www.gov.il
ממשל זמין – פרויקט תהיל"ה

דו"ח סיכום מחקר

רשת BOT- NET

-

MEGA – D / OZDOK

ממשל זמין – פרויקט תהיל"ה

מאפייני מסמך

מחבר	פולינה חזנוב, יול בהט
מספר גרסה	1.0
סטטוס	סופית
תאריך הוצאה	דצמבר 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	14/12/09	פולינה חזנוב, יול בהט	גרסה סופית

הפצה

מ. גרסה	נמענים
1.0	רשימת תפוצה SI

תוכן עניינים

1. כללי 4
1.1 רקע 4
1.2 קצת על Mega-D 4
2. רשתות Bot Net באופן כללי 4
3. רשת Mega-D בפירוט 5
3.1 כללי 5
3.2 דרכי הפצה 5
3.3 אופן פעילות ויכולות שונות 8
3.3.1 התבססות במחשב המותקף 8
3.3.1 שליחת דואר זבל 9
3.3.2 מנגנוני ההגנה של Ozdok 9
3.3.3 Alternate Data Stream 14
3.4 היסטוריה וסטטיסטיקות 15
3.4.1 התחלת הפעילות 15
3.4.2 התפשטות Mega-D בעולם 18
3.4.3 הנפילה הגדולה הראשונה, וההתאוששות הזמנית 19
3.4.4 הפלת Mega-D על ידי חברת FireEye 21
3.4.5 סיכום ביניים 23
4. ביבליוגרפיה 24

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 קצת על Mega-D

רשת Mega-D הינה רשת זומבים, אשר בשיא גודלה והשפעתה הייתה אחראית על כ-30% מתעבורת דואר הזבל באינטרנט. במהלך חודש אוקטובר 2009 קבוצת חוקרים הצליחה להשתלט ולהפיל את הרשת. מסמך זה יסקור את ההיסטוריה של הרשת מתחילת פעולה, דרך ניתוח התשתיות שלה ועד להפלתה הסופית.

רשתות Bot Net באופן כללי

רשתות Bot (Bot Nets) הן רשתות של מחשבי זומבי (Bots), הנשלטים מרחוק באמצעות מנגנונים שונים, לרוב ללא ידיעתו של בעל המחשב. אף שרוב הזמן המחשב הנשלט מתפקד כרגיל, ניתן להורות לו מרחוק לבצע פעולה בניגוד לרצון בעליו. נותני הפקודות, הנקראים Bot Master או Bot Herder, מבצעים את השליטה משרתי שליטה ובקרה (Command and Control Center או בקיצור C&C). כאשר תוקף מסוים השיג שליטה שכזו במספר רב של מחשבים (כלומר, Bot Net), הוא יכול לבצע את הפעולות הזדוניות בהיקף רחב מאוד, ועל ידי כך להגביר את הנזק הפוטנציאלי.

רשת Mega-D בפירוט

1.3 כללי

רשת Mega-D היא אחת מרשתות ה-Botnet המפורסמות והפעילות שידע האינטרנט. הרשת החלה את דרכה בספטמבר 2007, ופעלה על ידי הפצת סוס טרויאני בשם Ozdok. ייחודם העיקרי של הסוס והרשת הוא שבניגוד לסוסים טרויאנים אחרים (ראה ערך Zeus), הם מעולם לא נוצלו למטרות זדונית כגון תקיפה מחשבים. ייעודם העיקרי והיחידי של הסוס והרשת היה להוות את רשת הפצת הספאם הגדולה בעולם – מטרה שהם אכן עמדו בה.

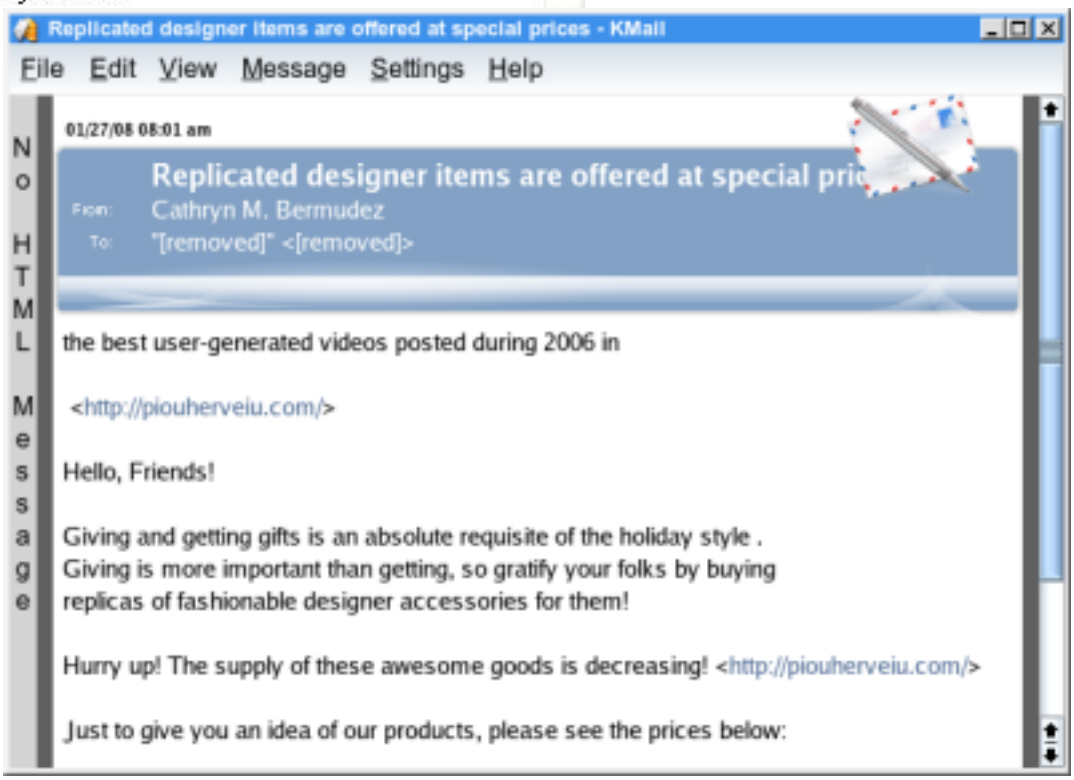
מהר מאוד הרשת מתחילת פעולתה הרשת טיפסה לעשירייה הגבוהה של מפיצי דואר הזבל, ואף הגיעה בשיאה ל 32% מכל דואר הזבל העובר העולם. גודל התעבורה של דואר זבל המופץ על ידי Mega-D אף גבר על גודל התעבורה של ה-Storm Botnet (ראה מסמך נפרד) שהגיע בשיאו ל 21%. נתון זה מרשים עוד יותר לאור העובדה שרשת Mega-D כללה בשיאה כ-35,000 מחשבים – מספר הקטן פי 3 מגודל רשת Storm, וגם זאת על פי הערכות חסר. שמה של הרשת ניתן לה בעקבות הקישור שנעשה בינה לבין אחד המוצרים שהיא עזרה לפרסם – מוצר להגברות האון הגברי.

2.3 דרכי הפצה

כאמור, Mega-D הינה רשת המרחיבה עצמה בצורה עצמאית. בין עשרות ומאות אלפי דברי הדואר שנשלחו על גבי תשתיות הרשת ביום, חלק מאלו כללו גם קבצי הדבקה של הסוס Ozdok. לרוב, נושאי המיילים הם מוצרים רפואיים, צמחי מרפא, תכשירי מין ומוצרים דומים. בוני ה Mega-D השתמשו גם בהנדסה חברתית על מנת לגרום לקוראי המייל להיכנס לקישור, כאשר שלחו מיילים לקהלי יעד מכוונים ידיעות על מותו של שחקן אוסטרלי מפורסם. יוצרי ה Mega-D גם משתמשים ברשתות חברתיות כגון פייסבוק; הם יוצרים אתרי Phishingייעודיים, ושולחים מייל הנראה כמו הזמנה של צפייה בפרטים של אדם הרשום ברשת החברתית. לאחר כניסת הקורבן לאתר הוא מתבקש לעדכן את ה Flash Player שלו, ולמעשה מריץ את הקוד של הסוס Ozdok. האתרים הזדוניים שהמפיצים בנו מכיל תוכן על מנת לשמור על ההטעיה או למכור מוצר כלשהוא.

