ממשל זמין – פרויקט תהיל"ה

דו"ח סיכום

-

STORM WORM

ממשל זמין – פרויקט תהיל"ה

מאפייני מסמך

מחבר	פולינה חזנוב, יול בהט
מספר גרסה	1.0
סטטוס	סופית
תאריך הוצאה	נובמבר 2009
שם קובץ אלקטרוני	

תשומות / הערות

שם/תפקיד	הערה (אופציונאלי)	תאריך	חתימה

היסטוריה

מ. גרסה	ת. הוצאה	מחבר	שינויים מרכזיים בגרסה
0.1		פולינה חזנוב, יול בהט	גרסה ראשונה
1.0	03/11/09	פולינה חזנוב, יול בהט	גרסה סופית

הפצה

מ. גרסה	נמענים
1.0	רשימת תפוצה SI

ממשל זמין – פרויקט תהיל"ה

תוכן עניינים

1. כללי 4

1.1 רקע 4

1.2 Storm worm 4

2. סוסים טרויאניים באופן כללי 5

2.1 מה הוא סוס טרויאני 5

2.2 שימושים נפוצים 5

3. Storm Worm - בפירוט 6

3.1 כללי 6

3.2 דרכי הפצה 7

3.2.1 כללי 7

3.2.2 הפצה דרך דואר אלקטרוני 7

3.2.3 הפצה דרך בלוגים 9

3.3 אופן פעילות ויכולות שונות 11

3.3.1 כללי 11

3.3.2 גישה לאתר להורדת הקוד (רשתות Fast-Flux) 11

3.4 למה P2P? 17

3.5 היסטוריה וסטטיסטיקות 18

3.5.1 כללי 18

3.5.2 קמפייני ההפצה הגדולים 19

3.5.3 אירועים חריגים 20

3.5.4 תפוצת ה-Storm בעולם 20

3.5.5 סטטיסטיקות תפוצה בממשלת ישראל 22

3.6 גילוי והסרה 22

4. ביבליוגרפיה וקריאה נוספת 23

5. נספחים 24

5.1 רשימת שמות של ה Storm worm 24

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.

2.1 Storm worm

מסמך זה מסכם את הידע הצבור כיום בידי צוות אבטחת המידע על סוס טרויאני הידוע בכינוי Worm Storm. הסוס, אשר למעשה מפגין מאפיינים מעורבים לסוסים טרויאניים, תולעים ווירוסים, מפיץ עצמו בעיקר באמצעות דואר אלקטרוני. מטרתו העיקרית היא פתיחת דלת אחורית (Back Door) למחשב המודבק וחיבורו לרשת זומבים (Bot Net).

2.סוסים טרויאניים באופן כללי

1.2 מה הוא סוס טרויאני

סוס טרויאני (Trojan horse) הינו תוכנה מזיקה ("נוזקה") החודרת למחשב תוך התחזות לתוכנה תמימה. סוס טרויאני מופיע בדרך כלל כקובץ המצורף לדואר אלקטרוני או כתוכנה חופשית להורדה. בעת הפעלתו יבצע פעילות משעשעת או מועילה, כדי לגרום למקבל התוכנה לשלוח אותה הלאה לחברים נוספים. אותה פעילות משעשעת (למשל סרטון קצר) היא הסוואה לכך שהתוכנה מתקינה את עצמה במחשב, ועלולה לגרום נזק.

2.2 שימושים נפוצים

ישנם סוסים טרויאנים שתפקידם לתת הרשאות למשתמש אחר להיכנס למחשב הנפגע מרחוק. פעולה זו נקראת גם התקנת 'דלת אחורית' (BackDoor).

סוסים טרויאנים אחרים הם מסוג רוגלה , כלומר אוספים מידע מהמחשב שבו הותקנו (למשל מספרי כרטיסי אשראי או סיסמאות), ואז שולחים אותו ליעד מוגדר מראש.

סכנה נוספת היא הפיכת המחשב ל"זומבי" באמצעות תוכנת הסוס הטרויאני. מחשב זומבי הוא מחשב שנשלט מרחוק באמצעות המנגנון של תוכנת הסוס הטרויאני. אף שרוב הזמן הוא מתפקד כרגיל, ניתן להורות לו מרחוק לבצע פעולה בניגוד לרצון בעליו. כאשר מחשב כזה מחובר לרשת הוא עלול לשמש לביצוע מתקפת מניעת שירות, שליחת דואר זבל אלקטרוני וכו'. כאשר תוקף מסוים השיג שליטה שכזו במספר רב של מחשבים, הוא יכול לבצע את הפעולות הזדוניות בהיקף רחב מאוד, ועל ידי כך להגביר את הנזק הפוטנציאלי. רשת מסוג זה ידועה כ-Botnet.

3.Storm Worm - בפירוט

1.3 כללי

בראשית שנת 2007 זיהו חוקרים קוד זדוני חדש שזכה לכינוי Storm Worm. שם זה איחד למעשה רשימה ארוכה של תולעים וסוסים שונים כגון Zhelatin, Nuwar ו-Peacomm, אשר התגלו כזנים שונים של אותו הקוד. הסוס נחשב לחלוץ במובנים רבים, בין היתר בעקבות בטכניקות חדשניות בהן הוא עושה שימוש על-מנת להפיץ ולהסוות את עצמו, ברוחב תפוצתו ובשימוש הכלכלי הנעשה בו. למרות כינויו, Storm Worm למעשה אינה תולעת, אלא סוס טרויאני, וזאת משום שהוא אינו משתכפל באופן עצמאי. יוצרי הסוס מפיצים אותו בדרכים שונות, תוך שימוש ברשת ה-Botnet עצמה, והפעלה של טכניקות של הנדסה חברתית. שמו, Storm, ניתן לו עקב כך שבראשית דרכו הנושא של הדואר האלקטרוני בו הופץ היה מקושר לסופות (Storm) גדולות באירופה.

היקף ההידבקות ב-Storm, אינו ידוע במדויק; ההערכות השמרניות ביותר מדברות על כרבע מליון מחשבים נגועים בספטמבר 2007 ואילו הערכות אחרות מדברות על עד 50 מיליון מחשבים בשיאו. בתקופה זו יוחסה לו התפוצה של כ-8% מהקוד הזדוני על גבי מערכות Windows.

הסברה המקובלת היא שהארגון העומד מאחורי הStorm Worm, ושולט ב-Storm Botnet, הוא לא אחר אלא הארגון הרוסי RBN, אשר מידע עליו ניתן למצוא באינטרנט, וכן במסמך הסיכום על הסוס הטרויאני Zeus, שנכתב גם כן על ידי צוות Security Intelligence.

2.3 דרכי הפצה

1.2.3 כללי

כאמור למעלה, Storm אינו מפיץ את עצמו בצורה עצמאית, כדוגמת סוסים טרויאנים נפוצים, אלא משתמש בשיטות שונות של הנדסה חברתית (Social Engineering). בדרך כלל הקורבן מקבל דואר אלקטרוני, אך קיימות גם שיטות נוספות.

