ממשל זמין – פרויקט תהיל"ה

דו"ח סיכום

סוסים טרויאניים נפוצים

-

ZEUS

ממשל זמין – פרויקט תהיל"ה

מאפייני מסמך

מחבר	פולינה חזנוב, יול בהט
מספר גרסה	1
סטטוס	סופי
תאריך הוצאה	ספטמבר 2009
שם קובץ אלקטרוני	

תשומות / הערות

שם/תפקיד	הערה (אופציונאלי)	תאריך	חתימה

אישורים

שם/תפקיד	תאריך	חתימה

היסטוריה

מ. גרסה	ת. הוצאה	מחבר	שינויים מרכזיים בגרסה
0.1	11.09.09	פולינה חזנוב, יול בהט	גרסה ראשונה

הפצה

מ. גרסה	נמענים
0.1	אסף קרן, עידו קרופקין, שלומי מוסרי

ממשל זמין – פרויקט תהיל"ה

תוכן עניינים

1. כללי 4

1.1 רקע 4

1.2 Zeus 4

2. סוסים טרויאניים באופן כללי 5

2.1 מה הוא סוס טרויאני 5

2.2 שימושים נפוצים 5

3. Zeus בפירוט 6

3.1 כללי 6

3.2 דרכי הפצה 7

3.3 אופן פעילות ויכולות שונות 8

3.3.1 בניית הסוס 8

3.3.2 התבססות במחשב המותקף 10

3.3.3 גניבת מידע רגיש 11

3.3.4 שליטה מרחוק 12

3.4 שליטה ובקרה 13

3.4.1 קובץ קונפיגורציה 13

3.4.2 אתרי שליטה ובקרה (C&C) 14

3.5 היסטוריה וסטטיסטיקות 17

3.5.1 כללי 17

3.5.2 אירועים חריגים 17

3.5.3 רמת ההתפשטות של Zeus בעולם 19

3.5.4 סטטיסטיקות תפוצה בממשלת ישראל 21

3.6 גילוי והסרה 22

3.6.1 זיהוי הדבקה 22

3.6.2 זיהוי תקשורתי 23

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 Zeus

מסמך זה מסכם את הידע הצבור כיום בידי צוות אבטחת המידע על הסוס הטרויאני הידוע בכינויים Zeus או Zbot. סוס טרויאני זה החל לפעול בשנת 2007 ומאז הושתל בכ-4 מליון מחשבים ברחבי העולם. כיום, כמעט שנתיים לאחר תחילת פעילותו, Zeus עדיין נחשב לאחד הסוסים הטרויאניים הפעילים והמסוכנים ביותר[1].

[1] http://msmvps.com/blogs/harrywaldron/archive/2009/08/22/trend-labs-10-of-most-dangerous-malware-attacks-of-all-time.aspx

2.סוסים טרויאניים באופן כללי

2.1 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 ושולחים אותו ליעד מוגדר מראש (למשל מספרי כרטיסי אשראי או סיסמאות).

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.Zeus בפירוט

3.1 כללי

הסוס הטרויאני Zeus, המוכר גם בשם Zbot, הוא סוס טרויאני אשר מוריד את הגדרות האבטחה, מחדיר ומשנה קבצים במחשב הפרוץ. Zeus פותח למעשה חלון כניסה, דרכו מאות תוכנות פרסום ותוכנות ריגול זדוניות נוספות יכולות לחדור למחשב. בנוסף, Zeus פותח דלת אחורית קבועה, המאפשרת לתוקף מרוחק שליטה מלאה במחשב הנגוע. התוקף יכול לשלוף כל מידע מהמחשב, ובמיוחד מידע פיננסי המאוחסן במחשב המותקף – מספרי אשראי, חשבונות בנק וכו'.

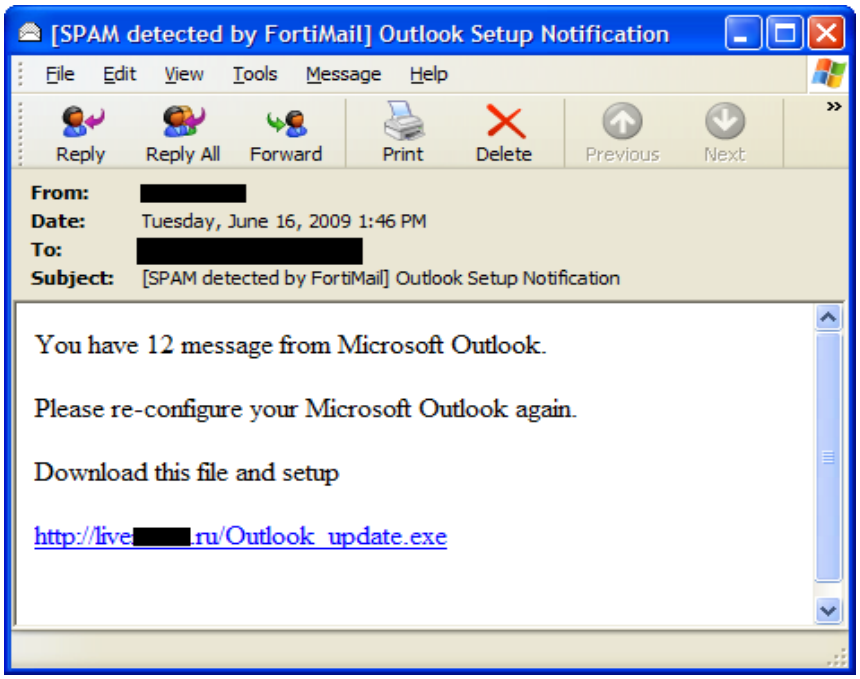
לא ידוע בוודאות מי כתב והפיץ במקור את Zeus, אך סוס זה נקשר רבות עם שמו של ארגון פשיעה קיברנטי ידוע בשם Russian Business Network. ארגון זה, אשר כונה בעבר "הרע מתוך הרעים" (Baddest of the bad[2]), לוקח חלק במגוון רחב מאוד של פעילות פשע מקוון. הארגון עומד מאחורי רשת מחשבים המארחת אתרי תוכנות זדוניות, פורנוגרפיית ילדים, מפיצי דואר זבל, גניבת נתונים ועוד. נטען כי רווחי הארגון מרשת זו, בשנת 2007, עמדו על **יותר משני מיליארד דולר**. ניתוקה של הרשת כמעט בלתי אפשרי משום שזו לא חברה רשומה, ואין שמות אמיתיים על שמם נרשמים האתרים. לרוב, כל מי שמנסה לפגוע ברשת מותקף על ידה. בעלי הרשת ככל הנראה יושבים בסנט פטרסבורג, אך ידוע גם כי הם פועלים גם בלטבייה וגם בקזכסטן. הרשת מקושרת עם המאפיה הרוסית ונטען אף כי הם מקיימים קשרים ישירים גם עם הממשלה הרוסית.

