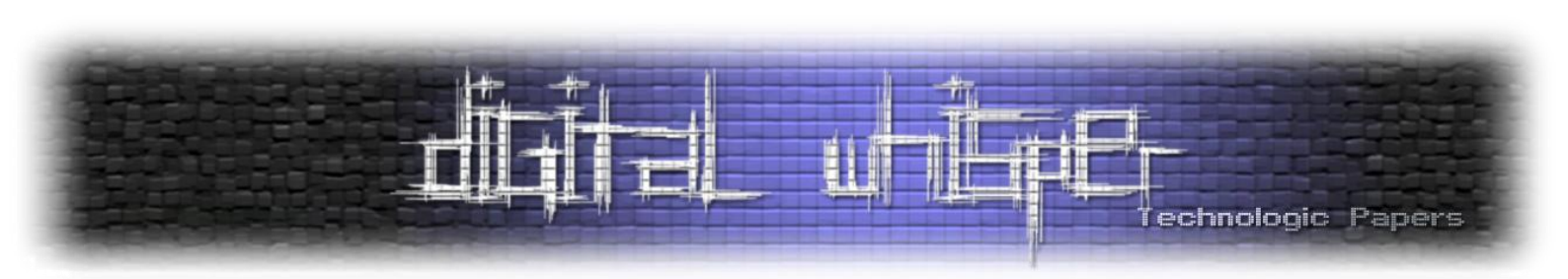


למה מומלץ לבדוק לסוס את השיניים

מאת: אפיק קסטיאל (cp77fk4r)

הקדמה

במאמר הזה אני הולך להציג מקרה שקרה בחודש האחרון. מסיבות שאציג בהמשך, אשתדל (עד כמה שאפשר) לתת כמה שפחות נתונים מזהים על המקרה, למרות שידוע לי שבעזרת גוגל תוכלו למצוא בדיוק את המקרה שאני מדבר עליו. ובכל זאת, אני מקווה שהדבר לא יפגע בחוויית הקריאה.

הכל התחיל מכניסה שגרתית למערכת אתגרי ההאקינג שאני מנהל: TryThis0ne.com באחד מסופי השבוע. אחד הפיצ'רים במערכת הוא שכל משתמש יכול לפתוח לעצמו עמוד פרופיל, לכתוב בו מידע על עצמו ולעצב אותו כמו שהוא מעוניין. בסופו של דבר על העמוד לעבור אישור של צוות האתר (גם בכדי שנוכל לשלוט בחומר שמתפרסם וגם בכדי שנוכל לוודא שלא מנסים להכניס שום קוד זדוני שיפגע בשאר המשתמשים במערכת).

כאשר נכנסתי למערכת קפצה לי התראה כי יש משתמש שערך את הפרופיל שלו והוא מעוניין שאאשר את השינוי. מכניסה לעמוד העריכה, התברר לי כי השינוי הוא הוספת הקוד הבא:

```
<meta http-equiv="refresh" content="0;URL=[illegible]"/>
```

active:0

בתחילה נראה כי מדובר בנסיון של המשתמש לעשות "Deface" טפשי בעזרת ניצול של חולשת Cross Site Scripting (שכמובן לא קיימת) ולאחר בירור עם המשתמש עלתה האפשרות שהחשבון שלו נפרץ.

הלינק מפנה לעמוד ש(בעבר היה)נראה כך:

כן, בטח, בהחלט נשמע אמין.

אישית, בלי להעליב כמובן, אני לא תופס יותר מדי מחברי קבוצת Anonymous, ואף פעם לא אמרתי שניתן להאשים אותם ביתר בגרות, אבל אני חושב שאם שמענו עליהם כל כך הרבה, סביר להניח שהם לא טפשים עד עדי כך, כך שברור לי שאין כל קשר בין העמוד הנ"ל לבינם.

באותו עמוד, לחיצה על התמונה של הלוגו של Anonymous, הובילה לעמוד באתר שיתוף הקבצים "Mediafire.com", לקובץ בינארי השוקל קצת פחות מ-1MB המכיל בשמו, בין היתר, את המחרוזת "Web Hack Pack".

פה חשדתי. ☺

כאן נשאלת השאלה: למה שבן אדם שפרץ לשרת / מערכת מסויימת יפרסם את הכלים שבעזרתם הוא עשה זאת? והתשובה לכך- לא באמת מדובר בכלים לפריצה, אלא מדובר בשיטת הפצה מעניינת של סוס-טרויאני.

הרעיון הוא שבכדי להפיץ את אותו הסוס הבחור היה פורץ לאתרים, מפנה את הגולשים לאותו עמוד, וכך לנסות לגרום להם לחשוב שהאתר נפרץ על ידי אותה קבוצה ולגרום לגולשים הסקרנים לנסות להריץ את אותו הכלי על ידי זה שהם יחשבו שמדובר בכלי האקינג מתקדמים.