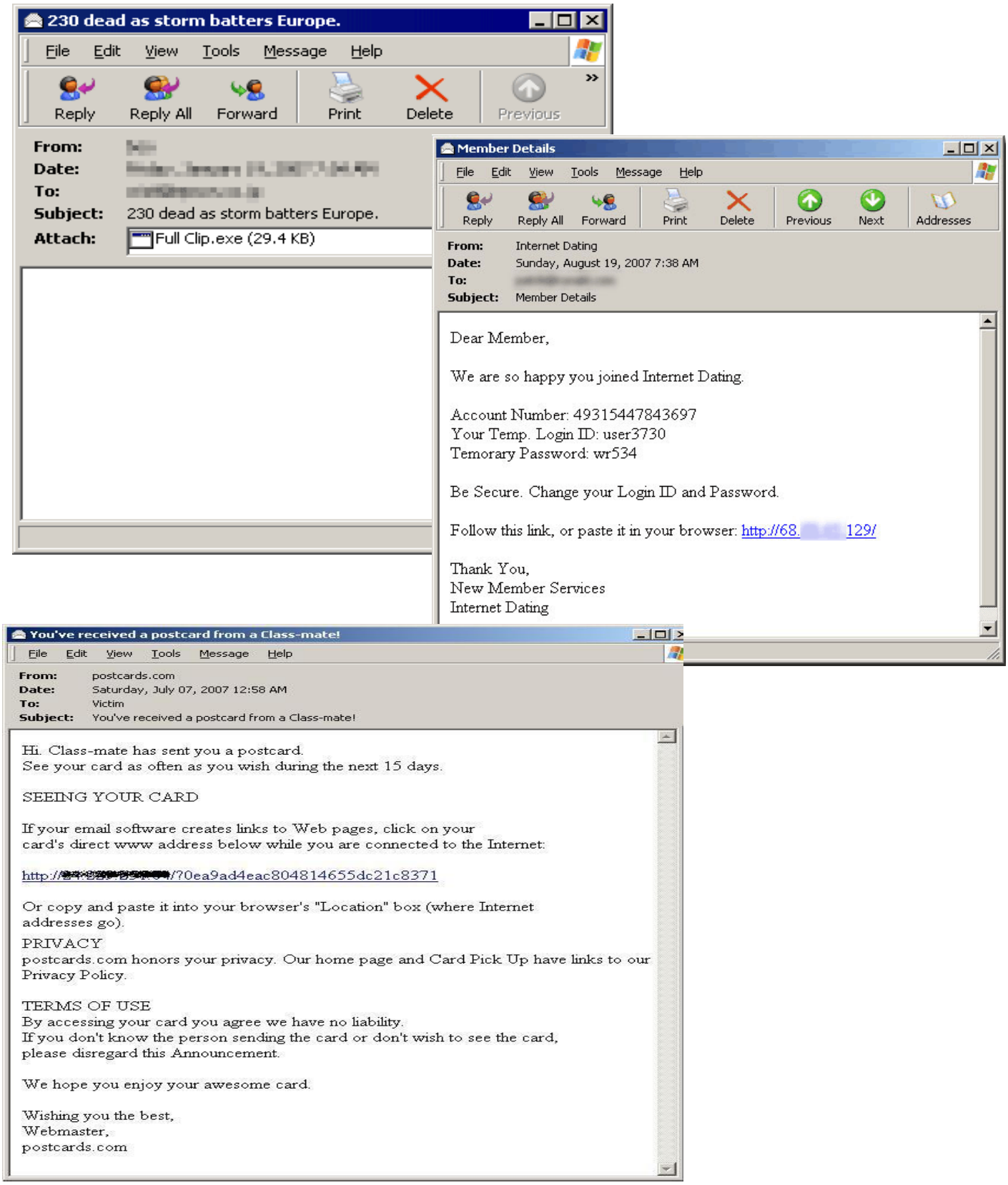
2.2.3 הפצה דרך דואר אלקטרוני

הדך הנפוצה להפצת Storm הינה דואר אלקטרוני המכיל קישור לאתר מפתה כגון חשדות דרמטיות, כרטיס ברכה מאדם קרוב, מכתב מבחורה רווקה ורבים אחרים. שיטה נוספת היא צירוף קובץ הרצה בשם מעניין ותמים הגורם לקורבן להריצו בלי חשש. ישנן ואריאציות שונות ומגוונות לשמות של הקובץ למשל: FullVideo.exe, Full Story.exe,Read More.exe, או GreetingPostcard.exe. את הכינוי קיבל Storm לאחר שהמיילים הראשונים שזוהו עימו נשאו את הכותרת: "230 הרוגים כתוצאה מסופה באירופה". יש להדגיש כי כותרות המיילים הזדוניים ותוכנם משתנים בתדירות גבוהה על מנת למנוע זיהוי שלהם עם Storm , ויוצרי המיילים דואגים שיהיו אקטואליים. כך למשל המייל שבישר על הסופה הקטלנית, נשלח בדיוק בזמן שבו סופה גאתה במרכז אירופה. הדבקות אחרות נעשות על ידי מיילים שמפנים ל"כרטיסי ברכה" בדיוק בתקופות החגים. פירוט על קמפייני ההפצה הגדולים ניתן למצוא בהמשך המסמך.

www.gov.il

ממשל זמין – פרויקט תהיל"ה

מיילים לדוגמא :



230 dead as storm batters Europe.

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous

From: [redacted]
Date: [redacted]
To: [redacted]
Subject: 230 dead as storm batters Europe.
Attach: Full Clip.exe (29.4 KB)

Member Details

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous Next Addresses

From: Internet Dating
Date: Sunday, August 19, 2007 7:38 AM
To: [redacted]
Subject: Member Details

Dear Member,

We are so happy you joined Internet Dating.

Account Number: 49315447843697
Your Temp. Login ID: user3730
Temorary Password: wr534

Be Secure. Change your Login ID and Password.

Follow this link, or paste it in your browser: http://68.[redacted]129/

Thank You,
New Member Services
Internet Dating

You've received a postcard from a Class-mate!

File Edit View Tools Message Help

From: postcards.com
Date: Saturday, July 07, 2007 12:58 AM
To: Victim
Subject: You've received a postcard from a Class-mate!

Hi. Class-mate has sent you a postcard.
See your card as often as you wish during the next 15 days.

SEEING YOUR CARD

If your email software creates links to Web pages, click on your card's direct www address below while you are connected to the Internet:

http://[redacted]/?0ea9ad4eac804814655dc21c8371

Or copy and paste it into your browser's "Location" box (where Internet addresses go).

PRIVACY
postcards.com honors your privacy. Our home page and Card Pick Up have links to our Privacy Policy.

