computer. Your system might be at risk now.

100% Satisfaction
We guarantee that Spywa
more secure or your mone
let us know within 30 day
That's risk-free protection

Why Choose Spyw
Proactive security for wha
most sophisticated securit
automatically and continua

Maximum Support Guarantee !
Fast support will help you with any troubles and will answer your questions within 24h. We work 24/7 for You.

Qty.	Item	Delivery	Support and Updates	Price
1	Spyware Protect	Online download	Lifetime	USD 49.95

☑ Yes, I have read and agreed to the following Terms and Conditions

NOTE: **Download and install full version after purchase.**

CONTINUE TO SECURE ORDER PAGE

VISA MasterCard We accept Visa and MasterCard credit or debit cards. Your order will be entered using a secure server witch SSL certificate and data encryption.

2.5 היסטוריה וסטטיסטיקות

2.5.1 אירועים חריגים

בינואר 2009 הקונפיקר שיתק את הרשת הצבאית של צרפת. מפעילי הרשת הניחו שהיא מוגנת עקב היותה מנותקת מרשת האינטרנט, אך לא לקחו בחשבון הכנסה של מדיה ניידת. שיתוק זה גרם לביטול של מספר טיסות עקב כך שלא יכלו להוריד את התוכנית של הטיסות מבסיס הנתונים.

באותו החודש קונפיקר חדר למשרד הביטחון הבריטי ושיתק מערכות חיוניות ורשתות אדמיניסטרטיביות של המשרד. לאחר מכן הוא התפשט לאניית קרב ולצוללות של הצבא המלכותי ולאחר מכן לבית חולים בעיר שפילד. במתקפה זו נדבקו כ-800 מחשבים.

ב-2 לפברואר נדבקו כמאה מחשבים של הבונדסוור - הצבא של הרפובליקה הפדראלית של גרמניה.

ב 13 לפברואר חברת Microsoft הציעה פרס של $250,000 לכל מי שימסור מידע שיגרום למעצרם של בוני התולעת.

קונפיקר הגיעה גם למערכות של המועצה העירונית של מנצ'סטר, הנזק המוערך שהוירוס גרם הוא כ£1.5 מיליון - המועצה לא הצליחה להנפיק דוחות, לשלוח דואר אלקטרוני ואף להדפיס מסמכים. עקב המקרה נאסר השימוש בהתקני USB ברשת של המועצה.