מבדיקה ברשת, התברר שלאותו עמוד הפנו מספר רב ביותר של סרטוני Youtube אשר מתיימרים להסביר לגולש כיצד פורצים לשרתים ולמערכות Web אפליקטיביות. המשותף לכלל הסרטים (חוץ מהיוצר שלהם) הוא שבסופם היוצר היה מראה איך הוא מפנה את כלל הגולשים לאותו עמוד וכך בעצם, ע"י פרסום הלינק בהקשר "תמים" היה מפיץ את הכלים הזדוניים שלו.

אז הרצתי את אותה ערכה לפריצת אתרים תחת VM. התוצאות משום מה לא היו מפתיעות במיוחד... מבחינה טכנית אותו קובץ התקין Keylogger על המכונה בשם "Ardamax Keylogger". מדובר ב-Keylogger בשם "Ardamax Keylogger" שמסוגל לתקשר עם היוזם שלו במספר דרכים כגון העלאת המידע שלו לשרת FTP שנקבע מראש או דרך התחברות לתיבת אימייל ושליחת אימיילים לעצמו עם המידע מצורף כ-Attachments.

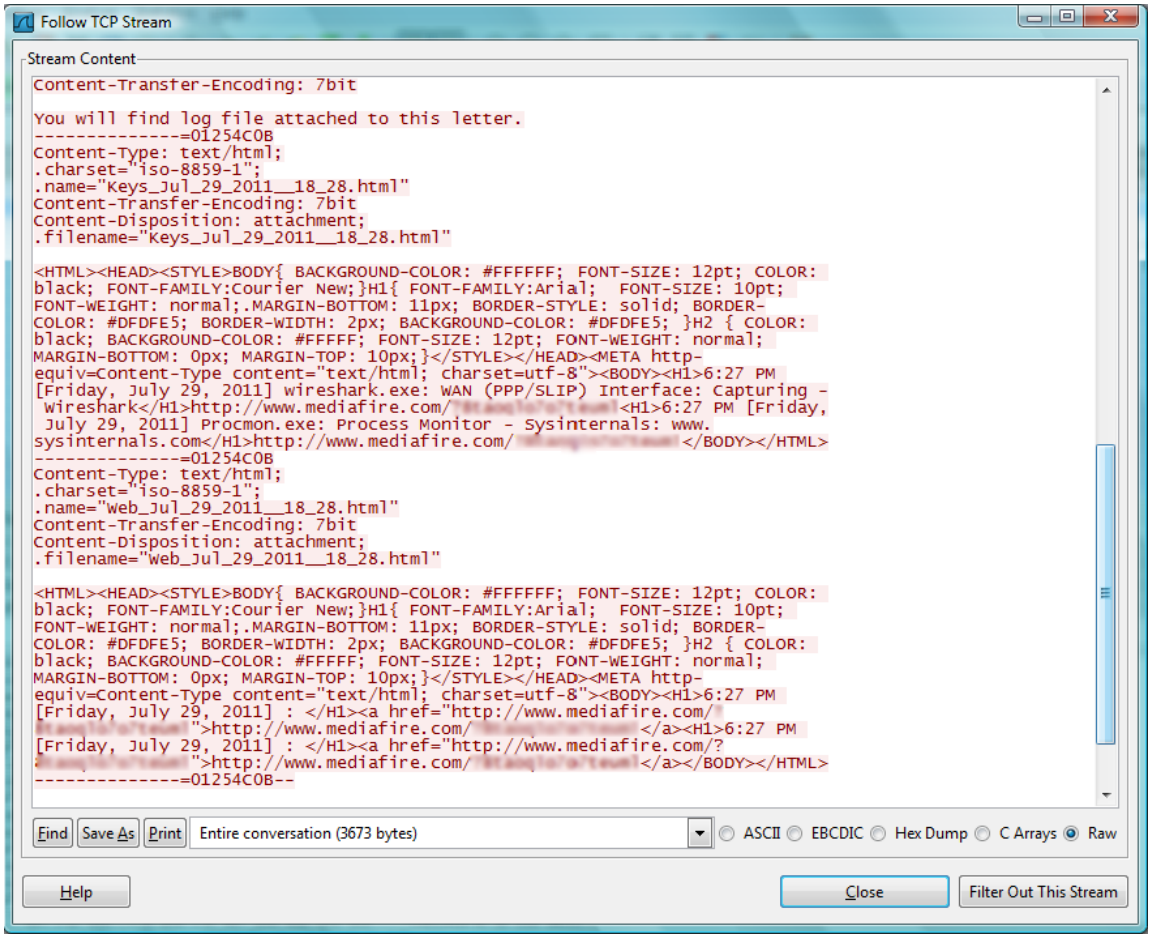
שימו לב ששתי הדרכים שהזכרתי פה מאוד בעייתיות, בשני המקרים פרטי ההזדהות לשרת הביניים נמצאים Hardcoded בקובץ שרץ בשטח. מה שאומר שאם מישהו ימצא את הכלי ויחקור אותו- בקלות רבה תהיה לו גישה לשטח האחסון שעליו מעלה הסוס הטרויאני את המידע אותו הוא אוגר.