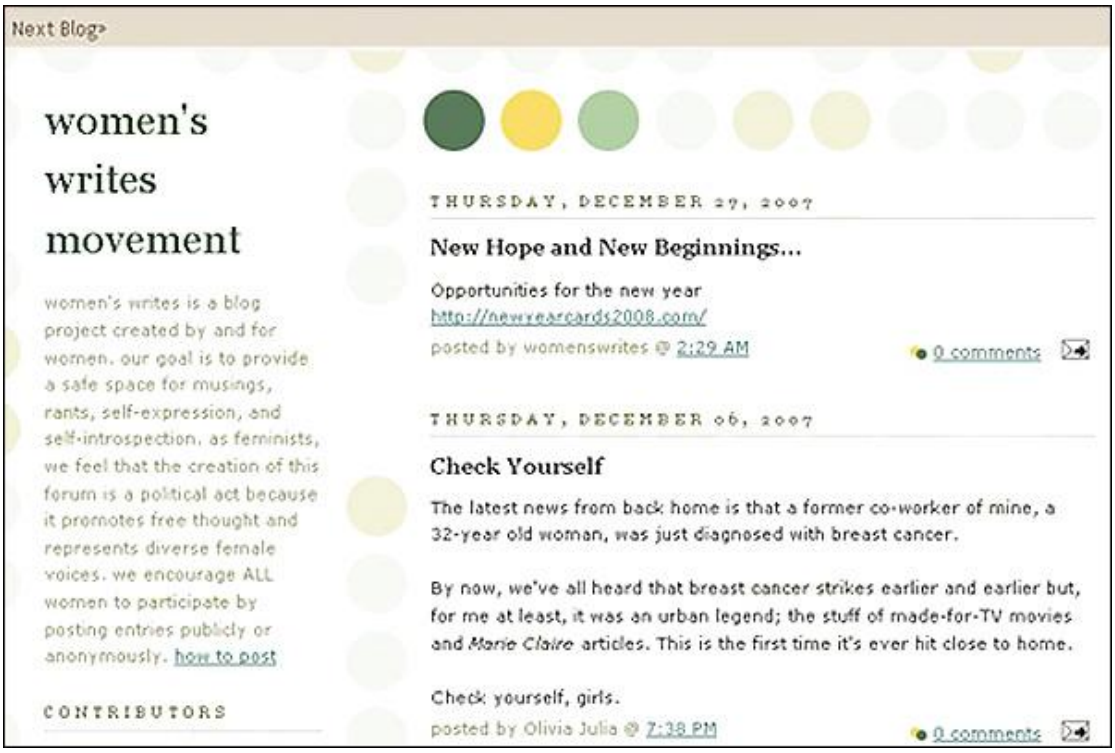
TERMS OF USE
By accessing your card you agree we have no liability.
If you don't know the person sending the card or don't wish to see the card, please disregard this Announcement.

We hope you enjoy your awesome card.

Wishing you the best,
Webmaster,
postcards.com

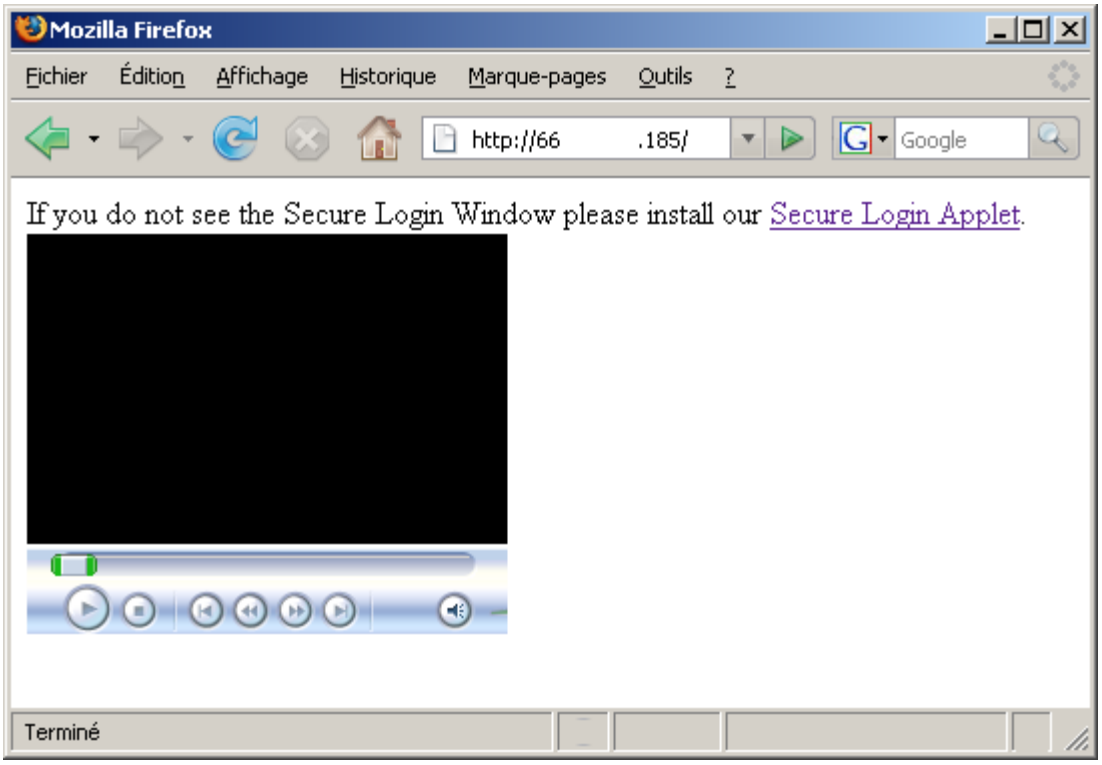
3.2.3 הפצה דרך בלוגים

Storm היה גם אחד הסוסים הראשונים שהפיץ עצמו באמצעות שימוש בבלוגים. מפיצי הסוס עמלו על הקמת מספר לא מבוטל של בלוגים פעילים ותמימים למראה, בעיקר דרך שירות הבלוגים Google Blogspot. בדוגמה הנמצאת מטה, מפיצי הסוס הקימו בלוג פמיניסטי המתיימר לספק לנשים ברחבי העולם פלטפורמה להתבטא על כל נושא בעולם. בין שאר הפוסטים האינפורמטיביים נשתלו לינקים זדוניים.



כאשר הגולש מקליק על הקישור, הוא מופנה לאתר ומתבקש להוריד ולהתקין תכנה תמימה לכאורה (פקד ActiveX), על מנת שהאתר "יעלה כראוי". תכנה זו היא למעשה תכנה זדונית והיא השלב הראשון בהדבקתו של הקרבן.

FunnyPostcard.Com - Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 收藏夹 媒体
地址(D) http://76.112.[redacted]/
转到 链接
Its a howl!
FunnyPostCard
www.funnypostcard.com
Your download will start in 5 seconds.
If your download does not start, click here
©2000-2008 FunnyPostCard.com - All rights reserved.
http://76.112.[redacted]/postcard.exe
Internet


Mozilla Firefox
Fichier Édition Affichage Historique Marque-pages Outils ?
http://66 .185/
Google
If you do not see the Secure Login Window please install our Secure Login Applet.
Terminé