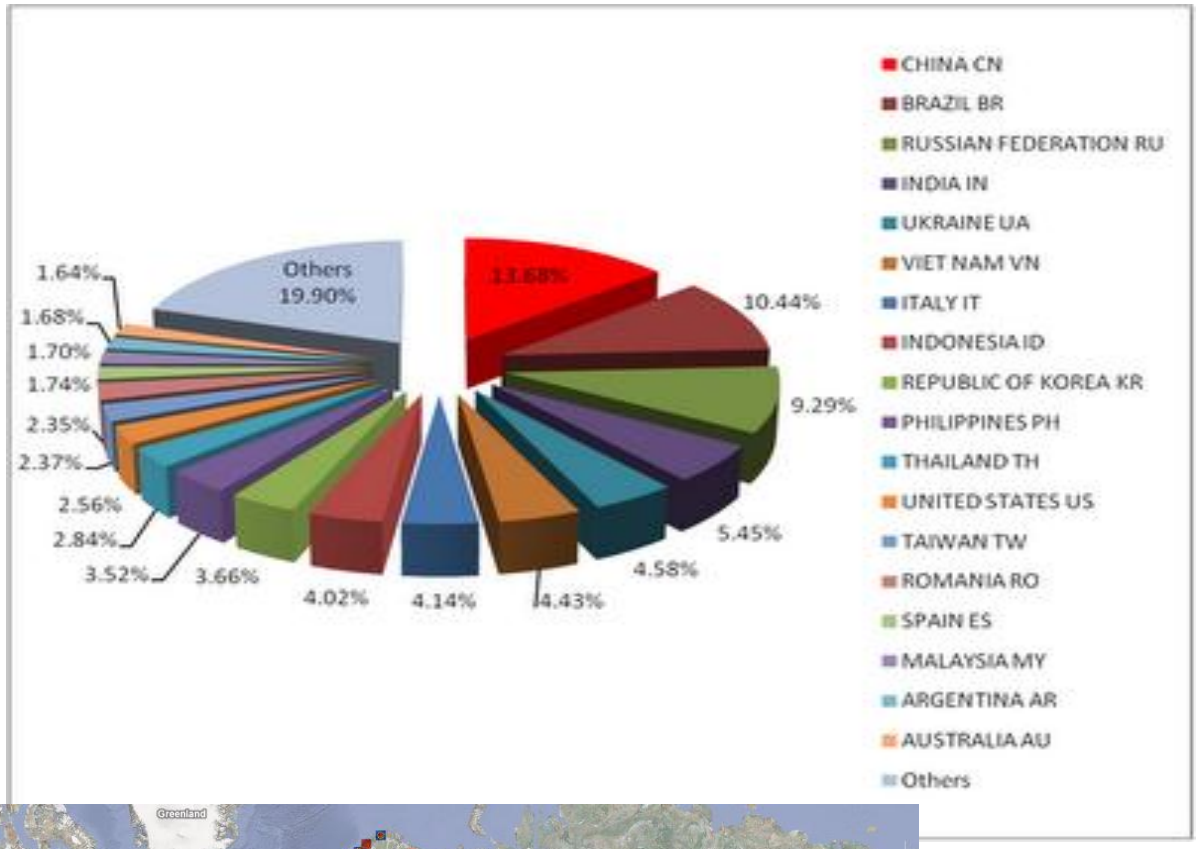
בפבואר 2009 קונפיקר פגע גם בחברת בזק הישראלית. לבזק לקח למעלה משבוע ימים כדי להתגבר על התקלה, שבעטיה נפלו מערכות חיוניות. תולעת המחשבים תקפה גם את פלאפון, חברת הבת של בזק.

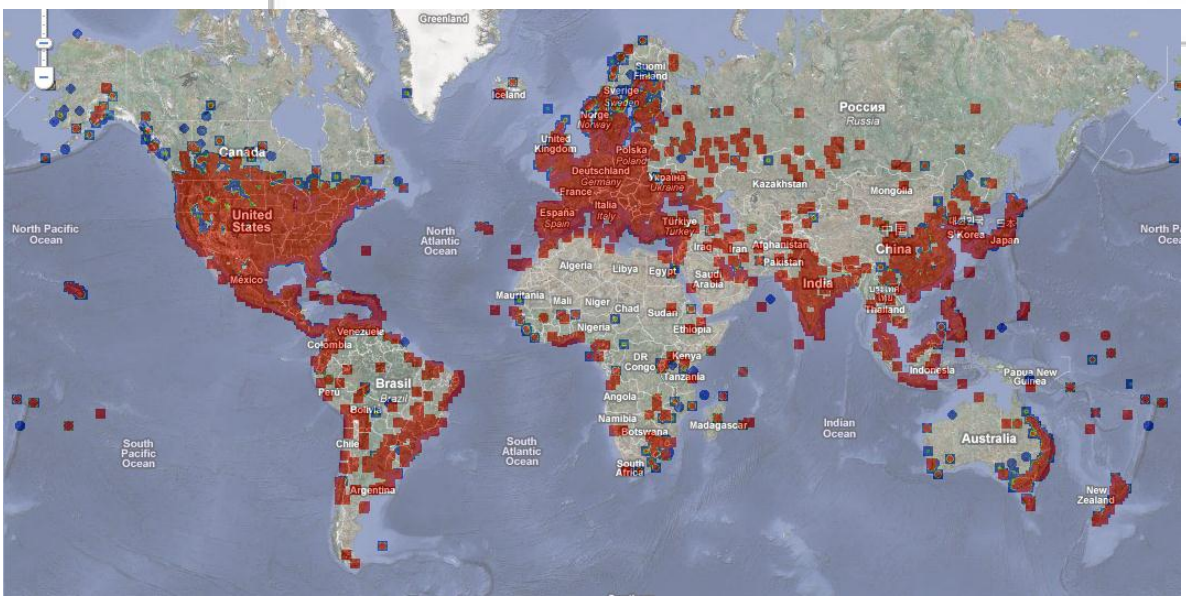
במאי התולעת תקפה ציוד של בתי חולים בארצות הברית. הדבר קרה עקב כך שהרבה מהציוד היה מחובר לרשת מקומית וחלק מהציוד היה מבוסס על מערכת חלונות. החשד הוא שמישהו התחבר לרשת עם מחשב נייד שהיה נגוע בתולעת והדביק את כל הרשת.