דרך נכונה לעשות היא יצירת שני ערוצים שונים שבהם ניתן להתחבר לשרת הביניים: דרך אחת היא רק כתיבה **מבלי הצורך להזדהות** ודרך שניה היא גם כתיבה וגם קריאה, **דרך אשר דורשת הזדהות**. הסוס הטרויאני מתקשר עם שרת הביניים בעזרת הדרך הראשונה. ככה אין צורך שהוא יחזיק בפרטי ההזדהות לאותו מאגר. אגב, למי שעוקב אחר סדרת המאמרים הזאת, יוכל להזכר במאמר על Koobface, שפורסם בגליון ה-14 של Digital Whisper, שבו בדיוק נתקלנו במקרה שתולעת היו רק הרשאות כתיבה ולא הרשאות קריאה.

אז.. למה מומלץ לבדוק לסוס את השיניים?

על פני השטח הרצה של הקובץ לא עושה משהו מועיל, אבל בעזרת Process Monitor ו-Wireshark אפשר לראות בדיוק מה אותו בחור בישל לנו.

בלוגים של Wireshark ניתן לראות את ה-TCP Stream הבא:



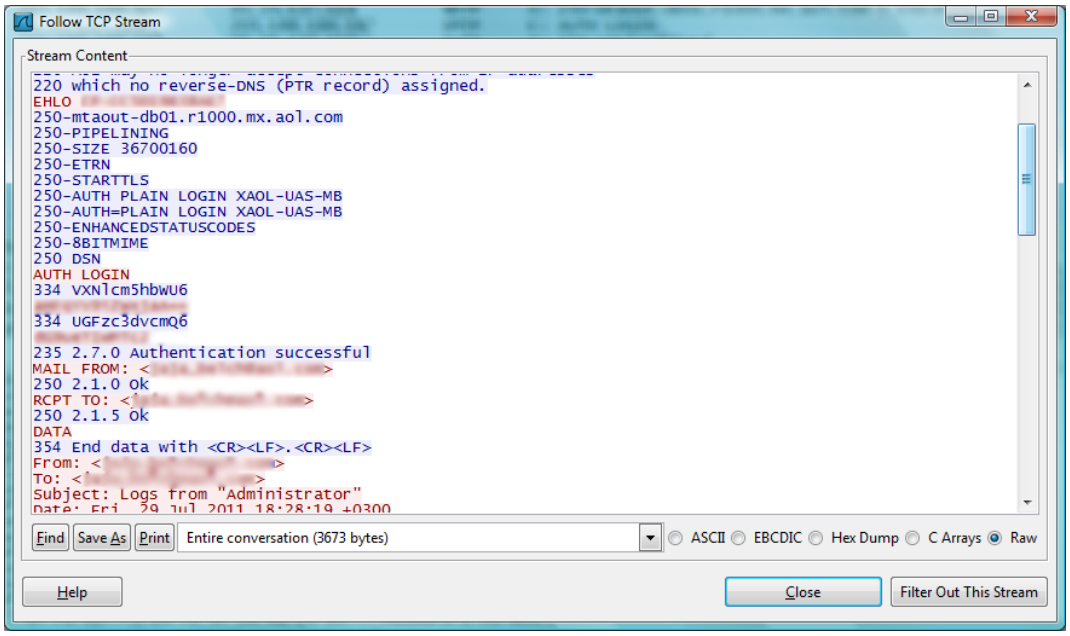
נראה שהקובץ שולח לשרת מסויים מספר קבצי HTML, אחד מהם מכיל את רשימת החלונות שהיו פתוחים בעת ההרצה:

```
<HTML><HEAD><STYLE>BODY{ BACKGROUND-COLOR: #FFFFFF; FONT-SIZE: 12pt; COLOR:
black; FONT-FAMILY:Courier New;}H1{ FONT-FAMILY:Arial;  FONT-SIZE: 10pt;
FONT-WEIGHT: normal;.MARGIN-BOTTOM: 11px; BORDER-STYLE: solid; BORDER-
COLOR: #DFDFE5; BORDER-WIDTH: 2px; BACKGROUND-COLOR: #DFDFE5; }H2 { COLOR:
black; BACKGROUND-COLOR: #FFFFF; FONT-SIZE: 12pt; FONT-WEIGHT: normal;
MARGIN-BOTTOM: 0px; MARGIN-TOP: 10px;}</STYLE></HEAD><META http-
equiv=Content-Type content="text/html; charset=utf-8"><BODY><H1>6:27 PM
[Friday, July 29, 2011] wireshark.exe: WAN (PPP/SLIP) Interface: Capturing -
 Wireshark</H1>http://www.mediafire.com/ <H1>6:27 PM [Friday,
 July 29, 2011] Procmon.exe: Process Monitor - Sysinternals: www.
sysinternals.com</H1>http://www.mediafire.com/ </BODY></HTML>
```