3.3 אופן פעילות ויכולות שונות

1.3.3 כללי

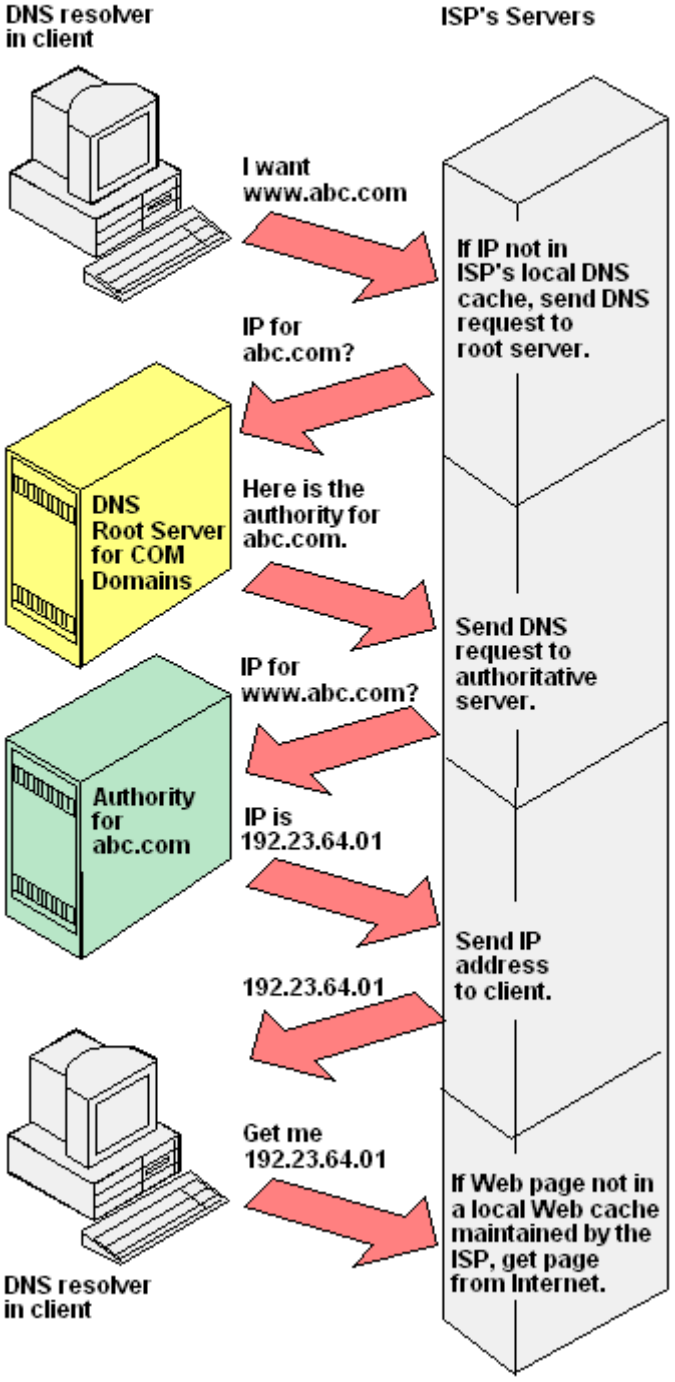
לפני הפירוט הטכני, יש לציין שקיימות עשרות ומאות וריאציות לסוס, ולכן שמות הקבצים המובאים מטה הם דוגמה בלבד.

2.3.3 גישה לאתר להורדת הקוד (רשתות xulF-tsaF)

כאמור, הקורבן אשר מתפתה להקליק על הקישור במייל שקיבל או באתר כלשהו, מופנה לאתר שבו נמצאת התכנה הזדונית. אם כך נשאלת השאלה, מדוע לא זיהו כתובות אלו והורידו אותם מהרשת. הדבר אינו כה פשוט.

כידוע, מחשבים ברשת האינטרנט מזוהים על פי כתובות ה-IP שלהם, ולא על פי שמם. כאשר אנו כותבים שם של אתר בשורת הכתובת (למשל http://www.gov.il), תחילה מתבצע תהליך של תרגום השם לכתובת המתאימה. הדבר נעשה באמצעות פניה לשרתי DNS בהיררכיות שונות.

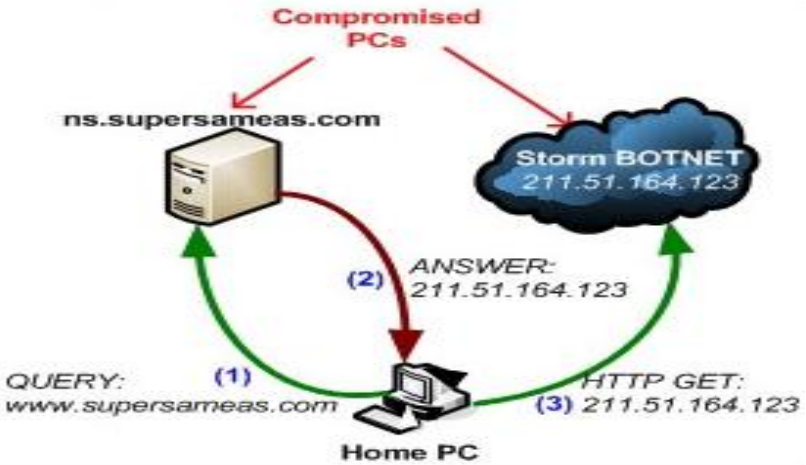
From Computer Desktop Encyclopedia
© 2005 The Computer Language Co. Inc.



על פי התפיסה המקובלת, שם של אתר מפנה לכתובת IP ספציפית. עם זאת, במקרים רבים אתרים מנצלים את המנגנון כך ששם אתר עשוי להיות מתורגם לכתובות IP שונות, על מנת לאזן עומסים בין מספר שרתים, לספק יתירות, או לספק למשתמש כתובת של שרת ש-"קרוב" אליו יותר ברשת.

את העיקרון הזה ניצלו מפתחי Storm על מנת לעבוד בשיטת Fast-Flux להתחמקות מגילוי. גולש שמקבל דואר אלקטרוני עם קישור, מקליק על הקישור שמפנה לאתר הזדוני של Storm worm ומופנה לכתובת IP אחת מבין רבות (מאות ואפילו אלפים) אפשריות. למעשה, אם אותו קורבן יכנס לקישור שוב ושוב כל שלוש דקות, סביר להניח שבכל פעם הוא יופנה למחשב אחר ברשת. דבר זה מקשה מאוד על מציאת המחשב המכיל את האתר הזדוני והשבתתו. כתובת ה-IP אליה מופנה הקורבן היא כתובת של אחד מתוך מחשבים רבים המשמשים כ-Proxy (מתווכים) בין הקורבן לבין "ספינת האם". מחשבים אלו הם לרוב מחשבים אישיים עליהם השתלט קוד זדוני ועכשיו מהווים בעצמם חלק מה-Botnet. כך, גם אם אחד או אפילו רבים ממחשבי התיווך יושבתו, עדיין יהיה ניתן לגשת אל האתר הזדוני דרך כל אחד מהמתווכים הנותרים.

מפעילי ה-Storm, רושמים שמות מתחם רבים ומחזיקים שרתי DNS רבים. למעשה, במקרים רבים שרתי ה-DNS עשויים להיות מוגנים בעצמם על-ידי רשת Fast-Flux, כך שגם כאשר אחד משמות המתחם נתפס ומושבת, אחרים עדיין פועלים. בזמן שעובר מרגע הפעלת שם המתחם ועד השבתתו, מחשבים רבים יודבקו בסוס. באתר TrustedSource ניתן לראות מעקב אחר שמות מתחם בהם נעשה שימוש לאחרונה ברשת.