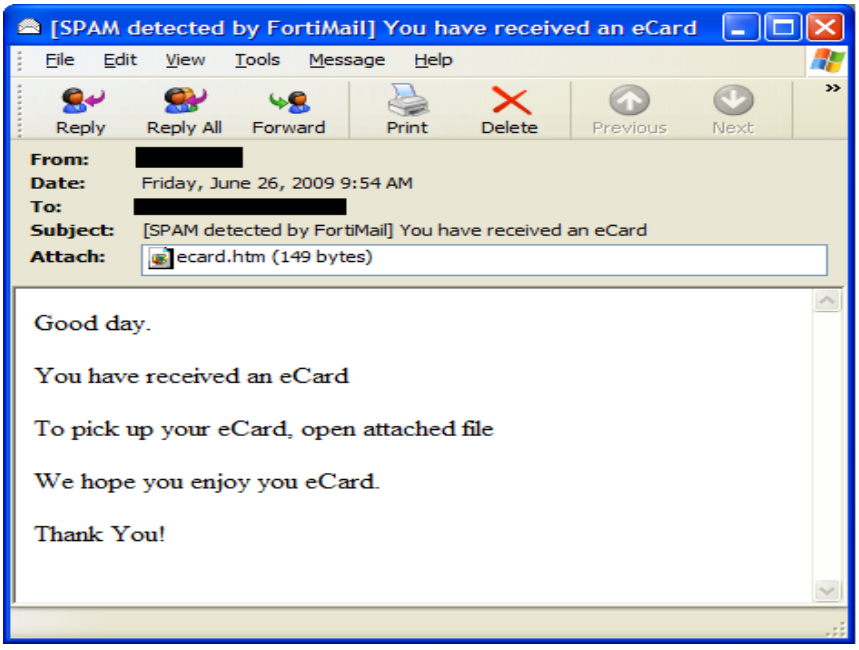
[2] http://www.itu.int/ITU-D/cyb/newslog/VeriSign+Classifies+RBN+The+Baddest+Of+The+Bad.aspx

3.2 דרכי הפצה

לרוב, הפצת Zeus מתבצעת על ידי קובץ מצורף במייל עם כותרות מושכות, אשר גורמות לקורבן לפתוח את הקובץ או קישור לאתר זדוני.

למשל מיילים כגון :





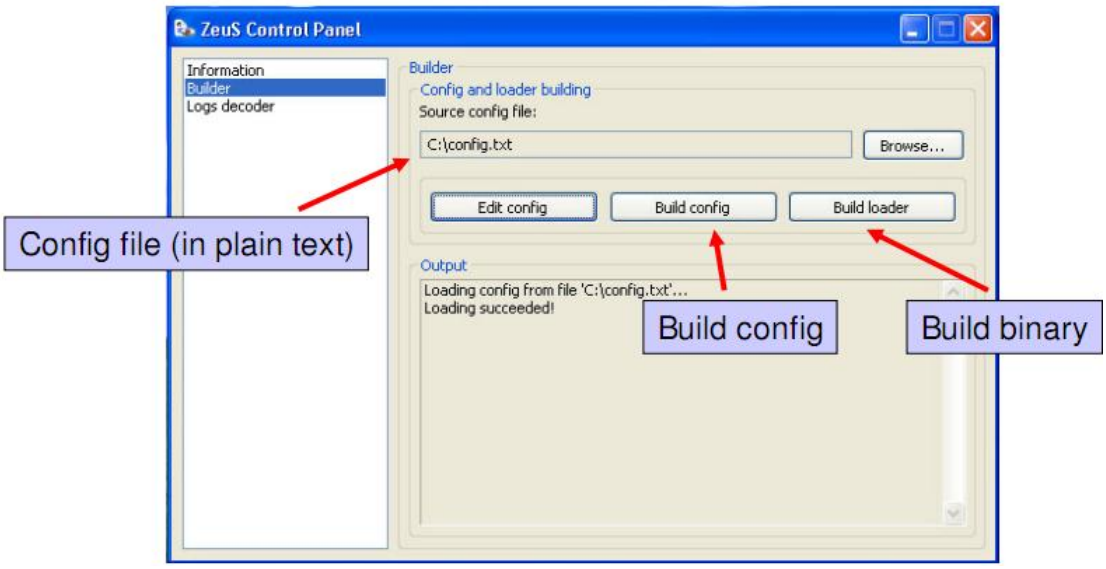
עם זאת, קיימות גם דרכים אחרות, כמו למשל ניצול Exploits במערכות ההפעלה או תוכנות שונות.. תוקף עלול גם לנצל Cross Site Scripting Vulnerabilities באתרים תמימים, על מנת לגרום למשתמשים לגלוש לאתרים זדוניים ללא ידיעתם, וכן ניתן גם לקבל את הסוס דרך צ'אטים או תוכנות שיתוף אחרות.