VPXL - Penis Enlargement Made Easy - Microsoft Internet Explorer
expressherbals
no 1 penis enlargement supplement worldwide!
AS SEEN ON TV
Gain An Amazing 1 to 3 full Inches!
"VPXL Has Worked For THOUSANDS of Clients." - Dr J.B. Dowd
Home | Faq | Testimonials | Order | Contact Us | Privacy Policy
Order Exp
Never lose hope to recover! - Central European (ISO)
File Edit View Tools Message Help
From: Mari Barnhart
Date: Tuesday, 26 February 2008 7:56 a.m.
To: -
Subject: Never lose hope to recover!
Many things can spoil the joy of your life.
Some of them are in particular widespread, such as:
* Pen*!s Growth medication
* erectyle and other s'e_xual dysfunctions
* obesity
* depressive disorders
* sleep disorders
* allergy
If you suffer from any of the above mentioned diseases, you are welcome to check our site.
We offer high-quality, U.S. licensed medicines at substantially reduced prices!
Clear off your sickness today!

Facebook Password Reset Confirmation. Help ...
File Edit View Tools Message Help
Reply Reply All Forward Print Delete Previous
From: Facebook Privacy Policy
Date: Monday, November 02, 2009 2:13 PM
To: [redacted]
Subject: Facebook Password Reset Confirmation. Help Centre.
Attach: Facebook_Password_ab525.zip (23.0 KB)
Hey bpb ,
Because of the measures taken to provide safety to our clients, your password has been changed.
You can find your new password in attached document.
Thanks,
Facebook Security Systems.


Replicated designer items are offered at special prices - KMail
File Edit View Message Settings Help
No HTML Message
01/27/08 08:01 am
Replicated designer items are offered at special pri
From: Cathryn M. Bermudez
To: "[removed]" <[removed]>
the best user-generated videos posted during 2006 in
<http://piouherveiu.com/>
Hello, Friends!
Giving and getting gifts is an absolute requisite of the holiday style .
Giving is more important than getting, so gratify your folks by buying
replicas of fashionable designer accessories for them!
Hurry up! The supply of these awesome goods is decreasing! <http://piouherveiu.com/>
Just to give you an idea of our products, please see the prices below:

3.3 אופן פעילות ויכולות שונות

1.3.3 התבססות במחשב המותקף

קובץ ההרצה של הסוס Ozdok נקרא ברוב המקרים באחד מהשמות הבאים: icf.exe, icf32.exe, cacglivin.exe, mm32nov.exe ו- guyymgvl.exe. לאחר ההרצה הסוס מחביא שני קבצים בשם:

%System%\svchost.exe:exe.exe

%Windir%\system32:svchost.exe

הקבצים מוחבאים בשיטת Alternate Data Stream (ADS), עליה נפרט בהמשך (ראה סעיף 3.3.3).

כמו כן הסוס מוסיף ערכי Registry :

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile\AuthorizedApplications\List\"%System%\svchost.exe" = "%System%\svchost.exe:*:Enabled:svchost"

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List\"%System%\svchost.exe" = "%System%\svchost.exe:*:Enabled:svchost"

על ידי שינוי זה הוא משנה את ההגדרות של חומת האש של מערכת ההפעלה כך שהתקשורת של הקוד הזדוני לא תחסם בו.

לאחר מכן הוא מוסיף Service בשם icf על מנת לוודא שבכל עליה של מחשב הקוד הזדוני שלו ירוץ.

לבסוף, הסוס יוצר תקשורת בפורט 80 עם שרתים מוגדרים מראש לשם קבלה ומסירה של נתונים. המידע לא עובר בפרוטוקול HTTP אלא בפרוטוקול מוצפן לא סטנדרטי. נכון להיום ידועים כ-45 שרתי שליטה ובקרה.

1.3.3 שליחת דואר זבל

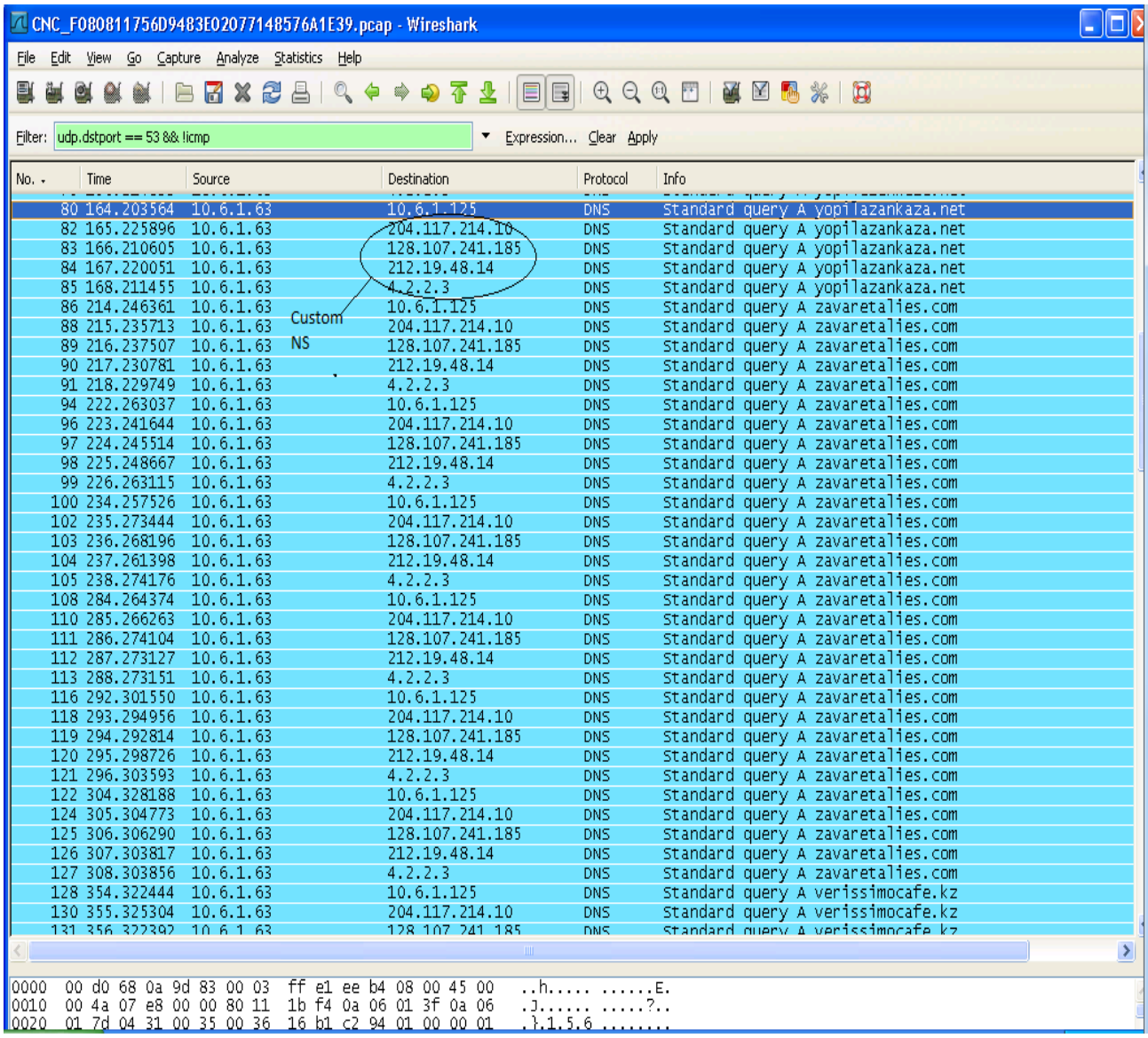
ברגע שהמחשב הנגוע מצליח להתקשר עם אחד משרתי ה-C&C, הוא שולח מייל בדיקה דרך פורט 25 לאותו השרת. אם המייל עובר בהצלחה, הסוס מוריד תבנית של מייל בערוץ המאובטח שיצר, ומתחיל לשלוח דואר זבל לרשימה של נמענים, המושגת גם היא מהשרת. כל מחשב נגוע שולח **כ-15,000** מיילים בשעה.