1.2.3.3 התבסוסות במחשב המותקף

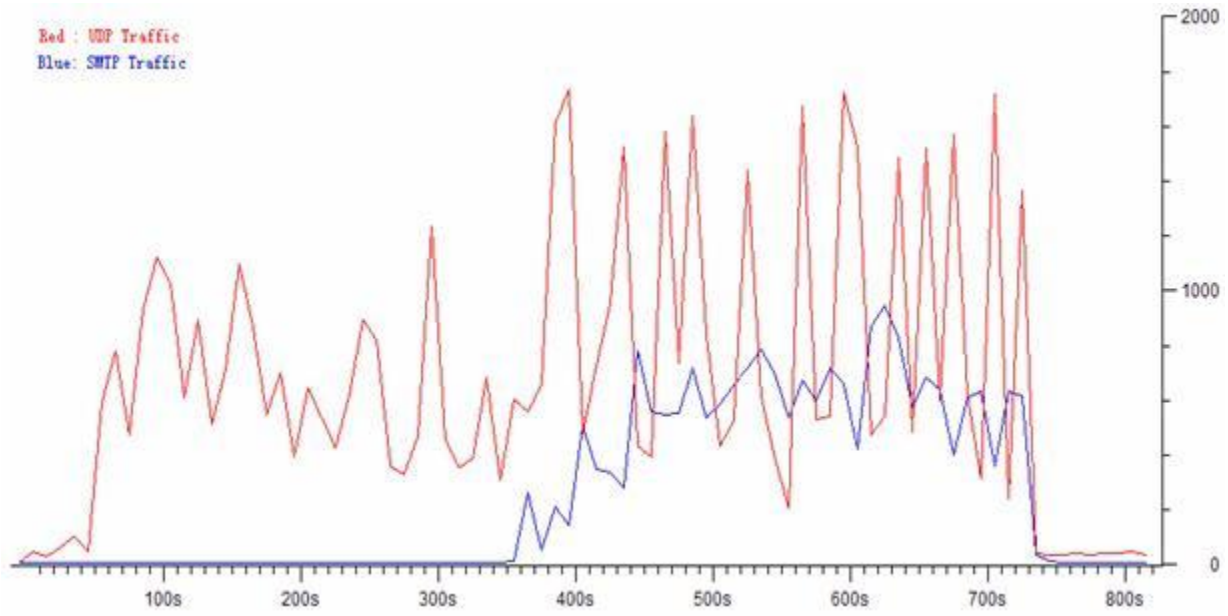
לאחר שהקורבן גולש לאתר עם הקוד הזדוני נוצר קובץ סמוי עם שם אקראי בתיקיה שבה הורץ הקוד. הסוס יוצר שני קבצים נוספים: ipeers.ini -wincom32.ini (כאמור, דוגמה בלבד, יכולים להיות שמות אחרים).

אחד הקבצים מכיל רשימה מוצפנת של לקוחות ומספרי הפורטים ברשת ה-P2P של הסוס. להלן קטע קוד מקובץ שכזה :

```
[counter]
Counter=0
[peers]
003964D3640550573F800125725481EF=5326859A123900
004982069E5DB75721B54CFF33A26170=5955FC93123900
00A1836AE91D076BC265F9735204714F=451AAE831EBF00
```

הקובץ השני מכיל רשימות שחורות (Black list). בשלב הזה הקובץ עדיין ריק מתוכן. הסוס סורק את רשימת הכתובות ומנסה להתחבר לרשת ה-P2P. בשלב הזה ניתן לראות חיבורי UDP רבים.

Topic / Item	Count	Rate	Percent
Port Type	77115	0.069655	
UDP	55561	0.050186	72.05%
TCP	21554	0.019469	27.95%



בתיקיית מערכת ההפעלה נוצר קובץ הסוס עצמו (wincom32.sys בדוגמה שלנו), וכן נוצר key ב-Registry, המפנה לקובץ הנוצר :

```
[HKLM\System\ControlSet001\Services\wincom32]
@ = "%WinSysDir%\wincom32.sys"
```

לרכיבים המותקנים יש תכונות של Rootkit. בין שאר הדברים, מאפיין זה מאפשר לסוס להסתיר את ה-Registry Key שנוצר, וכן להחביא את התהליכים (Processes) אשר הסוס מריץ.

על מנת לבצע פעילות זדונית על המחשב המותקף ללא זיהוי, הסוס מנסה לאתר תוכנות הגנה באמצעות בדיקת רשימת התהליכים (Processes) הרצים במחשב. אם הוא נתקל בתהליכים שמכילים רצף של אותיות המעיד על תוכנת אנטי-וירוס כגון: anti, avg, nod32, mcafee, firewall ורבים אחרים הוא הורג את התהליך.

2.2.3.3 קבלת פקודות

לאחר שהמחשב הקורבן נגוע, הסוס יכול להמשיך בתהליך של קבלת פקודות, ביצוע התקפות וקבלת עדכונים. את הפקודות והעדכונים מקבל ה-Storm דרך רשת ה-P2P שלו. מהמחשבים ברשת זו היא מקבלת, בצורה מוצפנת, כתובות URL מהן ניתן להוריד עוד רכיבים הנחוצים לה.

רכיבים אלו נמצאים, בדרך כלל, בקבצים הנושאים את השמות game0.exe, game1.exe…. game5.exe, כאשר לכל רכיב תפקיד משלו:

- game0.exe – פתיחת Backdoor והורדת קבצים.
- game1.exe - SMTP relay – שליחת דוא"ל.
- game2.exe - כלי לגניבת כתובות דוא"ל.
- game3.exe - כלי להפצת התולעת בדוא"ל.
- game4.exe - כלי לביצוע התקפות DDos.
- game5.exe – עדכון גרסה.

4.3 למה P2P?

באופן מסורתי השליטה (Command & Control – C&C) ברשתות Botnet נעשית על ידי שרת מרכזי שנותן הוראות לבוטים באמצעות פרוטוקול Client/Server כמו IRC או HTTP. לפרוטוקולים מסוג זה יש שני חסרונות משמעותיים (מבחינת מחזיק השליטה, כמובן):

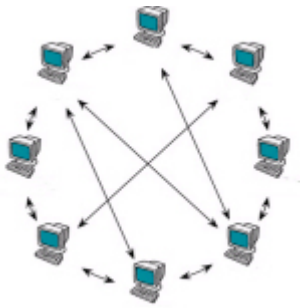
1. כל מחשב נגוע חייב להחזיק מידע לגבי השרת על-מנת שיוכל לתקשר עמו. לכן ניתן בקלות יחסית להתחקות אחר מקור הפקודות ולהגיע אל השרת.

2. אם מנתקים את השרת או פוגעים בו, השליט מאבד שליטה על המחשבים הנגועים.

כדי לפתור את הבעיות הללו, יצרו כותבי Storm רשת Botnet בה השליטה מבוססת על רשת P2P. בניגוד לפרוטוקולים המוזכרים מעלה, אין Client או Server, אלא כל הישויות שוות. ה-Storm Botnet היא רשת P2P, אשר עושה שימוש בשיטת Publish/Subscribe, שבה כל צומת ברשת יכול לפרסם מידע (Publish) לכל שאר הצמתים וכל צומת יכול להירשם (Subscribe) ולשמור פרטי מידע שצמתים אחרים מפרסמים. פרוטוקול ה-P2P עליו מתבסס ה-Storm Worm הוא פרוטוקול בשם Overnet, ששימש בעבר לרשת שיתוף הקבצים eDonkey2000 לפני שנסגרה. באותה רשת שיתוף קבצים, כאשר משתמש היה מעוניין למצוא קובץ, התוכנה בה השתמש הייתה מחשבת ערך MD4 (פונקציית HASH) של הקובץ שחיפש, ושולח את הערך המחושב כשאילתה ("למי יש קובץ המתאים לה-Hash הזה?"). כתשובה היה מקבל מצביע למיקומו של הקובץ.