בנוסף, לאחר התקנה מוצלחת במחשב, הסוס יודע לשלוח את עצמו מבלי ידיעתו של המותקף לקורבנות נוספים.

3.3 אופן פעילות ויכולות שונות

3.3.1 בניית הסוס

בכדי לקמפל סוס חדש להדבקה, כתבו מפיצי הסוס תוכנה, או Framework, לבנייה אוטומטית של סוסים על פי הגדרות שונות. Framework זה נמכר לכל דורש במחיר הנע סביב 4000 דולר, וממשק שליטה מבוסס Web ב-700 דולר נוספים.



מפתחי הסוס אף הגדילו לעשות, והוסיפו לתוך ה-Framework הסכם תנאי שימוש (EULA), וכן סנקציות כלפי מפירים:

"The vendor of the ZeuS crimeware kit provides professional technical support to the customer.
The customer is not authorized to disassemble or analyze the code of bot nor The builder, and is not authorized to submit parts of ZeuS to antivirus vendors.
If the customer violates this end-user license agreement (EULA) the bot of the customer will be immediately submitted to antivirus vendors.

למרבה האירוניה, בפורומים ואתרים שונים נפתח "שוק שחור" לנושא, וניתן להשיג גרסאות של ה-Framework במחיר "מציאה" של כ-1000 דולר בלבד.[3]

[3] http://www.opensc.ws/trojan-malware-releases/7537-zeus-actual-exploit-packs.html

3.3.2 התבססות במחשב המותקף

הסוס בנוי בצורה ערמומית על מנת לבצע פעילות זדונית על המחשב המותקף ללא זיהוי. בתחילה, הסוס מנסה לאתר תוכנות הגנה באמצעות בדיקת רשימת התהליכים (Processes) הרצים במחשב. אם הוא נתקל בתהליכים כגון outpost.exe ו zlclient.exe (שניהם processes של חומות אש) הוא רושם את עצמו בתיקיית ה system32 ויוצא.

אם הוא מוצא שניתן להמשיך בבטחה, הוא כותב ערכי registry על מנת להבטיח פעילות תקינה, וכן שהוא יורץ בכל הפעלה של המחשב.

דוגמא לערכי Registry כאלו:

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Network]
+ UID = "%ComputerName%" (adds computer name)

[HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer]
+ {F710FA10-2031-3106-8872-93A2B5C5C620} = F7 09 F2 0D

[HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings]
+ ProxyEnable = 0x00000000

הסוס יוצר תיקייה בתוך %windir%/system32/, ובתוך התיקייה הוא יוצר שני קבצים חדשים. אחד הקבצים משמש לאחסון כל הנתונים הגנובים של המערכת המותקפת, והשני הוא קובץ הקונפיגורציה המוצפן אשר מורד מכתובת מוגדרת מראש. את עצמו הסוס מעתיק גם כן לספריה %windir%/system32/, ובכדי להימנע מזיהוי על ידי תוכנות אנטיוירוס הוא מוסיף לעצמו נתונים אקראיים.

קיימות ארבע וריאציות נפוצות לשמות הקבצים בהם עושה הסוס שימוש:

Variant	Trojan Binary	Storage File	Configuration File
1	ntos.exe	wsnpoem\audio.dll	wsnpoem\video.dll
2	oembios.exe	sysproc64\sysproc86.sys	sysproc64\sysproc32.sys
3	twext.exe	twain_32\local.ds	twain_32\user.ds
4	sdra64.exe	lowsec\local.ds	lowsec\user.ds

לא מן הנמנע שקיימות וריאציות נוספות.

3.3.3 גניבת מידע רגיש

Zeus מוחק קבצי cookies ואת הcache של הכתובות בדפדפן. בצורה זו התוקף מכריח את הגולש להקליד את הכתובות שאליהן הקורבן רוצה לגלוש, התוקף "מאזין" לכל הקלדה במקלדת, וכך ומגלה לאילו אתרים גלש הקורבן ומה הוא מקליד. אם הקורבן גולש לאתרי בנקים או אתרי תשלומים, התוקף יכול לגלות את כל הפרטים האישיים של הקורבן כולל נתונים פיננסיים.

הסוס יכול לשנות את קובץ ה-Hosts במחשב, דרכו ניתן לקבוע בצורה סטטית כתובות IP של אתרים מסוימים. על ידי כך הסוס גורם לקורבן להיות מנותב לאתר שנראה זהה לאתר אליו הקורבן רצה לגלוש, וכל הנתונים שהקורבן יזין יגיעו לידיים זדוניות.

התוכנה הזדונית מסוגלת לבצע גם צילומי מסך של הקורבן, ולשלוף את הנתונים הרשומים ב Windows Protected Storage, כולל תעודות (Certificates) של המכונה המותקפת. התוכנה גונבת גם כן את שמות המשתמש והסיסמאות השונים של הקורבן.

המידע הרגיש מועבר בחזרה לשרת השליטה והבקרה באמצעות גלישה לקבצי PHP ייעודיים (הנקראים Dropzones). המידע עובר בצורה מכווצת ומוצפנת, כך שלא ניתן לפענח איזה מידע זלג החוצה.

דוגמה לתעבורת שידור מידע של Zeus

```
POST /[redacted]/cp/s.php HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: [redacted]
Content-Length: 309
Connection: Keep-Alive
Pragma: no-cache

k...+G.Z.....bTQ...n...=l.Dl.....G.l
.zM.m .c.h...?...@....R...C....{......D...5...db0.K.....G...kI.W.^.Az
+,pL.g=..y..m../(...R..(~.x.by..4'dxn.ZZ.!.W....+.5.......s..+c.h..=
..`...g.O.@Y.....8.H..O.+....j.G..+...Z.v-$.....HTTP/1.1 200 OK
Date: Sat, 18 Apr 2009 05:29:56 GMT
Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.5 with Suhosin-Patch
X-Powered-By: PHP/5.2.4-2ubuntu5.5
Content-Length: 44
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html

r...+G.Z.....`.j.=A.q`.Y.
@v.....G.l..zM.m .
```

3.3.4 שליטה מרחוק

Zeus יכול לצרף את המחשב לרשת bot וכך המחשב הופך להיות זומבי של ה Botnet. רשתות אלו משמשות לפעילות לא חוקית במסות גדולות. כמו כן, התוקף יכול להשתמש במחשב כמעין proxy, על מנת לבצע התקפות מבלי שיוכלו לגלות את כתובת המקור של התקיפה.