2.3.3 מנגנוני ההגנה של Ozdok

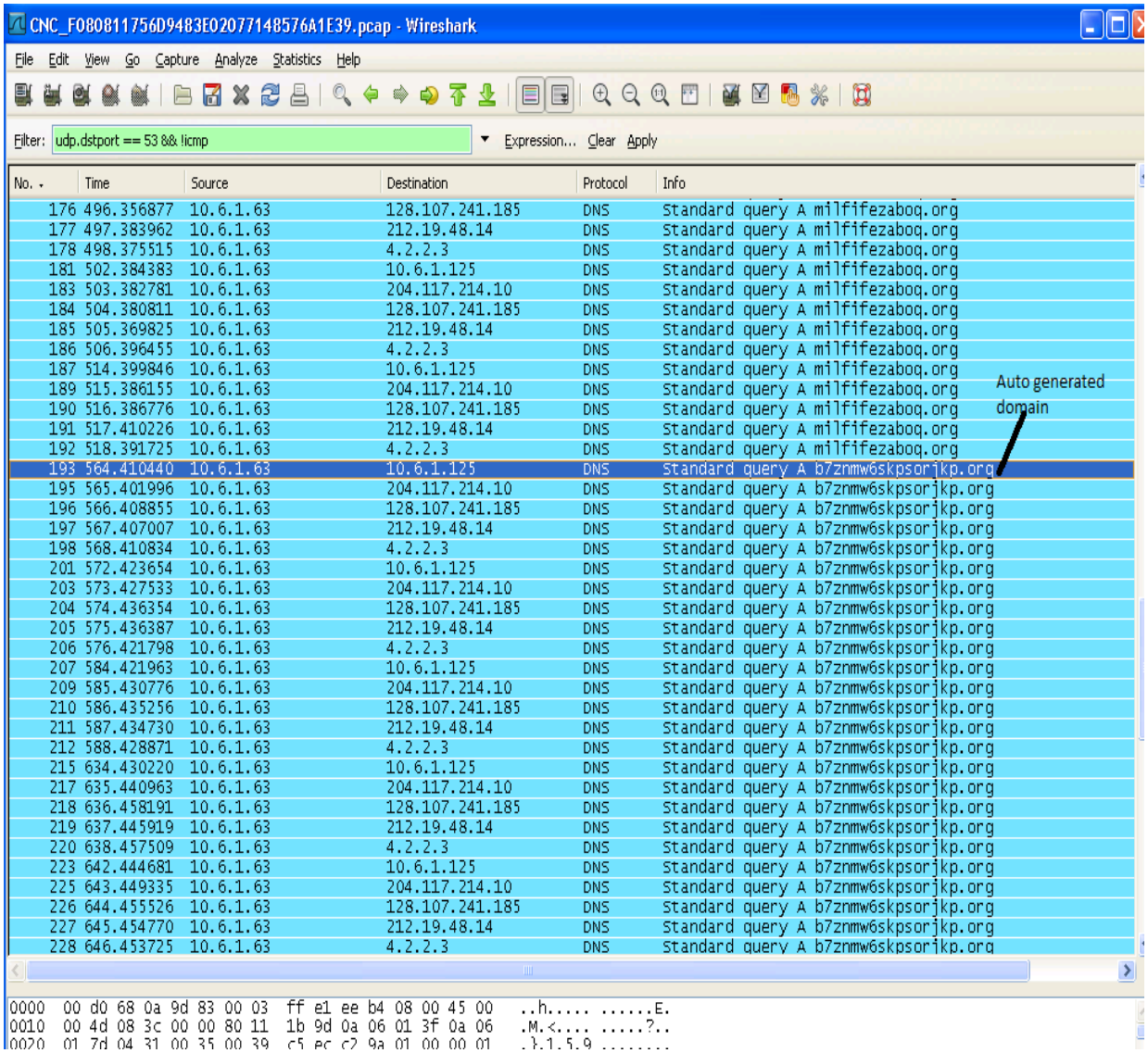
לאחר ההפלה של רשת McColo, שתתואר בהמשך, בוני הרשת לא סמכו על תת רשת אחת לכן הם פיזרו את שרתי שליטה ובקרה שלהם ברשתות שונות ופיתחו מנגנון תקשורת עם מספר מדרגות הגנה.

1. בתוך הקוד הזדוני נמצאת רשימה Hard Coded של שרתי שליטה ובקרה; אם תקשורת עם אחד מהם נכשלת הם עוברים לשרת הבא.
2. בתוך הקוד נמצאת גם רשימת שרתי DNS ייעודיים שיכולים לחברם לשרתי שליטה ובקרה. אם הסוס לא מצליח להתחבר לשום שרת שליטה ובקרה מהרשימה, הוא בודק את כתובת של אתר C&C דרך אחד שרתי ה - DNS הנמצא ברשימה ואם גם הDNS הייעודי לא מצליח למצוא את הכתובות של שרתי השליטה, הסוס עובר לשרת DNS נוסף מהרשימה.
3. אם כל אלו כושלים, כל יום הסוס יכול להגריל כתובת אקראית המבוססת על תאריך וזמן, ואם בוני הסוס ירצו להחזיר את השליטה לידיהם, הם פשוט צריכים לרשום את הדומיין החדש.
4. מנגנון נוסף נקרא BotnetWeb – כלומר, הסוס פותח דלת לתוכנות זדוניות נוספות, ובמקרה שיצליחו להתגבר על כל המנגנוני ההגנה של הסוס, בוני הסוס יצליחו להחדיר עדכון או שינוי של Ozdok דרך תוכנה זדונית אחרת.

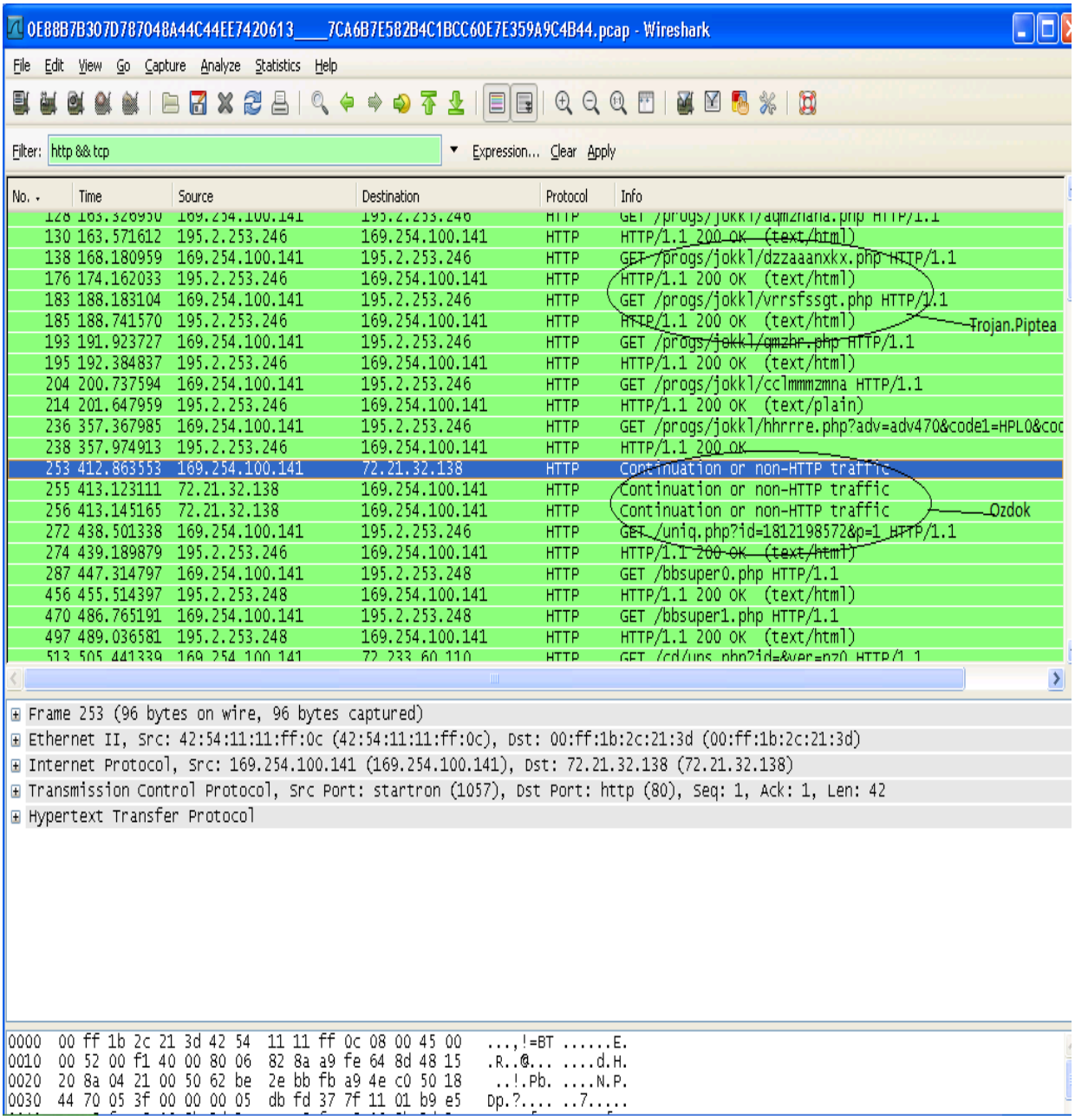
בתמונה הבאה ניתן לראות בקשות DNS סטנדרטיות לשרתי שליטה ובקרה של הסוס.