והקובץ השני מכיל את רשימת אתרי האינטרנט שהיו פתוחים בעת ההרצה של הכלי:

```
<HTML><HEAD><STYLE>BODY{ BACKGROUND-COLOR: #FFFFFF; FONT-SIZE: 12pt; COLOR:
black; FONT-FAMILY:Courier New;}H1{ FONT-FAMILY:Arial;  FONT-SIZE: 10pt;
FONT-WEIGHT: normal;.MARGIN-BOTTOM: 11px; BORDER-STYLE: solid; BORDER-
COLOR: #DFDFE5; BORDER-WIDTH: 2px; BACKGROUND-COLOR: #DFDFE5; }H2 { COLOR:
black; BACKGROUND-COLOR: #FFFFF; FONT-SIZE: 12pt; FONT-WEIGHT: normal;
MARGIN-BOTTOM: 0px; MARGIN-TOP: 10px;}</STYLE></HEAD><META http-
equiv=Content-Type content="text/html; charset=utf-8"><BODY><H1>6:27 PM
[Friday, July 29, 2011] : </H1><a href="http://www.mediafire.com/?
">http://www.mediafire.com/</a><H1>6:27 PM
[Friday, July 29, 2011] : </H1><a href="http://www.mediafire.com/?
">http://www.mediafire.com/</a></BODY></HTML>
```

אז לאיפה המידע הזה נשלח? אם נסתכל קצת לפני בלוגים של Wireshark, נוכל לראות את ה-Stream הבא:



אז הבינארי שלנו מבצע הזדהות אל מול שירות SMTP על השרת mtaout-db01-r1000.mx.aol.com, מדובר באחד משרתי המיילים של AOL. אישית אף פעם לא הייתה לי תיבת מייל ב-AOL, אבל שירותי SMTP זה דבר שאני מכיר.

בשניה הראשונה ניתן לחשוב שפרטי ההזדהות מוצפנים או משהו- אבל ברגע השני ניתן ישר להבין שפשוט מדובר ב-"Base64" סטנדרטי.

ניתן לראות בלוגים של Process Monitor בדיוק מה אותו בינארי עושה, אבל עצרתי כאן. הנחתי (מה שהסתבר לאחר מכן כנכון) שאותו קובץ בינארי מעלה את המידע שלו לאותה תיבת אימייל, כך שנבדוק מה עושה אותו הקובץ- פשוט נגש לתיבה ונשם נוכל לראות הכל באופן מסודר...

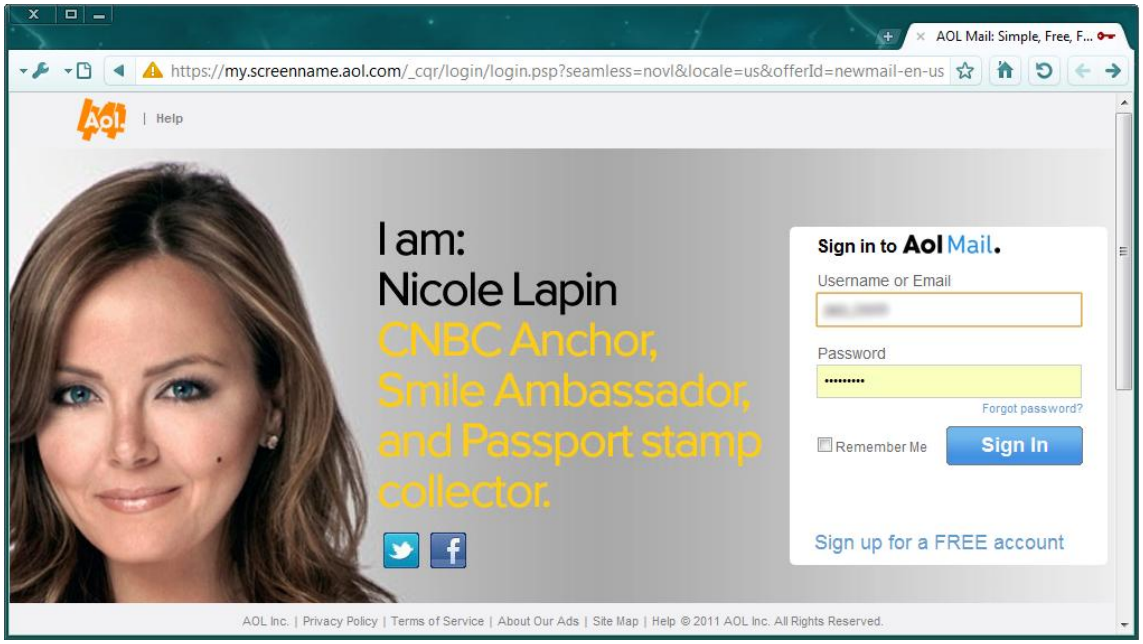
נסתכל שוב על מהלך ההזדהות לתיבה:

```
AUTH LOGIN
334 VXNlcm5hbWU6
[redacted]
334 UGFzc3dvcmQ6
[redacted]
235 2.7.0 Authentication successful
```

המרה פשוטה ל-Base64 ואפשר בקלות לאחזר את פרטי ההזדהות:

```
AUTH LOGIN
334 Username:
[redacted]
334 Password:
[redacted]
235 2.7.0 Authentication successful
```