התוכנה פותחת back door על מנת להריץ תוכנות אשר נמצאות במערכת, או לבצע עדכונים. במקרה הצורך משמש ה-BackDoor בכדי להרוס לחלוטין את המערכת המותקפת.

3.4 שליטה ובקרה

3.4.1 קובץ קונפיגורציה

קובץ הקונפיגורציה של Zeus אחראי להגדרות ולהעברת משימות אל הסוס המותקן במחשב.

הקובץ בנוי כמעין קובץ XML, עם כמה חלקים עיקריים:

1. כתובת למציאת הגרסה העדכנית ביותר של הסוס
2. כתובת למציאת הגרסה העדכנית ביותר של קובץ הקונפיגורציה
3. כתובת להעברת המידע שנאגר על ידי הסוס המותקן
4. רשימת כתובות "מעניינות במיוחד" להאזנה וגניבת פרטים רגישים.
5. רשימת כתובות ל-"הטיה" - אם המשתמש גולש לאחת הכתובות ברשימה, הסוס עוצר את הבקשה, ומפנה את המשתמש לאתר דמה.

בגרסה המקורית של הסוס, קובץ הקונפיגורציה לא היה מוצפן, אלא מעורבל. כלומר, במידה ואלגוריתם הערבול היה ידוע, ניתן היה לקרוא את הקובץ. לקראת סוף 2008 פוענח אלגוריתם הערבול על ידי חברות האבטחה, וכלי לקריאת קבצי קונפיגורציה פורסם והופץ בעולם.

בגרסה הנוכחית פתרו כותבי הסוס את הבעיה הזו, מבחינתם, על ידי כך שהוסיפו מנגנון הצפנה לקובץ הקונפיגורציה. ל-Zeus הוספו יכולות הצפנה באלגוריתם RC4, כאשר לכל סוס מקומפל מפתח הצפנה משלו. המפתח מוטמע בקוד של הסוס עצמו, כך שלמעשה רק הוא יהיה מסוגל לפענח את קבצי הקונפיגורציה אשר הוצפנו באמצעותו.

3.4.2 אתרי שליטה ובקרה (C&C)

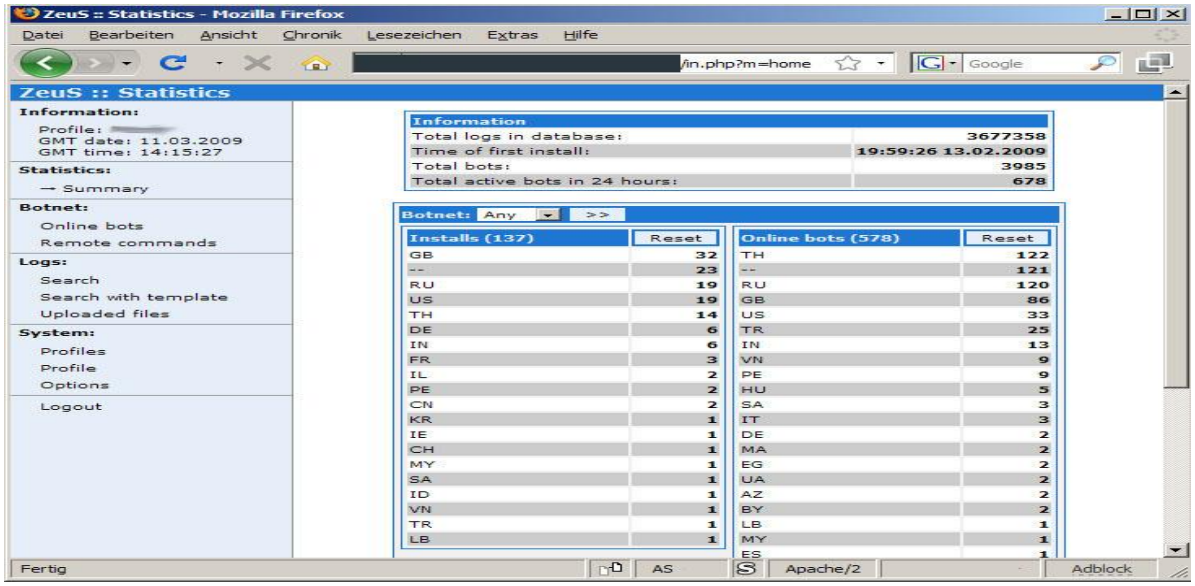
כאמור, Zeus מקבל פקודות ועדכונים באמצעות אתרי שליטה ובקרה שונים בעולם. מוערך כי קיימים כאלף אתרים כאלה בעולם, כאשר בכל רגע נתון פעילים מספר מצומצם יחסית של אתרים. קיימים אתרים ייעודים באינטרנט למעקב אחרי שרתים כאלו. המפורסם באתרים אלו הוא https://zeustracker.abuse.ch, בו ניתן לקבל בזמן אמת מידע רב על השרתים הפעילים.

