על פי פרסומים זרים

מאת: אפיק קסטיאל (cp77fk4r)

[במקור: www.riencha.com]

הקדמה

Malvertising היא שם של טכניקה רבת עוצמה, שבה עושים שימוש גופים בעלי כוונות זדון ברחבי האינטרנט על מנת להפיץ מזיקים תוך כדי שימוש בפלטפורמות הפרסום השונות. Malvertising היא שילוב של המילים Malware ו-Advertising. מדובר בתעשייה לא קטנה שעם הזמן רק תופחת ותופחת, מי שמתעניין בנושא, יכול להעיד שלאט לאט אנו שומעים יותר ויותר על שימוש בטכניקה זו.

חשוב להבין שכאשר משתמשים בביטוי Malvertising לא מתכוונים ל-Spam כמו שהוא מוכר כיום - משלוח דוא"ל פרסומי בכמות מאסיבית בכדי לפרסם אתר / מוצר. למרות שלפעמים, Spam המתקבל במייל יוכל להיות חלק מרכזי בקמפיין Malvertising מתגלגל.

לפני הכל, איך זה עובד?

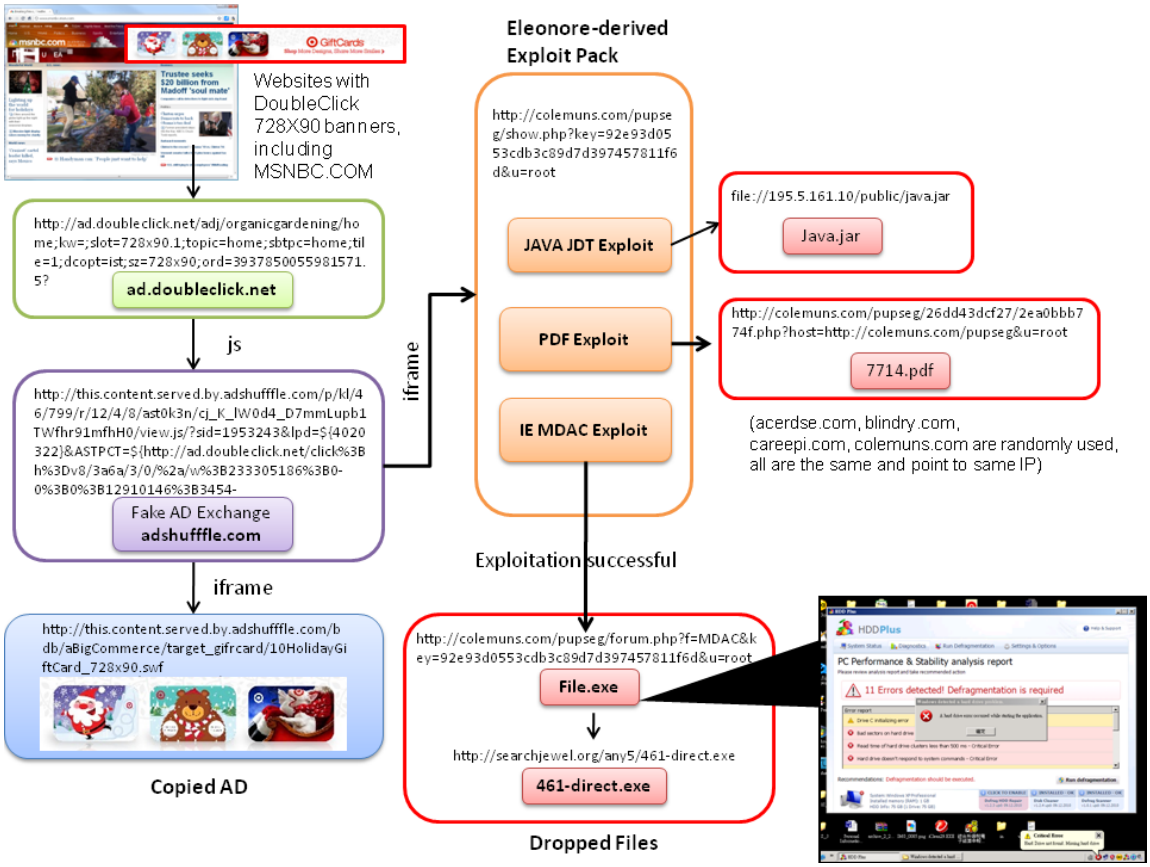
זה לא סוד שהכסף והכח של גופי הפשיעה האינטרנטיים הוא נגזרת ישירה של גודל רשת ה-Botnets שיש ברשותה, ככל שיש יותר מחשבים תחת שליטתה, כך יגדלו הרווחים שלה. גופים אלו ישקיעו הרבה בכדי להפיץ את ה-Botnet התורן שיש ברשותה. בגליון ה-26 של Digital Whisper ראינו איך עובד עולם