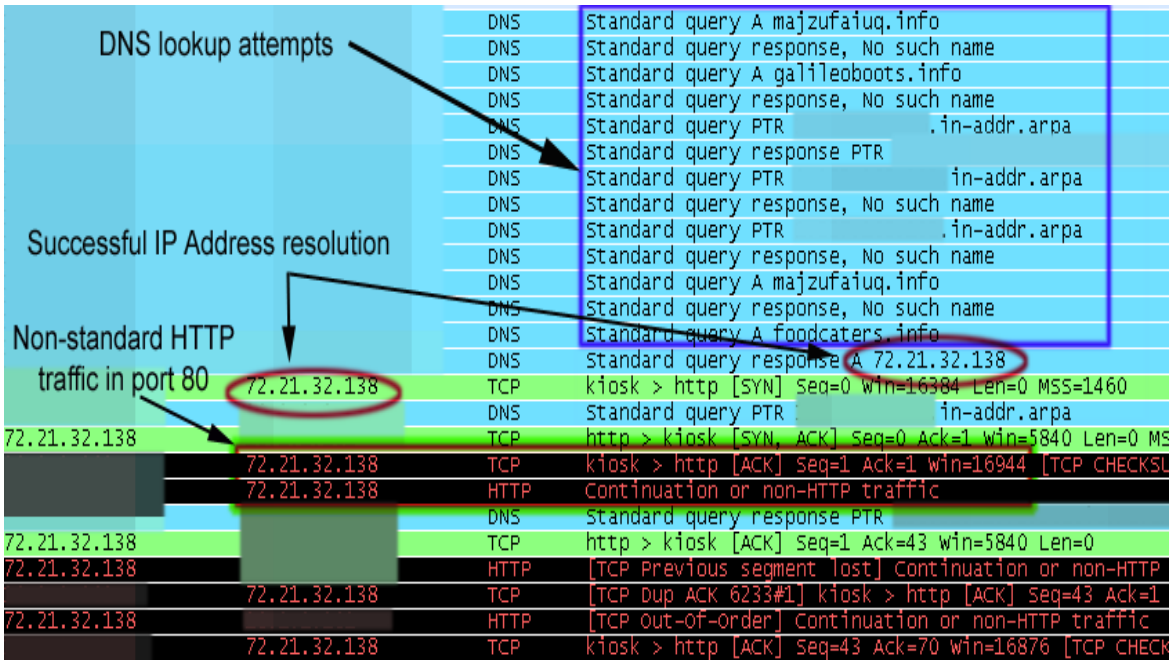
כאן ניתן לראות ניסיון לבקשת DNS לדומיין עם כתובת מוגרלת



בתמונה הבאה ניתן לראות שישנה גם תקשורת של סוסים אחרים במחשב הנגוע.



בתמונה זו ניתן לראות גם בדיקה של כתובת שרת שליטה ובקרה וגם תקשורת עם השרת



Alternate Data Stream 3.3.3

כאשר מדובר במערכת הקבצים NTFS, שהיא מערכת הקבצים המרכזית במערכות Windows, מערכת ההפעלה "יודעת" כיצד להריץ קבצים על פי הסיומת של הקובץ. כך למשל הוגדר כי קבצי exe הם קבצי הפעלה, קבצי gif הם קבצי תמונה וכו'.

במחשבי Macintosh, או לפחות מחשבים המבוססים על מערכת הקבצים הישנה של החברה Macintosh Hierarchal File System (HFS), מידע זה מחולק לשניים. בקצרה, בשיטה זו המידע עצמו נשמר באזור אחד בקובץ הנקרא Data Fork בעוד ה-Meta-Data נשמר באזור הנקרא Resource Fork.

בכדי שמחשבי Macintosh ו-Windows יוכלו "לתקשר" ביניהם, הוסיפה חברת Microsoft למערכת NTFS את האפשרות להגדיר עבור קבצים Alternate Data Stream, שתפקידו הוא זהה לחלוטין לזה של ה-Resource Fork. אפשרות זו היא לא אפשרות ידועה במיוחד בקרב קהיליית המפתחים והמשתמשים של Windows, אך היא בהחלט ידועה בקרב קהיליית התוקפים הזדוניים.

האיום המיידי של השימוש הזדוני בשיטה זו היא החבאת קבצים. צפייה פשוטה בספרייה בה נמצא קובץ עם ADS לא תראה את הקובץ. למעשה, בשביל לגלות קיום של קבצים אלו ללא ידיעה מוקדמת יש צורך בתוכנה מיוחדת (לדוגמה - Lads).

לשם ההדגמה, ניצור קובץ עם ADS. יש לוודא כי הפקודות לא מורצות בספרייה מרכזית, כי עלולות להיות לכך השלכות. באופן כללי, יש לנקוט משנה זהירות בהרצת פקודות אלו, והן לא מומלצות לאנשים ללא רקע טכני מתאים.

בהדגמה זו נניח כי קיימת ספריה בשם test, ובה אנו מריצים את הפקודות.

1) **C:\test>echo "ADS" > test.txt:hidden.txt**

על ידי הרצת פקודה זו יצרנו למעשה שני קבצים. הראשון, Test.txt, שהוא קובץ ריק לחלוטין. השני, קובץ בשם hidden.txt, שמכיל את הטקסט ADS. אם נסתכל על הספרייה דרך ה-Explorer של Windows, או לחילופין נעשה dir, לא נראה את הקובץ hidden.txt. למעשה, לא נראה אותו אלא אם כן נעשה שימוש בתוכנה מתאימה, כמתואר למעלה.

2) **C:\test>lads**

```
LADS - Freeware version 3.21
(C) Copyright 1998-2003 Frank Heyne Software (http://www.heysoft.de)
This program lists files with alternate data streams (ADS)
Use LADS on your own risk!

Scanning directory C:\test\

      size  ADS in file
----------  ---------------------------------
         8  C:\test\test.txt:hidden.txt

         8 bytes in 1 ADS listed
```

הקובץ בהחלט שם, ואפילו ניתן לגשת אליו:

3) **C:\test>notepad test.txt:hidden.txt**

בכדי למחוק את הקובץ המוחבא, יש למחוק את הקובץ המשמש כנקודת הקישור שלו:

4) **C:\test>del test.txt**

מצב חמור יותר הוא אם הקובץ המוחבא נוצר כאשר נקודת הקישור שלו היא ספריה, ולא קובץ:

5) **C:\test> echo test> :hidden.txt**

כעת, אם נרצה למחוק את הקובץ המוחבא, עלינו למחוק את הספרייה כולה.