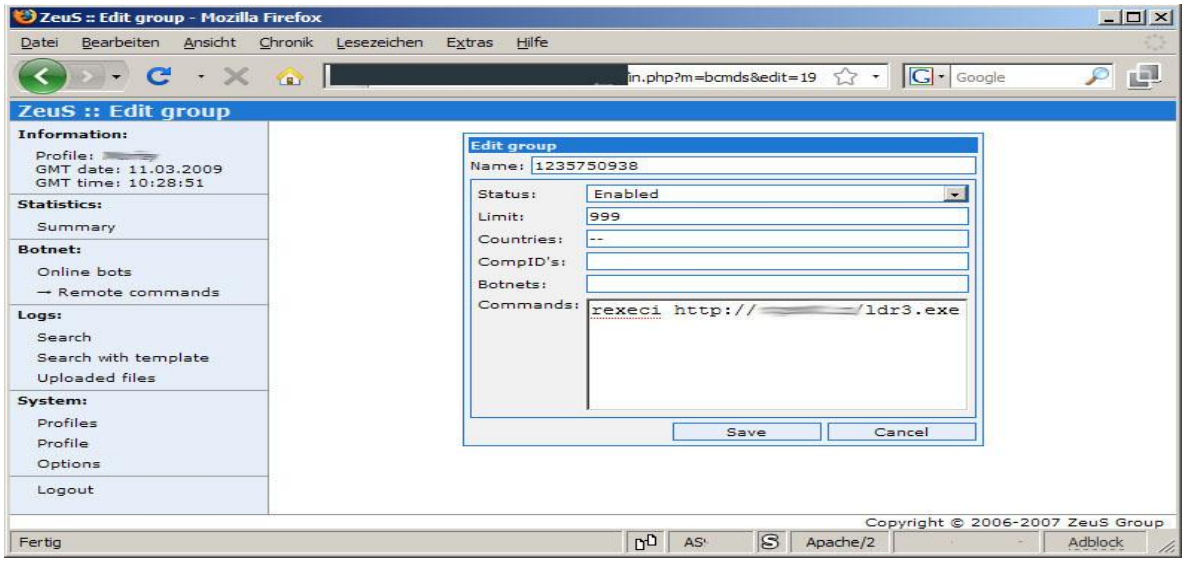
אתרי השליטה והבקרה מפוזרים בעולם, ולא מרוכזים במידה אחת, דבר המקשה על ריכוז פעילות נגד. על פי נתונים אחרונים, אלו הן עשרת המדינות המארחות את המספר הרב של אתרי C&C:

# of ZeuS hosts	country
96	Russian Federation (RU)
92	China (CN)
80	United States (US)
40	Netherlands (NL)
17	Ukraine (UA)
14	Germany (DE)
12	Latvia (LV)
11	Taiwan, Province of China (TW)
11	Kazakhstan (KZ)
8	Turkey (TR)

השליטה בסוס מתבצעת באמצעות ממשק שליטה פשוט ונוח, אם כי רחב ביכולותיו. בדרך כלל במסך ההזדהות ניתן לבחור אם להציג את הממשק בשפה האנגלית או ברוסית. לאחר הזדהות, ניתן לראות נתונים סטטיסטיים כגון מספר הbots הקיימים ומספר ה-bots המחוברים כרגע, מתי עודכנו ה-bot וכמות הלוגים הזמינים. ניתן גם לאחד מספר bot לקבוצות מסוימות, ובכך ליצור רשתות Botnet.

כמובן שניתן גם לראות נתונים על כל bot בנפרד (זמן הדבקה, ארץ, גרסת סוס ועוד), וכן לבצע בו פעולות שונות, כפי שיתואר בהמשך המסמך.



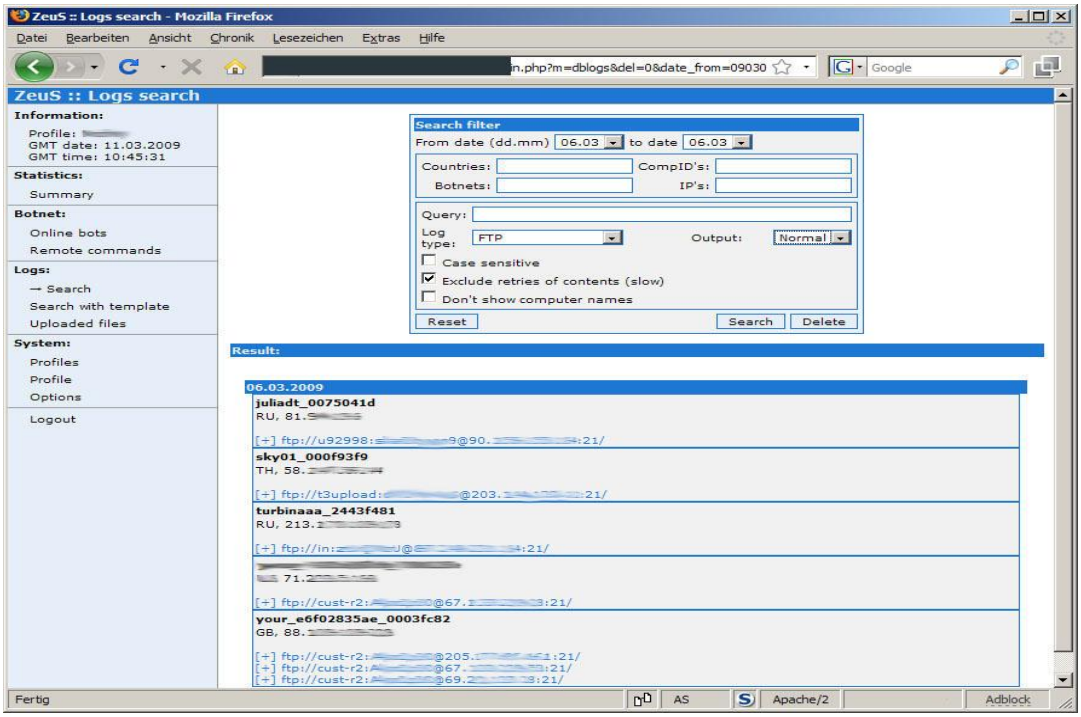


ניתן לבצע מספר פקודות דרך הממשק.

