Digital Whisper
Technologic Papers

שובם של ה-Web Bugs

מאת יניב מרקס

הקדמה

אחת הטכניקות בהן חברות תוכן (או לחילופין - ספאמרים) השתמשו בעבר על מנת לעקוב אחר הגולשים באינטרנט הינה טכניקת ה-Web bug. טכניקה זו הינה ישנה וכמעט לא נמצאת בשימוש כיום, זאת מפני שספקיות הדואר האלקטרוני חסמו, כברירת מחדל, את הדרכים הנפוצות אותן היה ניתן לנצל לטובת מימוש טכניקה זו, דרכים כגון טעינת תמונות או אובייקטים דומים בעת קריאת אימייל מסויים (אלא אם כן המשתמש מכיר את שולח המייל, ואז באופן מודע בוחר להציג את המייל עם כלל האובייקטים המקושרים אליו).

לאחרונה, שמתי לב כי ישנן מספר ספקיות דואר אלקטרוני שאינן אוכפות את חסימת האובייקטים בכל המקרים ובכך מאפשרים שוב שימוש בטכניקה זו (דוגמאות יוצגו בהמשך המאמר). לפיכך, חשוב לבדוק האם שרת המייל שבו אתם משתמשים (ולא משנה אם אתם עובדים עם POP3 או HTTP) חוסם אובייקטים כברירת מחדל על גבי הפלטפורמה בעזרתה אתם עובדים (מחשב, smartphone וכו').

בגדול, שימוש בטכניקה זו מאפשר לדעת האם אימייל שנשלח לתיבת מייל מסויימת נקרא או לא. לפני שנצלול קצת, להלן שימושים אפשריים:

- בדיקה האם יש מישהו שאכן משתמש בכתובת מייל מסוימת (בד"כ ספאמרים ישתמשו למטרה זו).
- מעקב אחר משתמשים (בד"כ חברות פרסום תשתמשנה למטרה זו):
  - האם ומתי המשתמש קרא מייל מסוים.
  - מהיכן המשתמש קרא את המייל (כתובת IP).
  - האם ולמי המשתמש שרשר את המייל.
  - האם המשתמש כבר ביקר באתר מסוים.
  - באיזה דפדפן המשתמש משתמש (User-Agent).
- טעינת קוד מפגע משרת מרוחק.

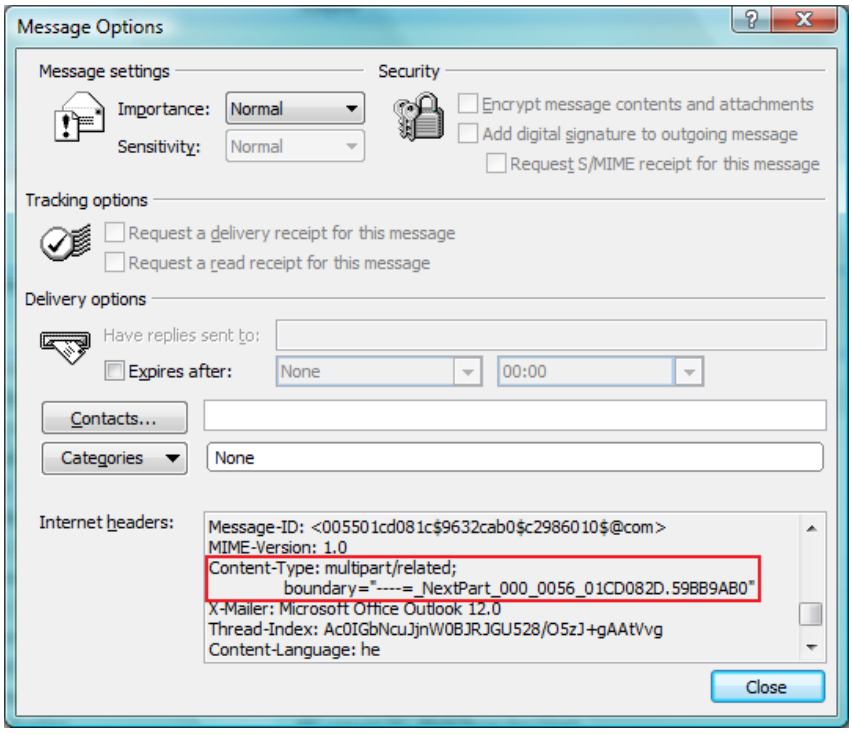
הטכניקה עצמה

רוב המיילים הנשלחים היום מכילים בנוסף למלל עצמו (text/plain), תמונות ואובייקטים נוספים. בדרך כלל, כאשר תקראו מייל הכולל בתוכו אובייקטים, תופיע הודעה בתחילת המייל המציינת כי הודעה זו כוללת בתוכה אובייקטים שנחסמו כברירת מחדל ע"י השרת, לדוגמא, ההודעה ב-Gmail:

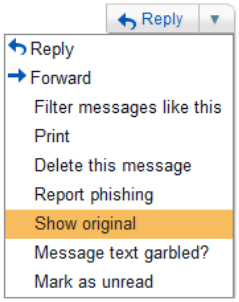
בדרך כלל (הכל כמובן תלוי במימוש של ספקית תיבת המייל), יוצג תוכן תג ה-ALT, במידה והוגדר כזה.