יש לנו את שם המשתמש ואת הסיסמה. כל מה שאנחנו צריכים בכדי להכנס לתיבה:

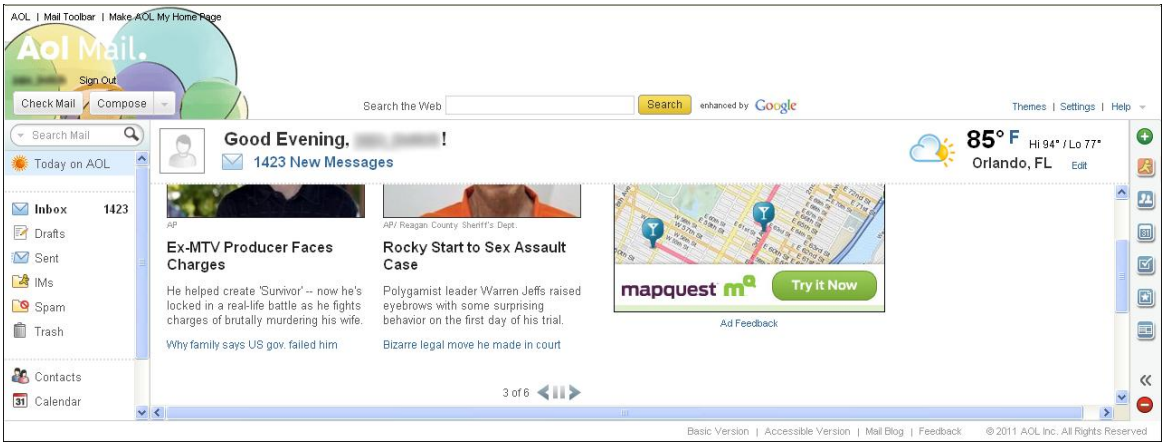


לאחר הזדהות מוצלחת ניתן היה להבין בדיוק מה שולח אותו סוס-טרויאני, חוץ ממה שכבר ראינו, ניתן היה למצוא בתיבה 1423 אימיילים שונים (והמספר עלה כל כמה דקות), שכל אחד מהם הכיל נתונים כגון:

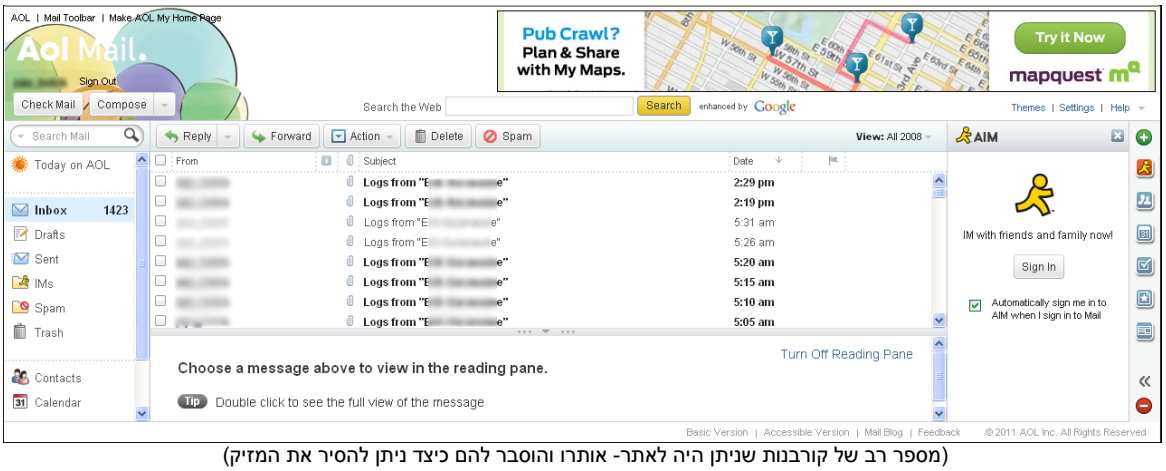
- תצלומי מסך (Print Screens)
- לוג הקשות מקלדת (Key Strokes),
- תהליכים וחלונות פעילים.
- אתרים שבהם ביקר המשתמש וכו'

מספר תמונות להמחשה (פרטים רבים יוצגו באופן מטושטש בכדי לשמור על פרטיותם של הקורבנות).

כאן ניתן לראות את כמות המיילים הנכנסים:

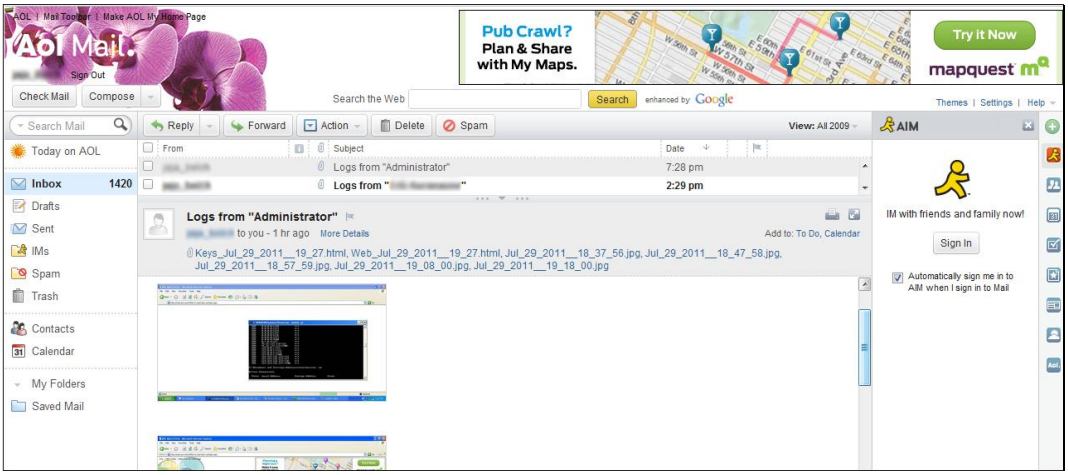


כאן ניתן לראות אימיילים שהגיעו מסוס-טרויאני שנמצא על מחשב בשם "E*** ********e":



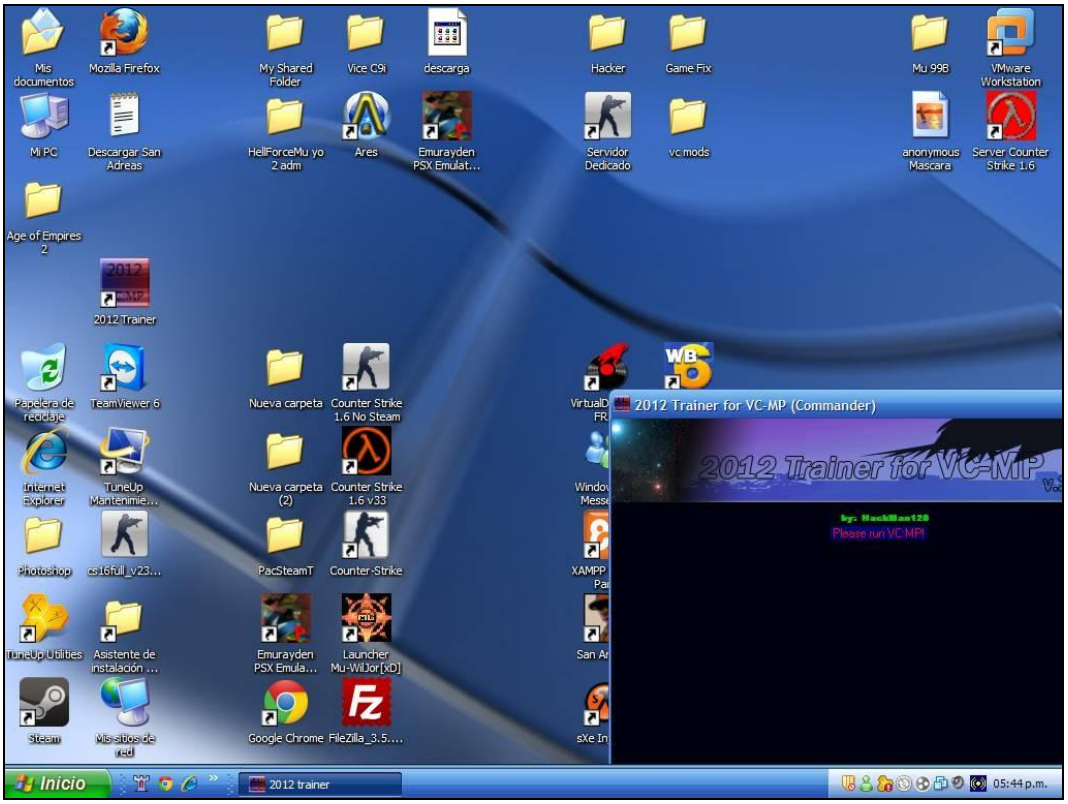
(מספר רב של קורבנות שניתן היה לאתר- אותרו והוסבר להם כיצד ניתן להסיר את המזיק)