ה-Browser Exploit Kits, ושאחד הפאקטורים במשוואת ההצלחה שלו הוא כמות התעבורה הנכנסת לאותם אתרים זדוניים.

הרעיון המרכזי הוא ניצול פלטפורמת פרסום מרכזית, או מספר כאלה, בדרך כלל כזאת המשתלבת כצד שלישי באתרים שונים בכדי לפרסם עמודים בעלי שתי זהויות שונות - זהות תמימה וזהות זדונית:

- **הזהות התמימה** תפקידה למנוע זיהוי של העמוד כעמוד זדוני, והצגתו כרלוונטי אל מול גוף הפרסום. בדרך כלל, זהו יהיה מצבו של העמוד, גולש שיכנס לעמוד זה לא יפגע.
- **הזדהות הזדונית** - מדובר בכמעט אותו עמוד כמו הזהות התמימה, חוץ מתוספת של מספר שורות קוד שתפקידן הוא להעביר את הגולש ל- Exploit Kits. העמוד יחשוף את אותן שורות קוד רק כאשר הוא יוגדר כ-"מופעל", ורק כאשר יגלשו אליו גולשים עם פוטנציאל הדבקה גבוהה (גולשים המשתמשים ברכיבים אשר אליהם קיימים אקספלויטים בערכת ההדבקה).

כאמור, המטרה בסופו של דבר היא להגדיל את נפח התעבורה לאותן ערכות הדבקה, ניתן לראות את הרעיון בתרשים הבא:



[במקור: http://blog.armorize.com/2010/12/hdd-plus-malware-spread-through.html]

מעל לפני השטח לגולש אכן מוצגות פרסומות רלוונטיות ותמימות, אך מתחת לפני השטח ניתן לראות כי אותו מנוע תמונות גורם לדפדפן לבצע פניות לבקשת תוכן זדוני מהדומיין של "adshufffle.com" המפנה לחבילת האקספלויטים בשם "Eleonore" המותקנת על הדומיין colemuns.com. אותה חבילה תנסה מספר וקטורי תקיפה על הגולש, במידה ואחד מהם יצליח - יורד הקובץ הזדוני ויהפוך את מחשבו של הגולש לחלק מרשת ה-Botnets של הארגון אשר עומד מאחורי קמפיין זה.

אפשר לראות כי עד שקמפיין זה לא נתפס והכונס למאגרים של Safebrowsing (אתם מוזמנים לגלוש ל-adshufffle.com) לא היה ניתן לדעת כי הוא אתר מדביק, חוץ מהשם, שנראה כי הוא נסיון לחכות את adshuffle.com. פלטפורמת הפרסום, במקרה שלנו היא doubleclick.net - יכולה לראות את ההפנייה ל-adshufffle.com, אך היא אינה מבצעת מעקב יום-יומי אחר התוכן המוצג שם, כך שכאשר מתבצעות בדיקות התוכן לדומיין adshufffle.com, הוא יחזיר תוכן רלוונטי פרסומי ולא מדביק, מבחינתה- אין שום סיבה לחשוש ממנו.