2.5.2 סטטיסטיקה

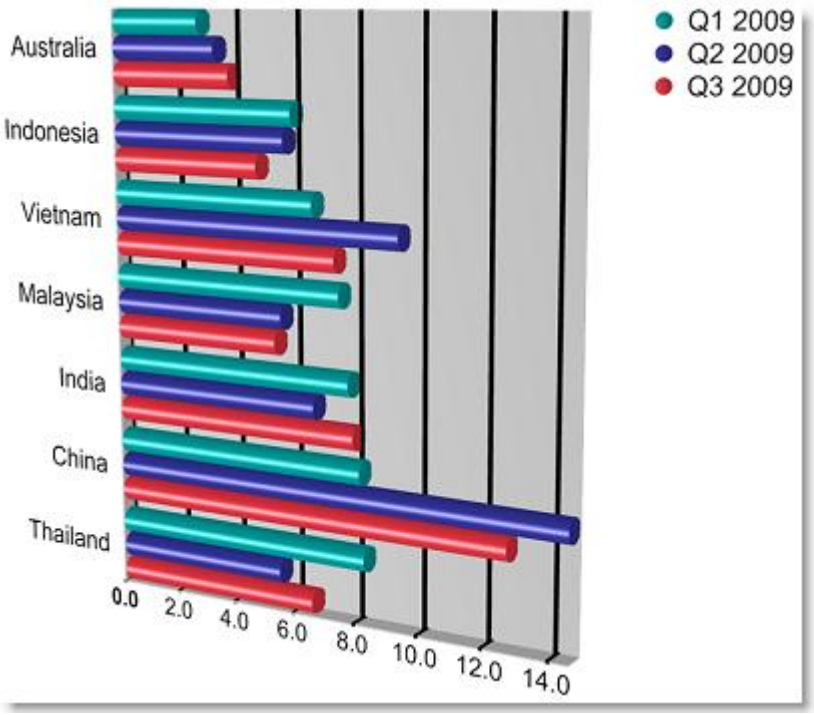
אין כרגע הערכה מדויקת של מספר המכונות שנדבקו מהתולעת אבל יש כאלה הטוענים שמספר המכונות הגיעה עד ל 15 מיליון. יש כאלה שמאריכים את הנזק הכלכלי ב-9.1 ביליון דולר. החישוב כולל לא רק את הנזק שנגרם אלא גם הוצאות של ניסיונות לחסום את התולעת, ורכישה של תוכנות אנטי וירוסים שונות.