לדוגמה:

- block_url - חוסם גישה לכתובת ספציפית
- resetgrab - משנה את קובץ ה cookies.
- rexec - גורם למחשב לבצע הורדה והרצה של קובץ ממחשב מרוחק.
- lexec - גורם למחשב הרצה של קובץ הנמצא על המחשב.
- getfile - הורדה של קובץ
- upcfg - הורדה של קובץ קונפיגורציה.
- kill operation system – Kos

ניתן גם לבצע חיפוש בלוגים של המכונה לפי פרמטרים שונים כגון טקסט מסוים, זמן כתיבה, סוג קובץ וכו'.



3.5 היסטוריה וסטטיסטיקות

3.5.1 כללי

ניתן למצוא עדויות בפורומים על קיומו של הסוס כבר בשנת 2005, אם כי אין הוכחות מוצקות. ההוכחות הראשונות לקיום הסוס מתוארכות לשנת 2007.

מאז הפצתו הראשונה, הסוס עבר מספר שדרוגים, וכעת הגרסה הרשמית הנוכחית היא 1.2.1.11.

רוב ההבדלים בין הגרסאות השונות נובע מפיצ'רים שונים ויכולות חדשות של הסוס. עם זאת, ללא ספק ההבדל המהותי הוא הוספת יכולות ההצפנה של קבצי הקונפיגורציה, כמתואר בפרק 3.4.

3.5.2 אירועים חריגים

בחודש מאי 2009 החליטו המפעילים של אחת מרשתות ה-Botnet מבוססות Zeus להפיל בבת אחת את הרשת. הסיבות לכך לא ברורות לחלוטין. השערה נפוצה אחת גורסת כי המפעילים הרגישו שהרשת מייצרת יותר מדי תשומת לב לא רצויה. השערה אחרת טוענת שהמפעילים רצו לקנות לעצמם זמן לנתח ולהשתמש במידע הפיננסי שהושג עד כה, תוך כדי כך שהם מונעים מהמשתמשים לעקוב אחר המידע כפי שהיו רגילים.[4]
כך או כך, החלטה זו גרמה ליותר ממאה אלף מחשבים ברחבי העולם להפסיק לעבוד לחלוטין, וגרמה לנזקים פיננסיים רבים.

עם או בלי קשר לאירוע זה, בחודשים האחרונים התגלו ותועדו ארבעה קמפיינים גדולים להפצת הסוס באמצעות דואר אלקטרוני. על פי הגדרת החוקרים, קמפיין "גדול" הינו קמפיין בו תועדו יותר מ-1000 גרסאות שונות של דואר אלקטרוני זדוני מסוים. כמו כן, קמפיינים אלו מפנים את המחשב המותקף להורדת הסוס מכמעט 100 אתרים שונים בעולם.

[4] http://arstechnica.com/security/news/2009/05/zeus-botnet-hits-the-kill-switch-takes-down-100000-pcs.ars

הקמפיין הגדול הראשון תועד בחודש יוני 2009, ונסב סביב הודעה מזויפת המתריעה מפני חור אבטחת מידע בתוכנת הדואר האלקטרוני Outlook, כולל לינק עם הפתרון (שהפנה כמובן לסוס).

הקמפיין הגדול השני תועד גם הוא בחודש יוני, וניסה להפיץ את הסוס תוך פיתוי המשתמש לקרוא את תיאוריות הקונספירציה האחרונות בנוגע למותו של מייקל ג'קסון.

הקמפיין השלישי, בחודש יולי, ניסה לפתות משתמשים לקרוא את כרטיסי הברכה האלקטרוניים שנשלחו אליהם לכבוד יום הולדתם או אירוע אחר. קמפיין זה היה מתוחכם מהרגיל, מכיוון שהלינק אכן הוביל לכרטיסי ברכה אלקטרוניים אמיתיים, שהסתירו בתוכם גם את התקנת הסוס.

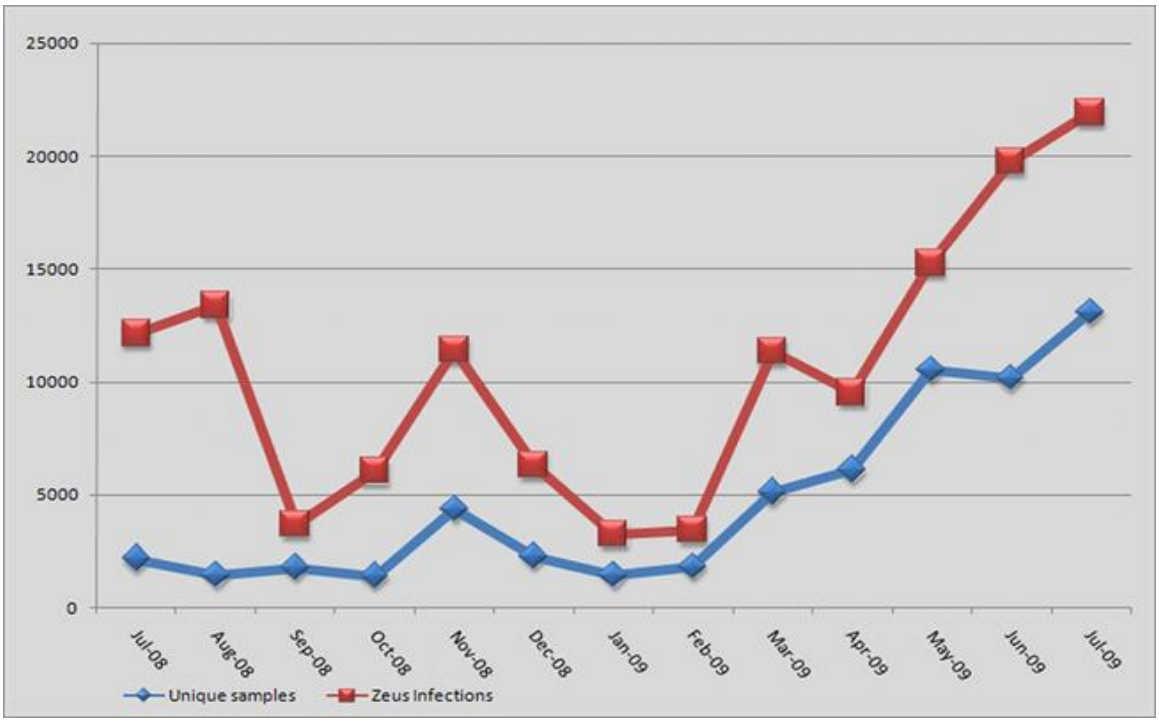
הקמפיין הרביעי והאחרון עד כה, החל בתחילת חודש ספטמבר, ולמעשה עדיין נמשך. הקמפיין הנוכחי מודיע למשתמשים כי התגלו אי דיוקים בדיווח האחרון שלהם למס ההכנסה (משרד ה-IRS האמריקאי), וכי עליהם להיכנס לאתר ולעדכן את הפרטים הרלוונטיים. הקמפיין מוסיף גם שאי דיוקים בדיווח מס ההכנסה עלול להוביל לקנות ואף מאסר.