אם תוקף זדוני ירצה לוודא כי הקובץ המוחבא שלו יהיה מוגן היטב ממחיקה, כל שעליו לעשות הוא ליצור אותו כשנקודת הקישור שלו היא הספרייה עליה מותקנת מערכת ההפעלה.

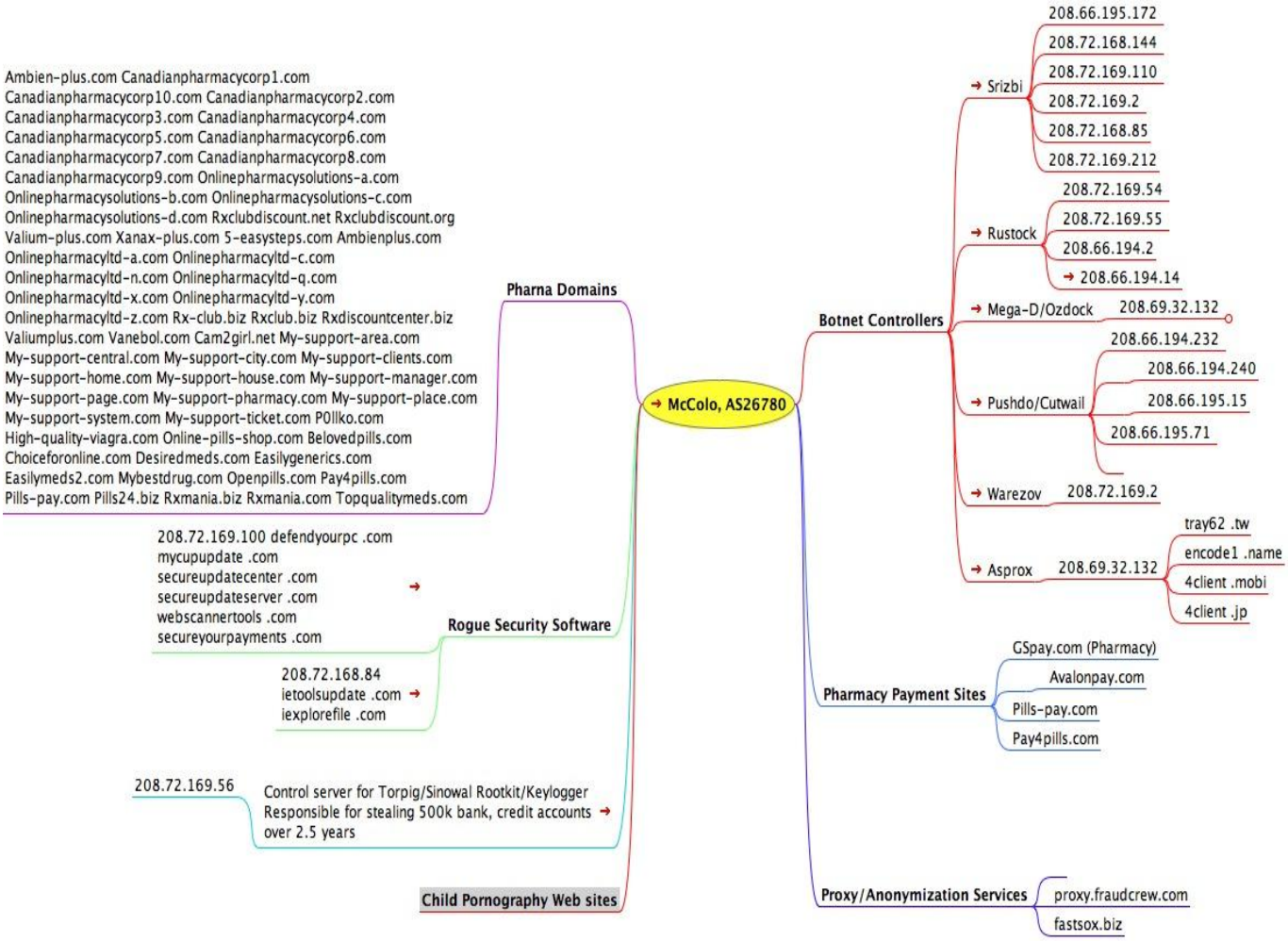
לבסוף, אין שום מניעה כי הקובץ המוחבא יהיה קובץ הרצה לכל דבר וכפי שנראה במסמך זה, מדובר בשיטה הנמצאת בשימוש בעולם.

4.3 היסטוריה וסטטיסטיקות

1.4.3 התחלת הפעילות

רשת Mega-D החלה לבנות עצמה בסוף שנת 2007, באמצעות הפצת סוס טרויאני בשם Ozdok, שהיווה פיתוח ייעודי לנושא. בתחילה, שרתי השליטה והבקרה שלה, כמו של רשתות Botnet רבות אחרות, התארחו ברשת נפרדת – רשת McColo. עד שנת 2008, רשת McColo רשת הייתה רשת מרכזית מאוד לאירוח אתרי תרופות מזויפות, פורנוגרפיה, תוכנות זדוניות וכאמור, שרתי שליטה ובקרה לסוסים טרויאניים.

בתמונה הבאה ניתן לראות את מפה חלקית של הקשרים בין רשת McColo לפשיעה הקיברנטית העולמית:

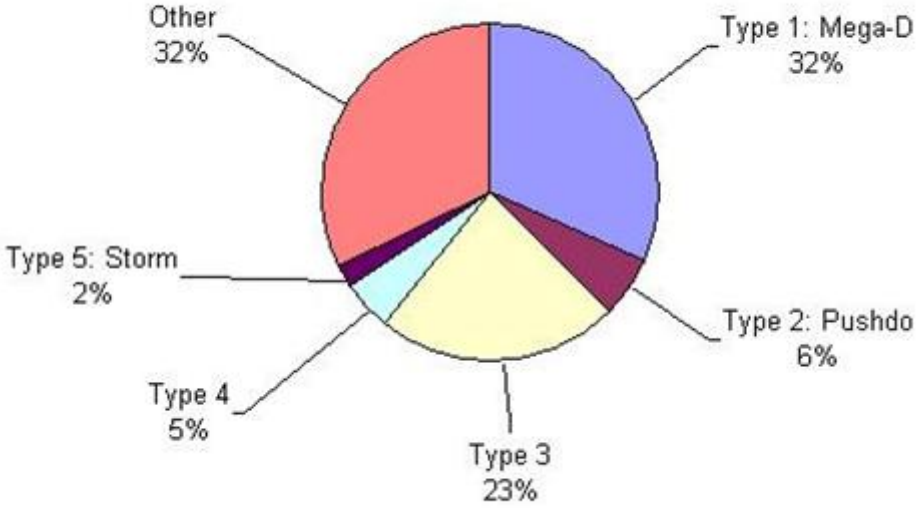


כבר בחודש הראשון לפעילותה רשת Mega-D נכנסה לעשירייה הראשונה של מפיצי הספאם הגדולים בעולם. חצי שנה בלבד לאחר תחילת פעילותה הגיעה הרשת להיקף שיא של 32% אחוז מתעבורת הספאם העולמית, והיא עשתה זאת באמצעות 35,000 מחשבים נגועים בלבד.

לשם ההשוואה, רשת הזומבים המפורסמת Storm Net, אשר חלשה בשיאה על יותר ממאה אלף מחשבים בכל רגע נתון, וגם זה על פי הערכות חסר, הייתה אחראית ברגע השיא שלה "רק" על כ-21% מתעבורת הספאם בעולם.