כמו כן, ניתן לדעת לפי ה-Mail Headers, כי המייל מכיל אובייקטים על ידי קריאת הערך של השדה Content-Type. על מנת לקרוא ערך זה, ניתן לבצע את הפעולות הבאות:

- **Mail Client (לדוגמא Microsoft Outlook):** ניתן לבדוק מה רשום בשדה Content-Type ע"י לחיצה בעזרת מקש ימני על המייל ובחירת "אפשרויות" (Options) בחלון התחתון תחת Internet headers קיים שדה Content-Type:



- **Webmail:** מאחר וכל אתר Webmail בנוי אחרת, לא ניתן לציין כיצד למצוא שדה זה בכל אתר, אבל בד"כ יש לחפש בתפריט "Options" ומשם להגיע ל-Internet Headers, לדוגמא, ב-Gmail:



ושם:

```
MIME-Version: 1.0
Received: by 10.182.27.74 with HTTP; Fri, 30 Mar 2012 06:20:06 -0700 (PDT)
Date: Fri, 30 Mar 2012 16:20:06 +0300
Delivered-To: empty0page@gmail.com
Message-ID: <CAAqOd6dEkdZrVwPJEvm2KV+nrSsgfmD=uE=RHcoA=gUPvLJa5w@mail.gmail.com>
Subject: x
From: cp77fk4r <empty0page@gmail.com>
To: "Empty0page@gmail.com" <empty0page@gmail.com>
Content-Type: multipart/alternative; boundary=90e6ba1ef338f98a5a04bc75b23e

--90e6ba1ef338f98a5a04bc75b23e
Content-Type: text/plain; charset=ISO-8859-1

[image: Google]

--90e6ba1ef338f98a5a04bc75b23e
Content-Type: text/html; charset=ISO-8859-1

<div dir="ltr"><img src="http://www.google.co.il/logos/classicplus.png" height="95"
width="275" style="padding-top:112px;border-width:0" id="hplogo" alt="Google"></div>

--90e6ba1ef338f98a5a04bc75b23e--
```

בכל מקרה, על מנת להשתמש בטכניקת ה-Web Bug, נדרש ליצור מייל הכולל תמונות גלויות, כדי לא לעורר חשד אצל המשתמש, וקישור לקובץ תמונה אחת נסתרת / שקופה בסיומת jpg. ובגודל מינימלי, ע"מ להקטין את התקורה של טעינת המייל. לדוגמא:

```
<img src="http://www.digitalwhisper.co.il/invisible.jpg">
```

על מנת למפות משתמש מסוים, יש להוסיף קישור לקובץ תמונה נסתר, כך שהקישור הינו ייחודי לאותו משתמש:

```
<img src=" http://www.digitalwhisper.co.il/invisible.jpg?id=12eff7">
```

במידה והשרת לא יחסום את הצגת או טעינת תמונות, כאשר משתמש מסוים יקרא את המייל המכיל קישור, תתבצע פנייה לאותה כתובת Web המופיעה במייל ע"ג פרוטוקול HTTP. בכך יוכל יוצר המייל

לדעת שקורא המייל אכן קיים וקרא את ההודעה (כי רק לו יש קישור לאותה כתובת ייחודית באתר מסוים השייך ליוצר המייל). בנוסף יוכל יוצר המייל לקבל פרטים נוספים על המשתמש, המועברים כחלק מפרוטוקול ה-HTTP (כגון: User-Agent) על ידי הסתכלות בלוגים של שרת ה-HTTP שברשותו:

```
*.*.*.* - - [30/Mar/2012:17:23:53 +0300] "GET /invisible.jpg?id=12eff7
HTTP/1.1" 200 211637 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.0; en-
US) AppleWebKit/533.4 (KHTML, like Gecko) Chrome/5.0.375.70
Safari/533.4"
```

שימו לב כי בחלק מאתרי ה-Webmail, גם כשאתם קוראים מייל מסוים, הדפדפן טוען באופן אוטומטי מספר מיילים נוספים, ע"מ לחסוך זמן בהורדת אותם מיילים, מתוך הנחה כי תרצו לקרוא גם את המיילים הבאים. באתרים אלו, ה-Web Bug מופעל גם כאשר טרם קראתם את המייל המכיל טכניקה זו או כאשר בכלל קראתם אימייל אחר.

דוגמאות

זה המקום לציין, כי הדוגמאות המופיעות במאמר זה נכונות לתאריך כתיבת המאמר (מרץ 2012). כמו כן, יש לציין שאין כוונה להביע ביקורת ו/או דעה על הספק, אלא להעלות את המודעות לנושא זה. בנוסף, ככל הנראה, ישנן דוגמאות נוספות שאינן מופיעות פה. הנכם מוזמנים לשלוח לי במייל הודעה על ממצאים נוספים שלכם.

דוגמא א':

גלישה ל-Webmail של חברת וואלה! (http://newmail.walla.co.il), מאפשר קריאת מיילים כברירת מחדל ללא חסימת אובייקטים.

דוגמא ב':

ב-iPad, ישנה אפליקציית דוא"ל המגיעה כחלק ממערכת ההפעלה המאפשרת גישה לדוא"ל של המשתמש (מדובר ברשימה של מספר ספקי דוא"ל פופולריים, כגון: Yahoo, GMail וכו'), שימוש באפליקציה זו חושף את המשתמש למתקפה זו מפני שהיא מציגה אובייקטים אלו כברירת מחדל ללא בקשת אישורו של המשתמש.

סיכום

כמו שניתן לראות, מדובר בטכניקה ישנה, אך עדיין קיימת בחלק מהמקרים. כיום המודעות לכך קטנה מאחר והאובייקטים המקושרים למייל, חסומים כברירת מחדל, אולם מאחר וישנן דוגמאות לפיהן האובייקטים אינם חסומים כברירת מחדל, כדאי להגביר את המודעות בנושא זה.

על המחבר

יניב מרקס הנו מומחה לאבטחת מידע העובד בחברת אלתא מערכות בע"מ. הערות / הארות ניתן לפנות בדוא"ל: yanivmar@yahoo.com