3.5.3 רמת ההתפשטות של Zeus בעולם

לפי נתונים מעודכנים לינואר 2009, יותר מ 74,000 נתוני כרטיסי אשראי נגנבו באמצעות Zeus. כמו כן נגנבו נתוני חשבונות בארגונים גדולים כגון : NASA, Cisco, Kaspersky, McAfee, Symantec, Amazon, Bank of America, Oracle, ABC, BusinessWeek, Bloomberg, Disney, Monster, ורבים נוספים.

למרות היותו סוס "ותיק", קצב ההתפשטות שלו נותר גבוה, והוא נחשב בעיני רבים לסוס הפעיל והמסוכן ביותר כיום. לפי מחקר של אוניברסיטת אלבאמה, רק בארה"ב נדבקו יותר מ- 3.6 מיליון מחשבים. [5]

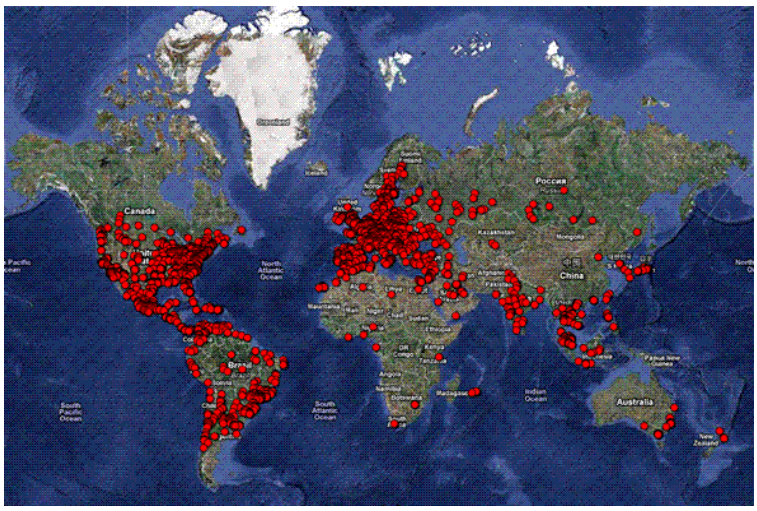
התפשטות הסוס בשנה האחרונה:



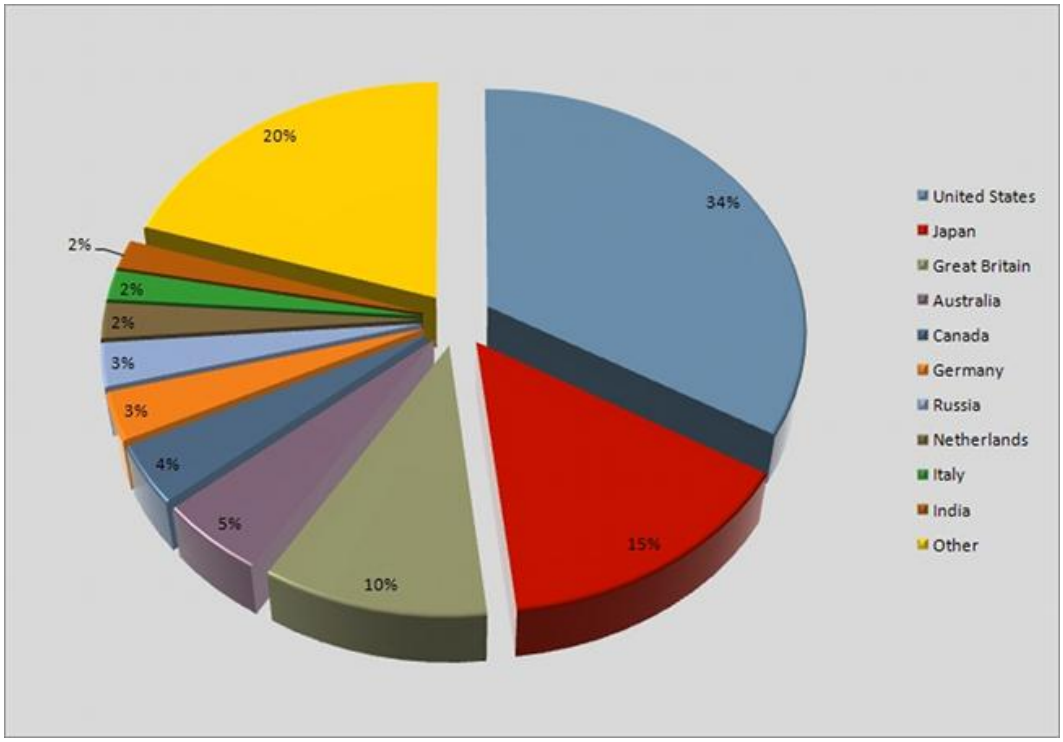
ציר ה Y - משקף את כמות הסוסים שהתגלו. ציר ה X - ציר הזמן.