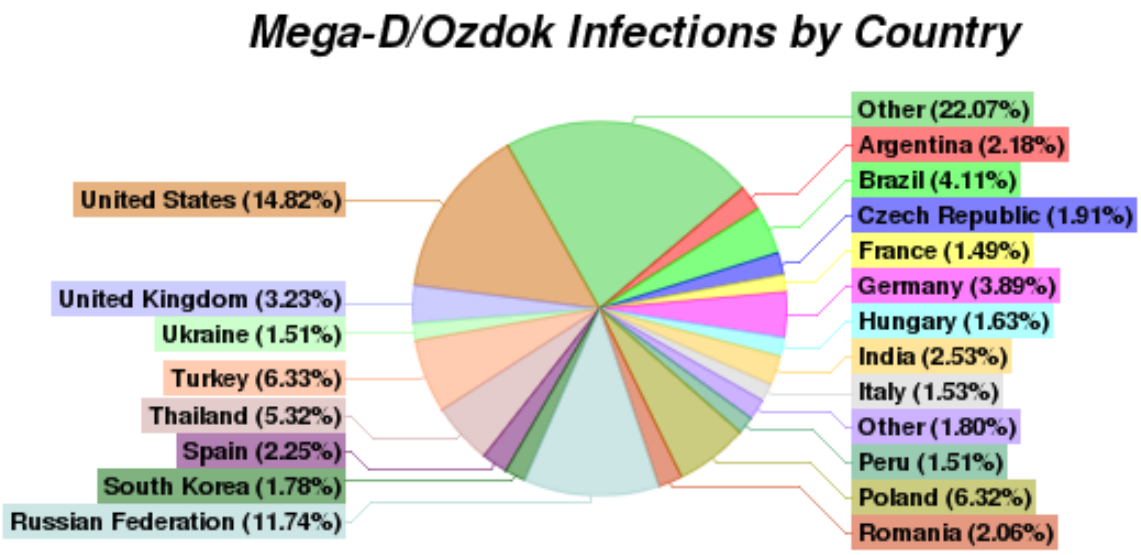
Mega-D לא שברה שיאים אך ורק באחוזי השליטה שלה, אלא גם ברווחיות כלכלית. חוקרי אבטחת מידע וכלכלה, מעריכים כי על כל 12.5 מליון דברי ספאם שנשלחים בעולם, אדם

אחד יתפתה ויבצע רכישה בגובה ממוצע של $96.5[1]. מספר זה מיתרגם לרווח של $0.0000077 על כל דואר ספאם שנשלח. מספר זה אולי נראה קטן מאוד ואולי גם לא כלכלי, אך בחודש ינואר 2008, שיא פעילות הרשת, רשת Mega-D שלחה **כ-1.5 מיליארד דברי דואר ביום**, או במילים אחרות, גרפה רווח של $350,000.



[1] http://www.techradar.com/news/computing/spammers-get-1-response-to-12-500-000-emails-483381

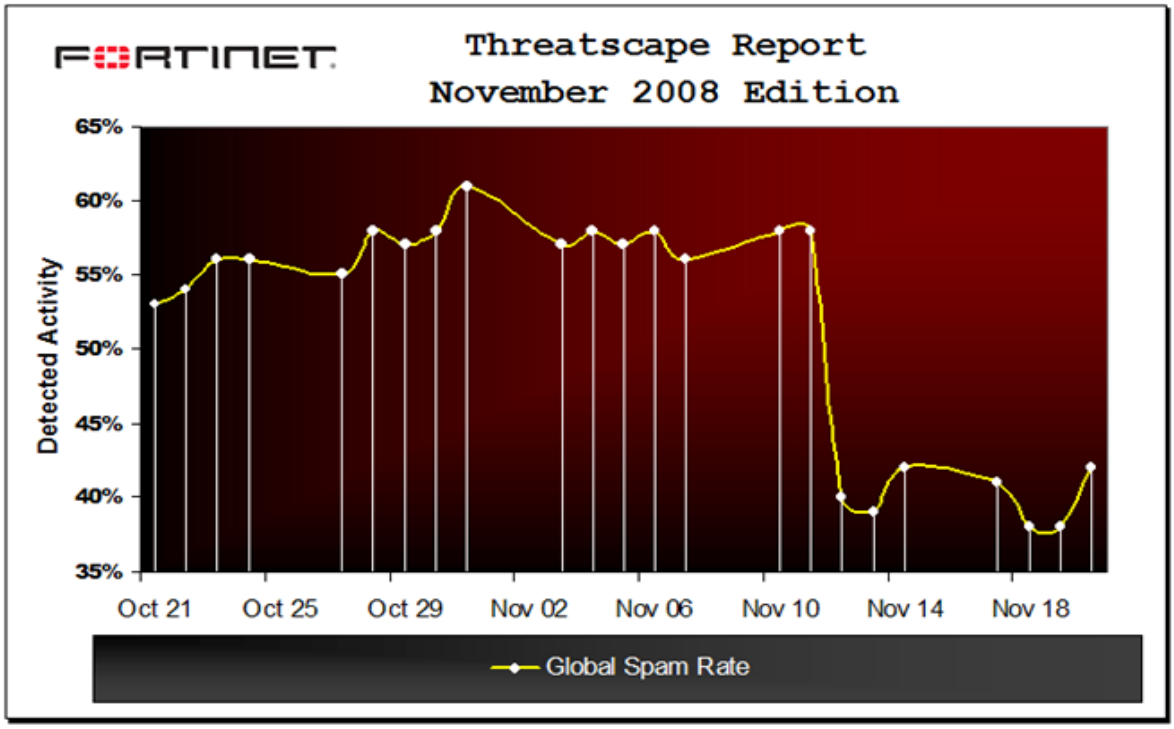
2.4.3 התפשטות Mega-D בעולם



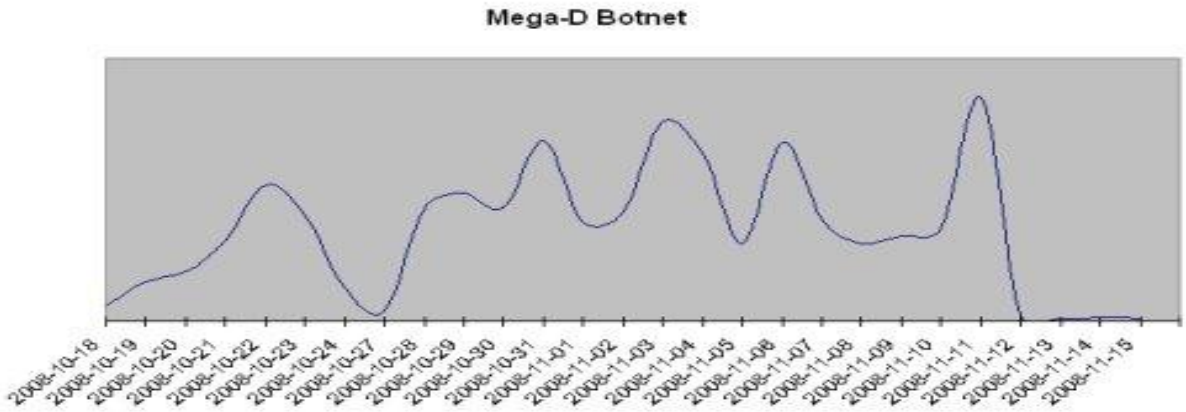
3.4.3 הנפילה הגדולה הראשונה, וההתאוששות הזמנית

בנובמבר 2008, לאחר פעילות משותפת של מספר גופי בטחון ומחקר באבטחת מידע, הורדה רשת McColo מעל גבי האינטרנט.

בתמונה הבאה ניתן לראות את גודל תעבורת הספאם כאחוז מתעבורת האינטרנט העולמית, ואת הנפילה הגדולה שבאה בעקבות הפלת רשת McColo.