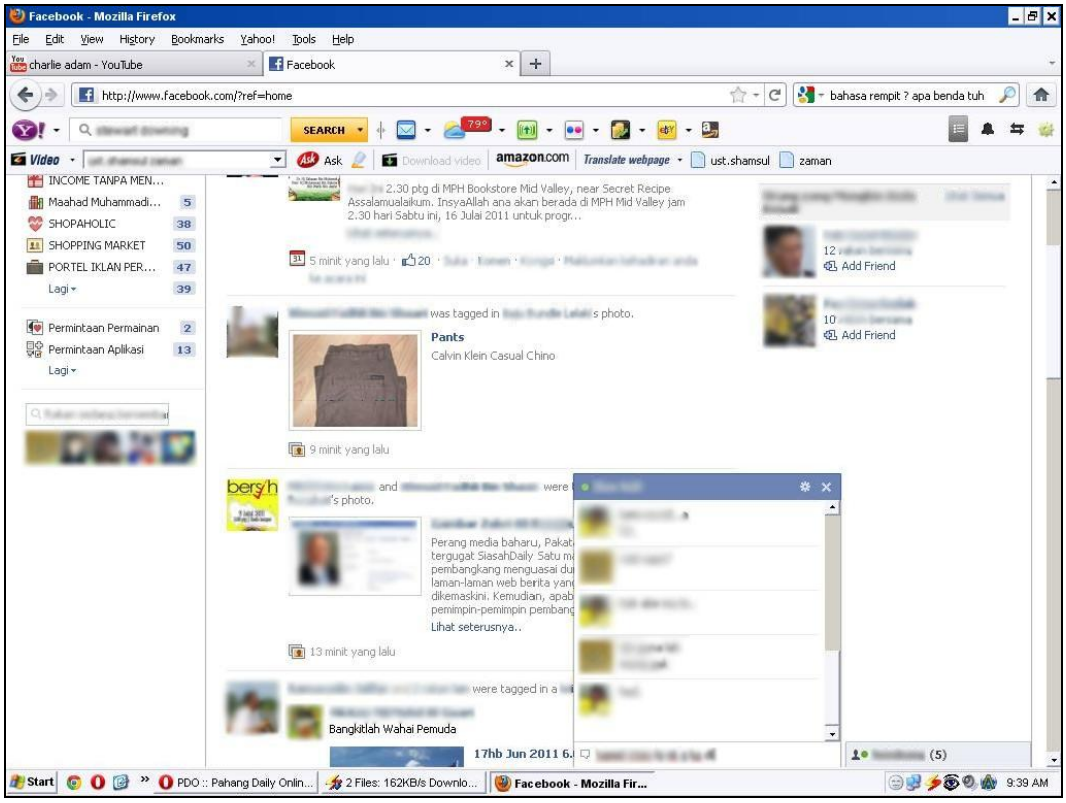
כאן ניתן לראות את תוכן של אימיילים שהגיעו לאחר ההרצה של הכלי על ה-VM שלנו!



(המיילים הספציפים שנשלחו מה-VM שלנו נמחקו מהתיבה)

התמונות הבאות הן מספר תמונות מסך שהגיעו ממחשבים שונים:


2012 Trainer for VC-MP (Commander)
2012 Trainer for VC-MP
Please run VC MP!
Inicio
2012 trainer
05:44 p.m.


Facebook - Mozilla Firefox
http://www.facebook.com/?ref=home
Pants
Calvin Klein Casual Chino
Add Friend
Bangkitlah Wahai Pemuda

ועוד ועוד... אותה תיבה הייתה מלאה בדברים בסיגנון הזה. במעבר על המיילים שהגיעו לתיבה ניתן לראות שבעל החשבון סימן בדגל-אדום (אופציה מובנת ב-AOL לסימון מיילים מעניינים/חשובים) כל אימייל שהגיע מהקורבנות שלו שבהם היה מידע עם סיסמאות לחשבונות שונים.

השבתת הטרויאן

אחרי הבנתה של איך הטרויאן המטרה שלי היתה להשבית את הכלי כדי שלא יפגע על משתמשים נוספים.

מחיפוש באימיילים הראשונים של התיבה, ניתן היה למצוא מספר נסיונות שאותו בחור ניסה על עצמו. החיפוש עלה יפה ונמצאו מספר ממצאים יפים. **ראשית**- תמונת מסך מכלי שהורץ על המחשב של בעל הכלי:

שנית- אותר לוג הקשות מקלדת ובו נצפה בעל החשבון מתחבר לחשבון המייל המקורי שלו ב-"Yahoo!".

מה עוד אפשר לבקש? ☺ עם גישה לחשבון המקורי של המשתמש הושגה נגישות לחשבון שבו אותו משתמש אחסן את עמוד ה-Deface (שהוצג בתחילת המאמר) והוחלף בעמוד אחר, שונו לו פרטי ההזדהות ואותה ספקית אחסון קיבלה מייל עם המידע על הפעולות הנעשות מאותו חשבון.

בנוסף הושגו פרטי ההזדהות לחשבון ה-Youtube שלו (החשבון שבו היו הסרטונים שהפנו לדף עם הטרויין) וגם שם שונו פרטי ההזדהות. שבסופו של דבר הכלי (לפחות הנוכחי) נוטרל. כמובן שאף אחד לא מבטיח לנו שמחר אותו ילד לא יתעורר בבוקר ויקים הכל מחדש תחת חשבונות חדשים...

האימייל עם פרטי ההזדהות לשטח האחסון שבו אוחסן עמוד ה-Deface:

AWARDSPACE.COM

Web Hosting, Domain Names & Online Services

Successful Signup!

PLEASE PRINT THIS EMAIL FOR YOUR RECORDS AND READ IT THOROUGHLY!

Dear Valued Customer,

Thank you for purchasing web hosting with awardspace.com.