מפתחי Storm worm לקחו את השיטה הזו, והפכו אותה לרשת שליטה ובקרה אנונימית. כאשר אחד מהסוס מחפש קובץ כלשהו, הערך שנשלח כשאילתה לא היה Hash של שם הקובץ, אלא ערך שנוצר על ידי ערבול התאריך הנוכחי ומספר אקראי בין 0 ל-31 (או בגרסאות מסוימות אחד מבין 32 מחרוזות טקסט אפשריות). מפעיל הרשת, שיודע מראש מה טווח הערכים שיחושבו בכל יום, יכול "לשתול" הוראות ברשת על-ידי ביצוע publish הממפה את ערכי ה-hash לכתובות URL המכילות קבצים זדוניים להורדה.

ברשתות שיתוף קבצים סטנדרטיות, תשובת השאילתה מצביעה למקור (מי שפרסם את הקובץ ומחזיק אותו). לעומת זאת, ב-Storm worm התשובה היא למעשה URL המצביע לאתר זדוני, כך שלא ניתן להתחקות אחרי הגורם שביצע את הקישור בין הבקשה לכתובת.



5.3 היסטוריה וסטטיסטיקות

1.5.3 כללי

בינואר 2007 ה-Storm Worm התחיל את דרכו המסחרית על ידי הפצת מיילים עם הנושאים הקשורים לסופה שהשתוללה באירופה. מרגע זה ועד יוני 2008 נרשמו התפרצויות דואר רבות. ההפצה הגדולה ביותר הייתה בספטמבר 2007, כאשר נשלחו כ1.2 מיליארד מכתבים המכילים את Storm. חוקרים מעריכים כי בשיא פעילותה רשת תפוצת המיילים של היוותה כ-20% מדואר הזבל באינטרנט ו-8% מכלל הקוד הזדוני על גבי מערכות Windows.

בחודש אוקטובר 2007 הודיעה חברת Microsoft כי היא מכריזה על Storm כיעד עיקרי, ומצהירה כי היא שיפרה את יכולות תוכנת ההגנה שלה – Malicious Software Removal Tool – כך שיתמקדו בניקוי הסוס. על פי טענות החברה, בחודש הראשון לפעולתה של הגרסה החדשה של תוכנה זו היא ניקתה יותר מרבע מליון מחשבים נגועים. בתקופה זו גם חברות האבטחה האחרות בשוק מוסיפות יכולות זיהוי והסרה של הסוס. עד סוף שנת 2008 ירד כוחה של Storm לכ-1% מכלל תפוצת דואר הזבל, ובשנת 2009 מספר זה הפך לכמעט אפסי.

רשת Storm עוד לא מתה לחלוטין, אך בהחלט אינה מהווה את האיום אשר הייתה בשיא כוחה.

2.5.3 קמפייני ההפצה הגדולים

בטבלה מטה ניתן לראות את קמפייני ההתקפות הגדולות ונושאי דברי הדוא"ל אשר ליוו אותן. ניתן לראות כי הקמפיינים היו מתוזמנים היטב לצד אירועים וחגים מרכזיים בעולם.

Theme	Time of usage
Actuality events (news items)	December 2006 - May 2007
Electronic greeting cards	June - August 2007
Electronic postcards	1-Aug-07
VPN Connector	August 2007 (only one day)
Beta program	August 2007 (only one day)
Video	August - September 2007
Labor day	September 2007 (only one day)
Tor installation package	September 2007 (only one day)
NFL Season	1-Sep-07
Arcade game download	September - October 2007
Halloween	October - November 2007
Screen Saver	Christmas 2007
New Year Greetings	8-Jan-08
Valentine's Day	1-Feb-08
Electronic greeting cards	1-Mar-08
April Fools Day	1-Apr-08
Fake video codecs	April - May 2008
Fake reports of another Chinese earthquake and the consequent probable cancellation of the Olympics	June 2008

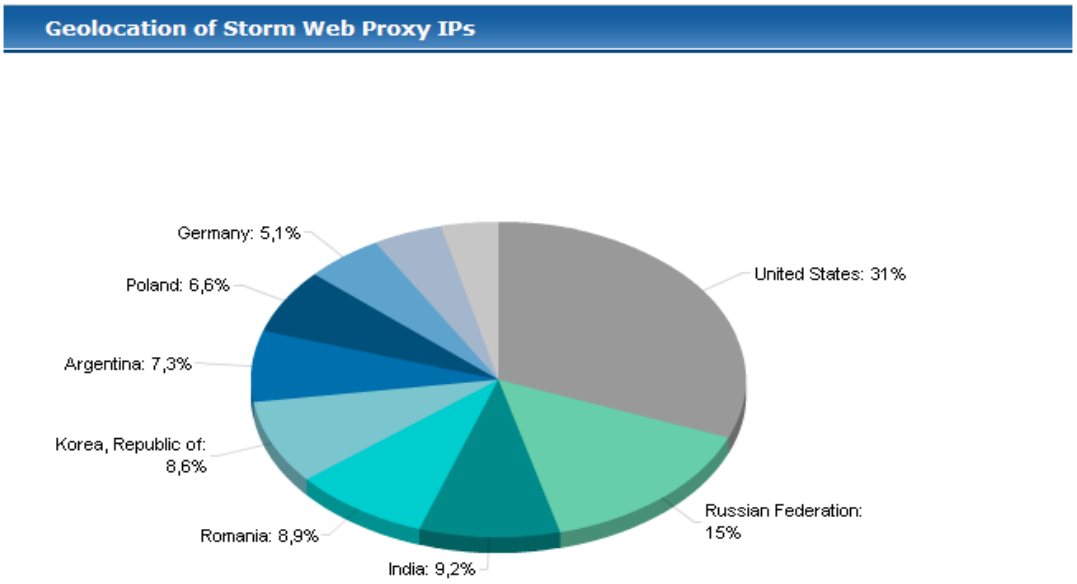
3.5.3 אירועים חריגים

לקראת סוף שנת 2007, לקוחות הבנק הבינלאומיBarclay קיבלו דואר אלקטרוני רשמי למראה מה-"בנק "ובו הודעה לפיה "הבנק מבצע בדיקה תקופתית שמטרתה צמצום מקרי ההונאה". כחלק מאותה בדיקה, התבקש הלקוח להקליק על קישור לאתר הבנק, המצורף בגוף ההודעה, ולבדוק את פרטי חשבונו. לקוח שאכן לחץ על הקישור והכניס את פרטיו, עשה זאת בעצם באתר מזויף http://www.i-barclays.com (במקום לאתר האמיתי www.barclays.com) וחשף אותם, בעצם, בפני התוקפים. לכאורה, אין מקרה זה שונה מעשרות אלפי דוגמאות Phishing שונות מאותה השנה. הסיבה לכך שמקרה זה התבלט היא שדבר הדואר נשלח על ידי Storm Worm, שנחשבת לרשת מקצועית מאוד, אך דבר הדואר עצמו יוצר באמצעות "ערכות Phising" מיושנות, דבר המצביע על עבודת חובבנים, שאינה אופיינית לארגון כמו RBN.