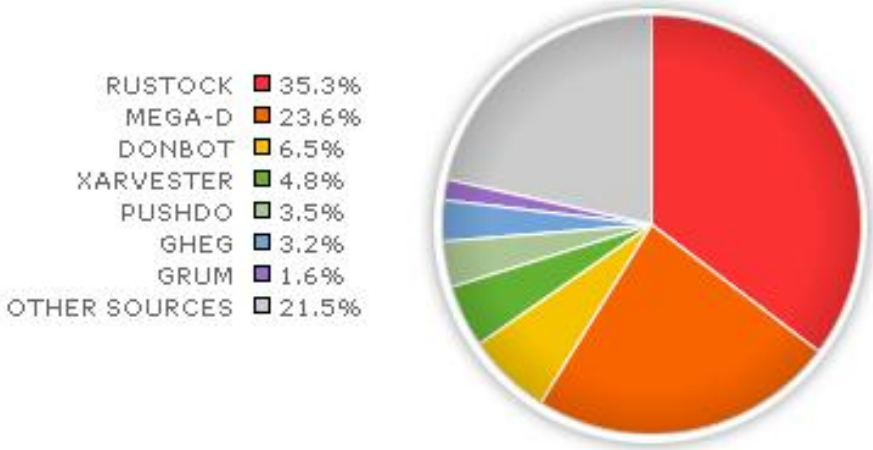


רשת Mega-D הושפעה ממהלך זה בצורה דרסטית



עם זאת, לאחר זמן קצר ניתן היה לראות שכמות דואר הזבל התחילה לצמוח בחזרה. בוני Mega-D החליטו ליצור לעצמם רשת חדשה וייעודית, ולמדו את הלקחים הנדרשים מהפלת McColo. על מנגנוני ההגנה השונים שהוספו לOzdok כתוצאה מכך, יפורט בהמשך.

במהלך השנה שבאה אחרי הנפילה הגדולה, רשת Mega-D הייתה בדרך הבטוחה לחזור לגדולתה. התמונה הבא מראה את חלוקת הספאם בעולם על פי רשתות ההפצה הגדולות. יש לקחת את הנתונים המובאים בפרופורציה הנכונה; גם אם אחוזי השליטה גדולים של המתחרה Rustock גדולים אף מהשיא הקודם של Mega-D, במספרים אבסולוטיים המספר אפילו לא קרוב לימי גדולת תעבורת הספאם של רשת McColo.



4.4.3 הפלת Mega-D על ידי חברת FireEye

כאמור, Mega-D הייתה בדרך חזרה למעלה, אך הפעם חברת אבטחת מידע בשם FireEye החליטה לקחת את העניין לידיה, ולהוריד את הרשת.

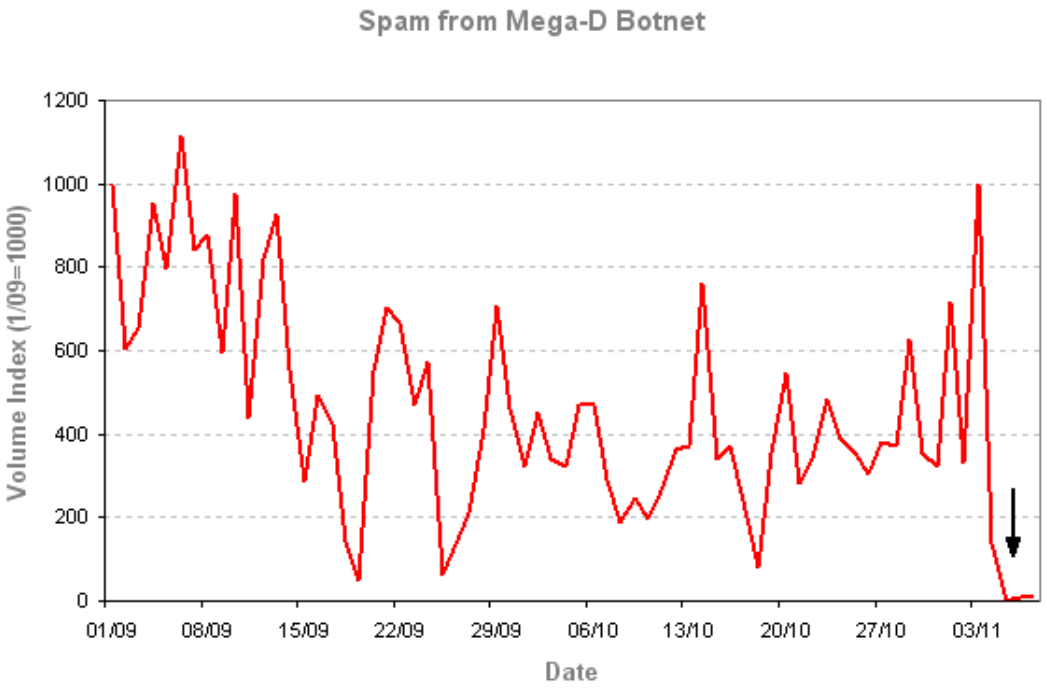
לאחר מחקר מעמיק על הסוס עצמו, יצרה חברת FireEye קשר עם כל ספקיות האינטרנט אצלם התארחו שרתי ה-C&C הידועים של Mega-D, וביקשה מהם להוריד את השרתים. לאחר פנייתם נשארו רק 4 כתובות IP של שרתי שליטה ובקרה.

בשלבים הבאים, חברת FireEye החלה בשיטתיות ובהדרגתיות להשתלט על שרתי השליטה והבקרה של הסוס. מצב זה אפשר לחברה לבנות שרתי דמה של שליטה ובקרה, ולהתחיל לקבל מידע רב לניתוח, כולל מידע על אופי פעילות הסוס, וכן על היקף ההתקנות שלו.

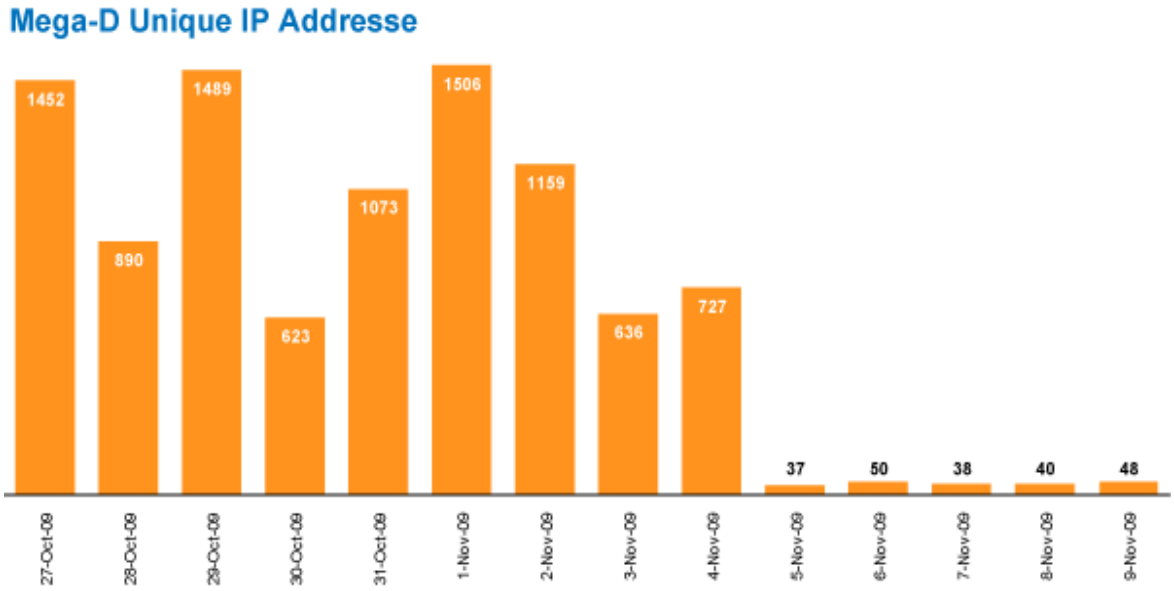
כפי שנאמר מעלה, כל סוס Ozdok מגיע עם רשימה מובנית של שרתי שליטה ובקרה. חברת FireEye הסתמכה על כך שבכל רגע נתון היו פעילים רק מספר שרתים בודדים, וכל שאר הרשימה שימשה לגיבוי בלבד. FireEye ניצלה את חוסר ערנותם של בוני Mega-D, וגילתה כי מספר דומיינים רשומים של שרתי שליטה ובקרה עומדים לקראת סיום תקופת הרכישה שלהם. ברגע שיכלו, רכשה החברה את הדומיינים, וניתקה בכך את הסוסים מהשרתים שלהם. לאחר מכן, FireEye רכשה את הדומיינים הלא פעילים הרשומים של רשת Mega-D.