2.5.2.1 חלוקה לפי מדינות

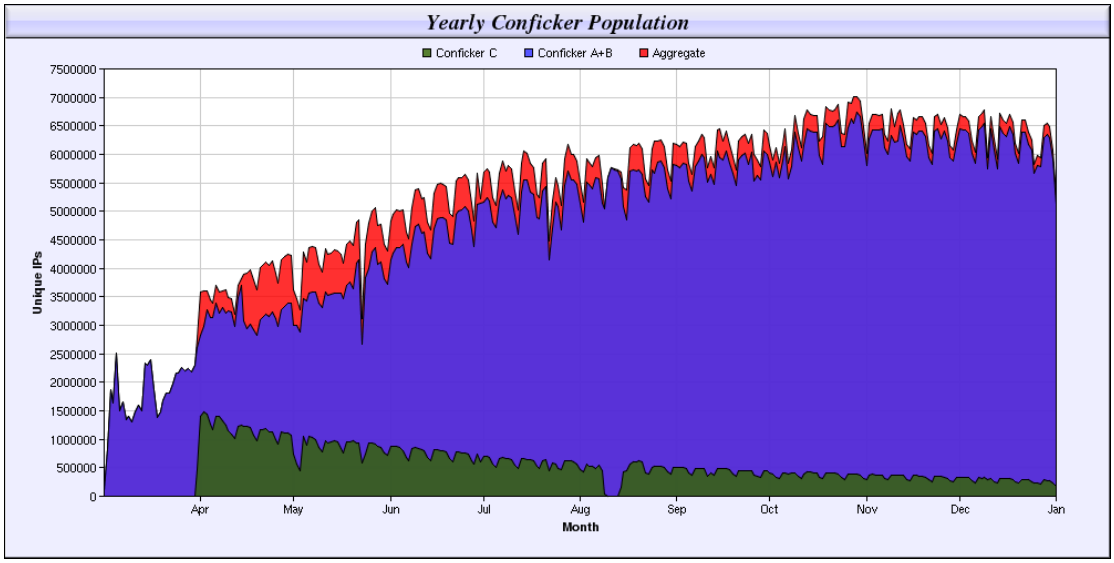




2.5.2.2 10 המדינות שנדבקו הכי הרבה לפי 3 רבעונים ראשונים



2.5.2.3 התפשטות הסוס בשנת 2008-2009



2.6 הימנעות מהדבקה

על מנת להימנע מהדבקה של התולעת יש לשמור על העקרונות הבסיסיים של אבטחת המידע במחשבי קצה ושרתים:

1. יש להתקין תוכנת אנטי וירוס.
2. יש לעקוב אחרי עדכונים של מערכת ההפעלה ותוכנות אנטי וירוסים ולפעול להתקנתם (במיוחד עדכונים קריטיים, ובפרט את Microsoft ms08-067).
3. יש לוודא שימושש בסיסמא חזקה למערכת ולתיקיות המשותפות.
4. יש לתת הרשאות קריאה בלבד לתיקיות המשותפות.
5. יש לבטל את האפשרות של AutoRun על המערכת.

2.7 גילוי והסרה

2.7.1 סימפטומים

ברגע שישנו מחשב ברשת שנדבק בתולעת יכולים להופיע סימפטומים הבאים:

1. העדכונים אוטומטיים למערכת ההפעלה ולתוכנות אנטי וירוסים לא פעילים.
2. תיקיות משותפות עם הגנה של שם משתמש וסיסמא ננעלות.
3. האטה בתעבורה ברשת.
4. אין אפשרות לגשת לאתרי אינטרנט הקשורים לאבטחת מידע.
5. כלים שונים הקשורים לאבטחת מידע לא יפעלו.

2.7.2 גילוי הידבקות

1. על מנת לבדוק האם המחשב מודבר בתולעת ניתן לגלוש לדף הבא: http://www.confickerworkinggroup.org/infection_test/cfeyechart.html. אם התמונות מופיעות כראוי הדבר יכול להצביע על 2 דברים - או שבמחשב המדובר אין תולעת או שהמחשב נימצא מאחורי Proxy.

2. ניתן להסניף תעבורה ברשת המקומית ולראות האם יש בקשות רבות לפורט 445, בפורט זה התולעת סורקת את הרשת ומנסה להדביק מכונות אחרות.