[5] http://www.scienceblog.com/cms/uab-computer-forensics-links-internet-postcards-virus-23371.html

מצב פעילות הסוס בעולם:



חלוקת ההתפשטות על פי מדינות:



3.5.4 סטטיסטיקות תפוצה בממשלת ישראל

בכדי לזהות את סטטיסטיקות הפעילות של Zeus ניתחנו שלוש שעות פעילות במהלך יום עבודה רגיל. עלה כי 500 בקשות גלישה זוהו כבקשות המקושרות ל-Zeus, מתוך סך כולל של 11,000,000 בקשות. מדובר בכ-0.00004% מסך תעבורת הגלישה. יש לציין שכל הבקשות האלו נחסמו על ידי מערכות ההגנה השונות של תהיל"ה.

בקשות אלו יצאו מארבעה משרדים.

בקשות אלו יצאו אל כעשרים שרתי C&C פזורים ברחבי העולם. עשרה משרתים אלו כבר לא קיימים בעולם, ולא ניתן להתחקות אחריהם. עשרת שרתי השליטה והבקרה האחרים פועלים ב: אוקראינה, סלובקיה, גרמניה, סין, פולין, ארה"ב והולנד.

3.6 גילוי והסרה

3.6.1 זיהוי הדבקה

הקושי בגילוי הסוס נובע מכך שתוכנות האנטי-וירוס מאתרות וירוסים/סוסים לפי תבנית מסוימת. Zeus מוסיף לקובץ ההרצה שלו נתונים אקראיים ולכן התבנית של הקובץ משתנה.

MHR AV detection rate	ZeuS Binary URL	status	MD5 hash
92%	allavers.org/_vps_lib/ldr.exe	offline	34ba74c9723caf2f85b5ddd65019b942
92%	serverinlit.cn/cgi-bin/ldr(serverinlit.cn).exe	offline	b08580083bc994420f05bd85bcfeece9
90%	ajal.ru/sloader/updates/file.exe	offline	70dc7e834631b1a8f6162bb3a42d908d
90%	goodsovclass.cn/1110/out/ldr.exe	online	b9f703d2aed81aa56465ccdfaac553db
90%	demonchik.real-host.org/web_cl/bot.exe	offline	d34f9b946ec22c97ea55c5de93c7692e
89%	lendrive.ru/nenxbcnzr/newmain.exe	offline	cda6572cc698571877810c4cf8e54023
89%	a311.ru/cfg/ldr.exe	offline	dadc59354462083f32dff0033023f0b7
89%	zatura.cn/sad/demo.exe	offline	edaf18c21aa047c32df7e0da263dead6
86%	foxholter.ru/loader.exe	offline	bdc02cdf436073e25398aee69032486a
86%	chixxxa.com/tru/ldr.exe	offline	42e8ecada9e3791a6b3dea798ce4362a
86%	onlineanalytics.cn/test/ldr.exe	offline	6709f7c7e9cce7042803b8c7c1e0fe9f
86%	infinitilancer.cn/forum/load.exe	offline	3130892196b38ebd653f489d288a63ab
86%	www.saiprogetti.it/r.exe	offline	1ed1d899561e79488132cd59dfd2d3b4
86%	zdbbd.cn/zsadmin/loader.exe	offline	932e58d2585f73c44168df862dd9eaa6
86%	arsofcaribion.com/lder/ldr.exe	offline	b3dee12684ebdc9440e4413c8866876c

ניתן לראות מהטבלה שגם עשרת הסוסים הכי מאותרים לא מתגלים ב 100%. כיום ידועות מעל 500 תבניות של קובץ ההרצה. כלומר, לא ניתן לסמוך על כלי האנטי-וירוס הנפוצים לזיהוי הסוס.

3.6.2 זיהוי תקשורתי

על פי המחקר שערך צוות אבטחת המידע בתהיל"ה, הדרך היעילה ביותר לזיהוי סוסים פעילים היא באמצעות ניטור התקשורת היוצאת (Sniffing).

דרך אחת למציאת סוסים פעילים היא השוואת התעבורה היוצאת מתוך הארגון אל אתרים הנמצאים ברשימות השחורות של אתרי ההגנה בעולם. אתר ZeusTracker מפרסם בכל רגע נתון רשימה של אתרי שליטה ובקרה פעילים ולא פעילים, אותם ניתן לחסום במערכות ההגנה. במצב זה, גם אם מותקן סוס באחד מהמחשבים בארגון, הוא אינו יכול לשדר החוצה את המידע שלו, ואינו יכול לקבל רשימה עדכנית של אתרי C&C.

עם זאת, שיטה זו אינה בטוחה במאה אחוז, מכיוון שבלתי אפשרי להיות מעודכנים ברשימות בכל רגע נתון, ובוודאות קיימים אתרים C&C אליהם אתרי המעקב לא מודעים. לפיכך, בנוסף לחסימה הרשימתית, יש לבצע ניטור של התקשורת היוצאת למאפיינים מסוימים.

דרך יעילה אחת היא מעקב אחרי בקשות HTTP לקבצים מסוג bin. על פי יומני האירועים של תהיל"ה, הרוב המוחלט של גישות אלו הן גישות המתבצעות על ידי Zeus. ניתן גם לאפיין פעילות תקשורתית של Zeus גם על ידי היעדר אתר בשדה ה-Referer, דומיינים בעלי נקודה אחת בלבד (host.name) ועוד.

כל אחד ממאפיינים אלו לבדו אינו יכול לשמש כמאפיין ייחודי וודאי ל-Zeus, אך שילובם במחקר ידני הופך את המשימה לאפשרית.