כמו כן, כפי שנאמר קודם, כמפלט אחרון, הסוס המותקן יכול לייצר שם אקראי ולנסות לבנות אליו. ברגע שחברת FireEye הצליחה להבין את החוקיות שבשמות האקראיים לכאורה, רכשה החברה גם את הדומיינים הללו, וקישרה אותם לשרת הדמה.

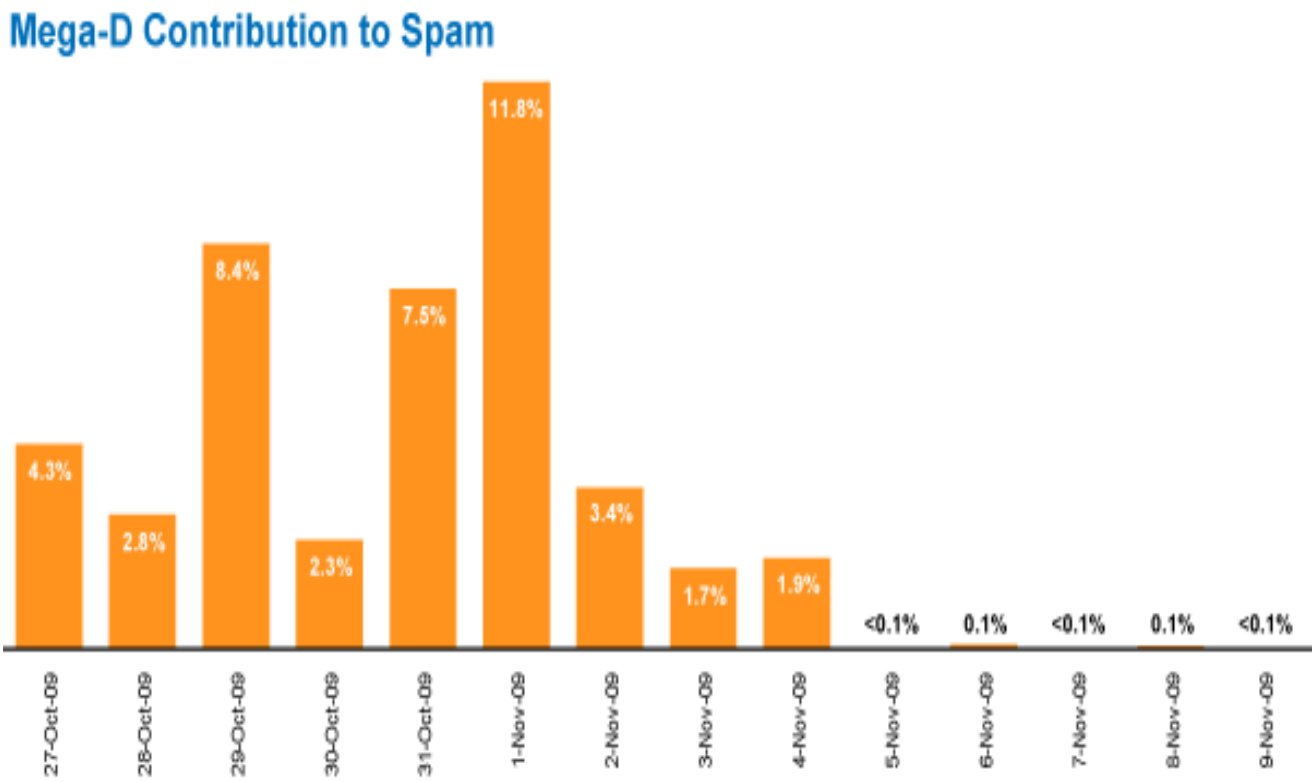
כאן ניתן לראות את ההשפעה של עבודתה של FireEye על כמות ה-Spam שנשלחה על גבי רשת Mega-D.



בגרף הבאה ניתן לראות נתונים לגבי מספרי ה IP הייחודיים של רשת Mega-D שנראו על ידי Symantec. לפי Symantec כל יום נצפו בין 600 ל 1600 כתובות IP ייחודיות המקושרות לרשת Mega-D. לאחר ה4 בנובמבר מספר זה ירד ל-50.



בגרף הבאה ניתן לראות את כמות הדואר הנשלח מMega-D לפי אחוז מכל הדואר בעולם. ניתן לראות שלאחר ה-4 בנובמבר כמות דואר הזבל שנשלח מMega-D הוא קטן מעשירית האחוז מכלל הדואר העולמי.



5.4.3 סיכום ביניים

מוקדם עדיין מכדי להעריך אם הפלת רשת Mega-D היא עניין סופי או זמני. לבטח ניתן להגיד שגם רשת Mega-D לא תשוב, יהיו אחרות שיתפסו את מקומה.

עם זאת, נשאלת השאלה – אם חברה קטנה כמו FireEye הצליחה להפיל את אחת מרשתות הספאם הגדולות, למה לא נעשתה פעולה כזו מצד ענקי אבטחת המידע. עולם אבטחת המידע כבר ידע הצלחות של התארגנויות מסוג זה – לדוגמא, בפברואר 2009 חברות כגון מייקרוסופט, VeriSign, AOL, Symantec ועוד רבות התאגדו בהצלחה כדי להפיל את תולעת הקונפיקר.

האם אין דרך לשמור על התארגנות זו פועלת ומצליחה לאורך זמן?

ביבליוגרפיה

http://blog.fireeye.com/research/2009/11/killing-the-beastpart-4.html

http://www.symantec.com/connect/blogs/mega-d-aka-ozdok-crippled

http://www.secureworks.com/research/threats/ozdok/?threat=ozdok

http://www.m86security.com/TRACE/traceitem.asp?article=510

http://tools.cisco.com/security/center/viewAlert.x?alertId=18233

http://www.spamfighter.com/News-9799-New-Mega-D-botnet-supersedes-Storm.htm

http://www.m86security.com/trace/traceitem.asp?article=1161

http://www.symantec.com/security_response/writeup.jsp?docid=2008-021215-0628-99&tabid=2

http://blogs.msdn.com/tzink/archive/2009/11/13/fireeye-knocks-mega-d-offline.aspx

http://www.m86security.com/trace/i/Botnets-show-signs-of-life,trace.820~.asp

http://blog.fireeye.com/research/2009/11/smashing-the-ozdok.html

http://www.zdnetasia.com/news/security/0,39044215,62037354,00.htm

http://www.securecomputing.net.au/News/102413,megad-botnet-stronger-than-storm-promotes-male-sexual-pills.aspx

http://www.m86security.com/support/search/SiteSearch.asp

http://www.mxlogic.com/itsecurityblog/1/2008/11/The-Day-the-Botnet-Died.cfm

http://www.avertlabs.com/research/blog/?cat=3

http://vil.nai.com/images/message.jpg

http://www.securecomputing.net.au/Feature/103968,superbotnets-megad-vs-storm-an-indepth-look.aspx

http://www.windowsecurity.com/articles/Alternate_Data_Streams.html

http://www.m86security.com/trace/i/Mega-D-Spam-Returns,trace.571~.asp

http://billmullins.wordpress.com/2009/11/13/the-mega-d-botnet-bites-the-dust-sort-of/

http://arstechnica.com/security/news/2008/12/mega-d-botnet-flexes-muscle-after-isp-takedowns.ars

http://www.pc1news.com/news/0298/herbalking-uses-mega-d-botnet-to-spam-millions.html