3. כפי שתואר קודם התולעת כל יום מייצרת 50,000 שמות Domain על מנת להתעדכן. הדבר מקשה מאוד על חסימת התקשורת עם השרתים, כי יש קושי לחשב כל יום 50,000 Domains. בנוסף חסימת שמות אלו לא תעזור, כי התקשורת מתבצעת לפי כתובת ה-IP. עם זאת, ניתן לזהות בקשות של התולעת, מכיוון שלכולן מאפיינים דומים:

גירסא A: http:/xxx.xxx.xxx.xxx /search?q=1003&aq=7

גירסא B ומעלה: http:// xxx.xxx.xxx.xxx /search?q=328924

כאשר ה xxx.xxx.xxx.xxx – מסמל מספר Ip של השרת המספר שמופיע לאחר האות q מסמל כמה מכונה נוספות התולעת הצליחה להדביק. (ערך זה נירשם ב Regestry של השרת ולכן גם אחרי Restart הערך נשמר). הערך שהופיעה לאחר האותיות aq תמיד נשאר קבוע, החוקרים משערים שהמטרה הייתה לסמל את הגרסא של התולעת אך כבר בגרסא השנייה ערך זה לא הופיעה.

3.ביבליוגרפיה וקריאה נוספת

- http://www.malwareinfo.org/files/W32.DownadupThreat.pdf
- http://download.nai.com/products/mcafee-avert/documents/combating_w32_conficker_worm.pdf
- http://www.sophos.com/sophos/docs/eng/marketing_material/conficker-analysis.pdf
- http://www.honeynet.org/files/KYE-Conficker.pdf
- http://www.bitdefender.com/files/Main/file/Conficker_-_One_Year_After_-_Whitepaper.pdf
- http://www.netsecdb.de/node/2407
- http://www.thepeople.co.il/_DailyMaily/ItemClean.asp?ArticleID=24395&Vol=844&SearchParam=&CategoryID=72
- http://www.eset.com/threat-center/encyclopedia/threats/confickera
- http://www.eset.com/threat-center/encyclopedia/threats/confickeraa
- http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepaper/the_downadup_codex_ed1.pdf
- http://www.honeynet.org/files/KYE-Conficker.pdf
- http://www.wenpoint.com/securityinfo/malware/how-conflicker-spread.php
- http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking
- http://apcsnh.com/vacm/vacm11509.php
- http://www.globes.co.il/news/article.aspx?did=1000433279
- http://www.246.co.il/daat/itmab.asp?fn=711051051-278
- http://mtc.sri.com/Conficker/
- http://vil.nai.com/vil/content/v_153464.htm
- http://www.viruslist.com/en/weblog?weblogid=208187654
- http://www.symantec.com/business/security_response/writeup.jsp?docid=2009-010717-4209-99
- http://tools.cisco.com/security/center/viewAlert.x?alertId=17121
- http://www.theregister.co.uk/2009/01/20/sheffield_conficker/
- http://voices.washingtonpost.com/securityfix/2009/03/obscene_profits_fuel_rogue_ant.html
- http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Trojan%3AWin32%2FFakeSpypro&ThreatID=-2147347278
- http://www.onlinesecurity-guide.com/online-security-news/conficker-attacks-hospital-devices/
- http://www.networkworld.com/news/2009/020909-conficker-worm-sinks-french-navy.html

- http://www.physorg.com/news160331005.html
- http://blogs.zdnet.com/security/?p=3207
- http://cybersecureinstitute.org/blog/?p=15
- http://www.newscientist.com/article/mg20227121.500-the-inside-story-of-the-conficker-worm.html?page=3
- http://voices.washingtonpost.com/securityfix/2009/03/obscene_profits_fuel_rogue_ant.html
- http://support.microsoft.com/kb/962007
- http://blogs.iss.net/archive/ConfickerwSQLInjecti.html