Hosting Information
Hosting Package: FREE Web
Client ID: [redacted]
Login email: [redacted]
Password: [redacted]

Domain Names
If you have purchased domains ragistration/transfer or you have existing domains, please add them inside your Domain Manager section. Additionally you should set the following name servers for all domains, except for the domains that has been registered with us.
Nameserver 1: ns5.awardspace.com
Nameserver 2: ns6.awardspace.com

Website Upload
Make sure you upload your files to the domain/subdomain directory on the server; otherwise they will not be visible on the Internet. Also, please be sure that your homepage is saved as an "index" file e.g., index.php, index.html, index.htm, etc. We suggest you download some advanced ftp client to manage your files quickly, or use the File Manager inside the Hosting Control Panel.

FTP Account Information
Your default FTP account information:

FTP Hostname: You should first add a domain/subdomain in your Hosting Control Panel.
FTP Username: [redacted]
FTP Password: [redacted]
You can manage your FTP accounts from the FTP Manager section.

E-mail Account Information

התחברות לחשבון עם התוכן הפוגע:

TIP: Connecting to the FTP server and upload your website, you should have FTP hostname (domain/subdomain).

File Manager Help!

Current folder: /home/www/

Warning: Directory protection for your hostnames is **disabled** - you can delete them by accident.
(You CAN delete hostname directories and upload files outside them) Directory protection: Enable

Delete Rename Move To Permissions: 755 Recursive Set

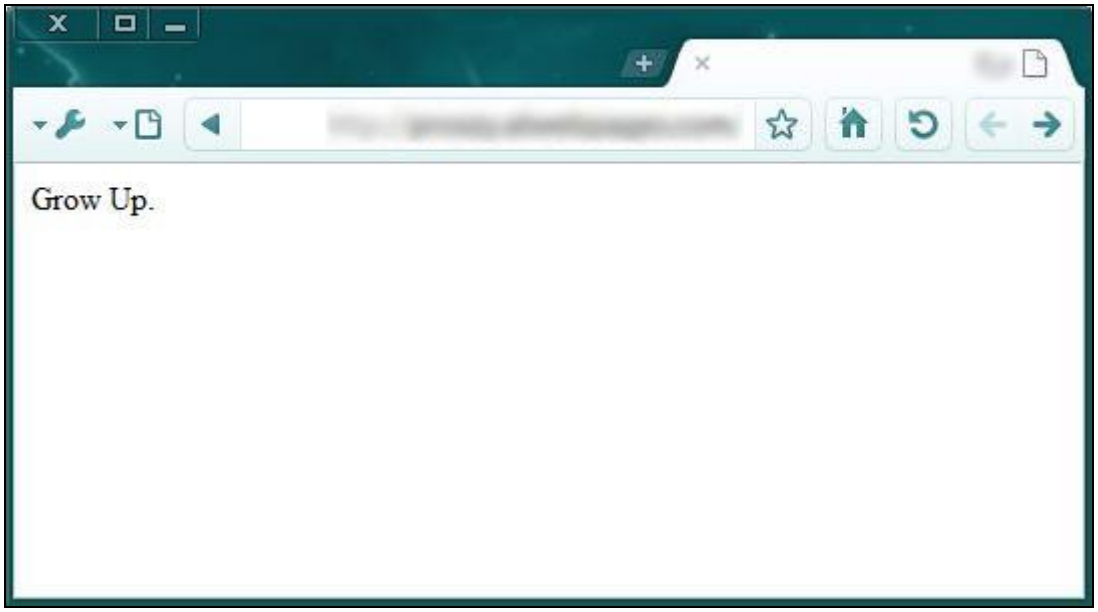
Options	Name	Size	Type	Date Modified	Permissions[?]
	.	-	Folder	Jan 31 19:15	drwxr-xr-x
	..	-	Folder	Jan 31 19:15	drwxr-xr-x
	[redacted]	-	Folder	Jul 8 22:02	drwxr-xr-x
Select All	Total: 1 folders				

Current folder: /home/www/

Warning: Directory protection for your hostnames is **disabled** - you can delete them by accident.
(You CAN delete hostname directories and upload files outside them) Directory protection: Enable

Delete Rename Move To Permissions: 755 Recursive Set

והתוצאה... עמוד Deface חדש ובלתי פוגע ☺



סיכום

כאן פחות או יותר הסיפור נגמר. את המטרה שהצבתי לעצמי- השגתי. אומנם אני לא בטוח שכעת האינטרנט הוא מקום בטוח לגלוש בו, אבל לפחות אני יודע שלא העלמתי עין, ואם בזכות הפעולה הזאת הצלחנו להציל עוד כמה משתמשים תמימים- את שלנו עשינו.

בקשר לחוקיות הדברים, ברור לי שמדובר בפעולות אפורות, וכששאלתי עורך-דין המתעסק בנושא האם פרסום הדברים כדאי- קיבלתי תשובה שלילית. ובכל זאת פרסמתי את הדברים, והנה הם לפניכם. הדבר נעשה אך ורק בכדי להראות לכם, הקוראים, שניתן להשיב לאותם סקריפט-קידיז שמנסים לפגוע במשתמשים תמימים ברחבי האינטרנט. מאמר זה אינו מהווה המלצה לביצוע פעולות דומות מצדכם - כאמור מדובר בתחום מאוד אפור.