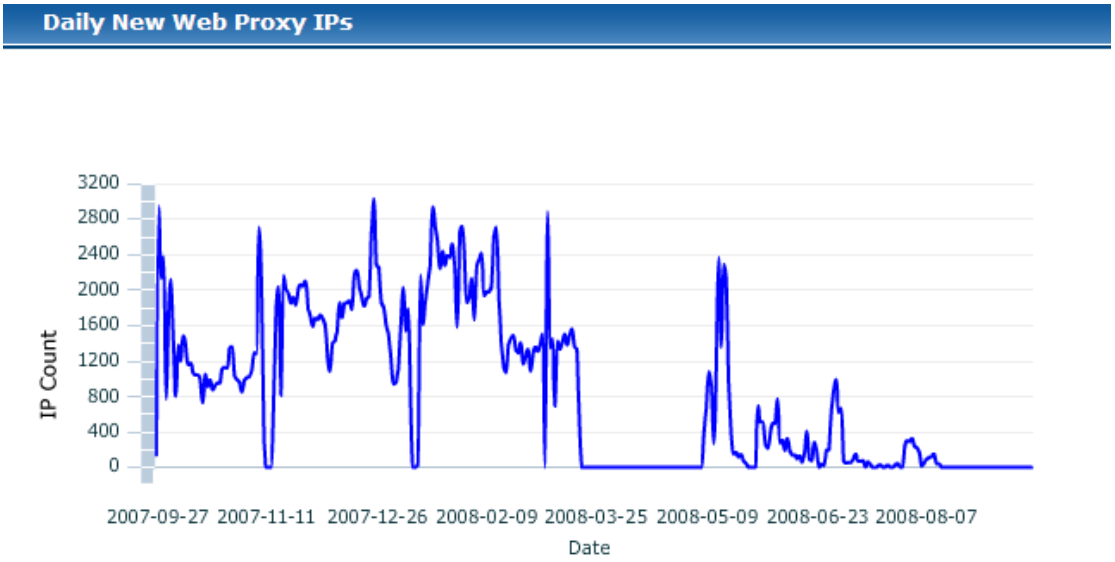
עובדה זו חיזקה את הסברה לפיה RBN השתמש ב-Botnet ככלי כלכלי, ומשכיר חלקים ממנה לכל המרבה במחיר. הייתה זו העדות הראשונה לפעילות מסוג זה, דבר שהועתק למספר רשתות Botnet מאוחרות יותר, ושוכללה מאוד עם הופעת Zeus.

4.5.3 תפוצת ה-Storm בעולם

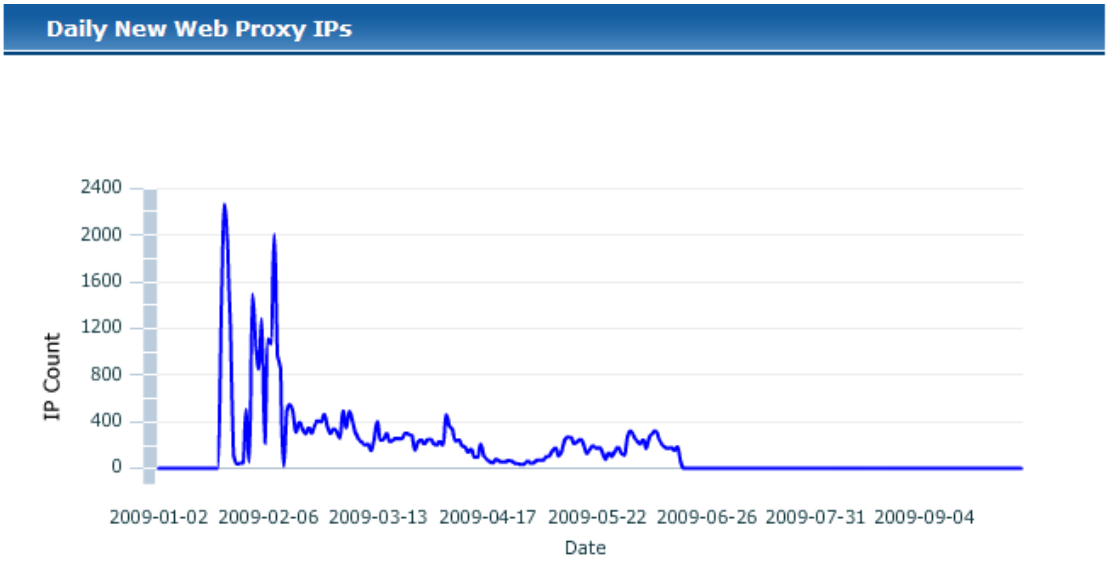
התפשטות על פי מדינות



פעילות הרשת בתקופות השיא



פעילות הרשת בשנת 2009



5.5.3 סטטיסטיקות תפוצה בממשלת ישראל

קיימת בעיה קונקרטית להתחקות אחר נפוצות ה-Storm במשרדי הממשלה המחוברים לרשת תהיל"ה. הבעיה, אם כי ניתן להסתכל עליה גם באופן חיובי, נובעת מצורת התקשורת של הסוס – אותה רשת P2P המתוארת מעלה.

מערכות ההגנה של תהיל"ה חוסמות תקשורת P2P כבר בשלב מאוד מוקדם. ברוב המוחלט של המקרים תקשורת מסוג זה נחסמת עוד במערכות ההגנה הממוקמות בצד הלקוח, ואפילו לא מגיעות אל מערכות ההגנה המרכזיות. במידה ותקשורת מסוג זה כן מגיעה אל מערכות ההגנה המרכזית, היא מזוהה כתקשורת P2P כללית, וקשה עד בלתי אפשרי להפריד בינה לבין כל ניסיון גישת P2P אחרת שנחסמת.

6.3 גילוי והסרה

כיום רוב תוכנות האנטי-וירוס הנפוצות כבר מזהות ברוב המוחלט של המקרים הדבקה של הסוס ויודעות להסירו. כאמור מעלה, חברת Microsoft השקיעו מאמצים נרחבים בשיפור תוכנת Malicious Software Removal Tool על מנת שתיאבק בסוס הספציפי הזה.

בנספח א' למסמך זה ניתן לראות רשימה (מפורטת אך חלקית) של השמות השונים אשר ניתנו לStorm על ידי חברות האבטחה השונות. ניתן לראות כי חברות אבטחה מסוימות נותנות מספר שמות שונים לסוס, דבר המלמד על כך שהם מפרידים בין זנים וגרסאות שונות שלו.

4.ביבליוגרפיה וקריאה נוספת

http://vil.nai.com/vil/Content/v_142621.htm

http://www.threatexpert.com/threats/email-worm-zhelatin.html

http://politech.wordpress.com/2007/09/03/zhelatin-worm-botnet

http://www.viruslist.com/en/viruses/encyclopedia?virusid=150767

http://www.f-secure.com/v-descs/email-worm_w32_zhelatin_cq.shtml

http://www.threatexpert.com/report.aspx?md5=db45bb16af23e14380e5fb3f3cb3d2dd

http://www.threatexpert.com/reports.aspx?page=10&find=Email-Worm.Zhelatin

http://en.wikipedia.org/wiki/Storm_Worm

http://en.wikipedia.org/wiki/Storm_botnet

http://webcourse.cs.technion.ac.il/236350/Spring2009/ho/WCFiles/StormWorm.pdf

http://www.threatexpert.com/threats/email-worm-zhelatin.html

www.iss.net/threats/W32.Worm.Nuwar.Gen.html

http://www.trustedsource.org/TS?do=threats&subdo=Storm_tracker

http://honeyblog.org/junkyard/paper/Storm-leet08.pdf

http://securitylabs.websense.com/content/Assets/Storm_Worm_Botnet_Analysis

http://www.f-seure.com/v-descs/small_dam.shtml

http://ezine.rusbiz.com/article/Are_You_Protected_from_Storm_Worm.html

http://ads.computer.org/portal/

http://www.icsiberkeley.edu/pubs/networking/2008-ccs-spamalytics.pdf

http://www.cyber-ta.org/pubs/StormWorm/SRITechnical-Report-10-01-Storm-Analysis.pdf

http://securitylabs.websense.com/content/Blogs/2822.aspx

http://www.wizcrafts.net/blogs/2007/08/email_threat_trojandownloader_Storm_worm_its.html

http://isc.sans.org/top10.html

http://securitylabs.websense.com/content/Blogs/2822.aspx#appendix

http://voices.washingtonpost.com/securityfix/2007/10/the_Storm_worm_maelstrom_or_te.html

5.נספחים

1.5 רשימת שמות של ה Storm worm

- Email-Worm.Win32.Zhelatin.my [Kaspersky Lab]
- Mal/DorfSys-A [Sophos]
- Trojan.Packed.13 [Symantec]
- Email-Worm.Win32.Zhelatin.kv [Kaspersky Lab]
- TrojanDownloader:Win32/Tibs [Microsoft]
- WORM_NUWAR.EN [Trend Micro]
- WORM_ZHELATI.AIR [Trend Micro]
- Win-Trojan/Rootkit.54016 [AhnLab]
- Downloader-BAI.gen.d [McAfee]
- Email-Worm.Win32.Zhelatin.ab [Kaspersky Lab]
- Email-Worm.Win32.Zhelatin.nc [Kaspersky Lab]
- TROJ_MULP.I [Trend Micro]
- W32.Mixor.Q@mm [Symantec]
- Email-Worm.Win32.Zhelatin.it [Kaspersky Lab]
- Possible_Nucrp-6 [Trend Micro]
- Trojan Horse [Symantec]
- Backdoor:WinNT/Nuwar.C!sys [Microsoft]
- Mal/Generic-A [Sophos]
- Win-Trojan/Zhelatin.7968 [AhnLab]
- Email-Worm.Win32.Zhelatin.pd [Kaspersky Lab]
- Trojan.Mespam [Symantec]
- WORM_NUCRYPT.GEN [Trend Micro]
- Downloader-ASH.gen.b [McAfee]
- Email-Worm.Win32.Zhelatin.afj [Kaspersky Lab]
- Trojan.Peacomm [Symantec]
- Rootkit.QQHelp.Gen.6 [PC Tools]
- Email-Worm.Win32.Zhelatin.d [Kaspersky Lab]
- BKDR_AGENT.AVJZ [Trend Micro]
- W32/Nuwar@MM [McAfee]
- Backdoor:WinNT/Nuwar.A!sys [Microsoft]
- Win-Trojan/Rootkit.15328 [AhnLab]
- TROJ_TIBS.AP [Trend Micro]
- Email-Worm.Win32.Zhelatin.a [Ikarus]
- WORM_NUCRP.GEN [Trend Micro]
- Tibs-Packed [McAfee]
- RTKT_NUWAR.UY [Trend Micro]
- Email-Worm.Zhelatin!sd5 [PC Tools]
- Downloader-BAI.sys [McAfee]
- Packed.Win32.Tibs.ab [Kaspersky Lab]
- Email-Worm.Win32.Zhelatin.vd [Kaspersky Lab]
- Email-Worm.Win32.Zhelatin.qa [Kaspersky Lab]
- Trojan.Win32.KillProc.s [Kaspersky Lab]
- WORM_ZHELATIN.EG [Trend Micro]
- Troj/Dorf-M [Sophos]
- Trojan.Peacomm.B [Symantec]
- TROJ_SMALL.EDW [Trend Micro]
- TROJ_TIBS.ART [Trend Micro]
- Packed.Win32.Tibs.ap [Kaspersky Lab]
- Generic.dx [McAfee]
- TROJ_AGENT.ZLH [Trend Micro]
- Bloodhound.Unknown [Symantec]
- TROJ_PEACOMM.BM [Trend Micro]
- W32/Nuwar.sys [McAfee]
- TROJ_PEACOMM.BQ [Trend Micro]
- Hacktool.Rootkit [Symantec]
- NTRootKit-J [McAfee]
- RTKT_AGENT.EBK [Trend Micro]
- Trojan.Peacomm.D [Symantec]
- Hacktool.Rootkit!sd6 [PC Tools]
- Troj/Tibs-TX [Sophos]
- Email-Worm.Win32.Zhelatin.vl [Kaspersky Lab]
- Email-Worm.Win32.Zhelatin.sd [Kaspersky Lab]
- VirTool:WinNT/Tibs.gen!A [Microsoft]
- TrojanDownloader:Win32/Vxidl [Microsoft]
- Troj/Tibs-TJ [Sophos]
- Packed.Win32.Tibs [Ikarus]
- Downloader-BAI.sys.gen.a [McAfee]
- Backdoor:WinNT/Nuwar.B!sys [Microsoft]
- Email-Worm.Win32.Zhelatin.vl [Ikarus]
- Troj/Dorf-Fam [Sophos]
- Win-Trojan/Tibs.7712 [AhnLab]
- Backdoor.WinNT.Nuwar.E [Ikarus]
- Troj/Dorf-AP [Sophos]
- Win-Trojan/Zhelatin.129792 [AhnLab]

- Possible_Nucrp-4 [Trend Micro]
- Possible_Nucrp-5 [Trend Micro]
- TROJ_TIBS.AB [Trend Micro]
- Trojan:Win32/Tibs.GH [Microsoft]
- Trojan-Downloader.Win32.Tibs.aam [Kaspersky Lab]
- Trojan-Dropper.Agent [Ikarus]
- W32/Zhelatin.gen [McAfee]
- Win-Trojan/Rootkit.46208 [AhnLab]
- W32/Dref-AB [Sophos]
- Win32/Zhelatin.worm.37747.G [AhnLab]
- Cryp_Xed-3 [Trend Micro]
- Downloader [Symantec]
- Email-Worm.Win32.Zhelatin.he [Kaspersky Lab]
- Email-Worm.Win32.Zhelatin.ki [Kaspersky Lab]
- Email-Worm.Win32.Zhelatin.nd [Kaspersky Lab]
- Mal/Dorf-E, Mal/TibsPk-D, Mal/Dorf-D, Mal/TibsPak [Sophos]
- Packed.Win32.Tibs.bl [Kaspersky Lab]
- Email-Worm.Win32.Zhelatin.al [Ikarus]
- Email-Worm.Win32.Zhelatin.al [Kaspersky Lab]
- Mal/Cimuz-D [Sophos]
- Spam-Mespam [McAfee]
- Trojan:Win32/Mespam [Microsoft]
- Trojan-Dropper.Win32.Agent.bbv [Kaspersky Lab]
- Email-Worm.Win32.Zhelatin.hc [Kaspersky Lab]
- Trojan:Win32/Nuwar [Microsoft]
- Trojan:Win32/Tibs.CG [Microsoft]