פלטפורמות פרסום צד שלישי, אלו אשר משתמשים מפרסמים צד שלישי באתר מסויים הם אחד המתפסים העיקיים בעולם ה-Malvertising, הדוגמא שהוצגה קודם לכן, עם DoubleClick ו-ADShufffle נצפתה גם תחת פלטפורמת הפרסומות של MSN, וקמפיינים דומים נראו תראו תחת Google Ads, Yhaoo, Fox, Clicksor, SpeedTest, NY Times ועוד.

ניצול מערכות ניהול פרסומות ל-Malvertising

חוץ מניצול של פלטפורמות פרסום המתבססות על תוכן מספקי תוכן צד שלישי, קיימת מגמה עולה של שימוש בפלטפורמות לניהול פרסום אירגוניות, כגון OpenX.

הרעיון מאחורי מערכת ניהול הפרסומות של OpenX הוא להפריד את תוכן הפרסומות מתוכנו הטבעי של האתר. ניתן ליישם בעזרתה פרסום על-ידי ספקי פרסומות או בכדי לפרסם פרסומות של הארגון עצמו-באתר של הארגון, אם מדובר באתר גדול ומסועף, הרי שהפרדת התוכן הפרסומי והתוכן הטבעי של האתר הוא צעד חכם, והטמעת מערכת לניהול אותו תוכן פרסומי - הוא צעד חכם עוד יותר. לאחר שהטמענו את המערכת לניהול פרסומות באתר וקבענו היכן נרצה למקם את הפרסומות באתר (פעולה הכרוכה בהוספת שורות קוד בודדות לקוד המקורי של האתר), נותר לנו רק להכנס למערכת הניהול ולקבוע את הפרמטרים השונים - אילו פרסומות נרצה למקם באילו עמודים, לכמה זמן, האם הם יתחלפו, נוכל לבצע מעקב אחר אילו פרסומות משכו יותר גולשים, באילו עמודים וכו'. במידה ונרצה לשנות את הפרסומות נעשה זאת דרך מערכת הניהול ולא נאלץ לשנות כלום בקוד המקורי של האתר.

מדובר ברעיון שיכול לקצר את כל תהליך העבודה עם הפרסומות, אך מדובר גם בסיכון - אם לא נדע לשמור על המערכת בצורה בטוחה, היא תוכל לשמש גופי פשיעה ולפעול נגנו. מערכות אלו הן מטרה נוחה מאוד לתוקפים, מפני שמדובר בקוד חיצוני, ולפעמים גם בשרת נפרד משרתי הארגון, מה שבדרך כלל (באופן טבעי) הופך אותו למטרת פריצה קלה יותר משרתי הארגון.

במידה ותוקפים אכן יצליחו לפרוץ למערכות בסגנון זה, תהיה להם היכולת לשלב קוד עויין בגוף הפרסומות הרלוונטיות או אף להשתול פרסומות משלהם. לגולש התמים פרסומת שתופיע באתר רלוונטי תחשב רלוונטית אף היא.

מחקר שבוצע לפני פחות מחצי שנה על ידי הצוות של Armorize.com, שהתבצע עקב גל פריצה לשרתי OpenX ע"י קבוצת האקרים, גילה כי הדבר בוצע על ידי ניצול של חולשה להעלת תמונות באחד מהפלאגינים הקיימים במערכת OpenX. ניצול של חולשה זו איפשר להשתלט על המערכת לתוקפים להשתלט גם על שרתי ה-OpenX המעודכנים ביותר.

החולשה התגלתה בפלאגין בשם "OpenX Video Plugin". לפי המחקר שפורסם, היו התוקפים בודקים תחילה האם הקובץ "ofc_upload_image.php" במיקום: "www/admin/plugins/videoReport/lib/ofc2".

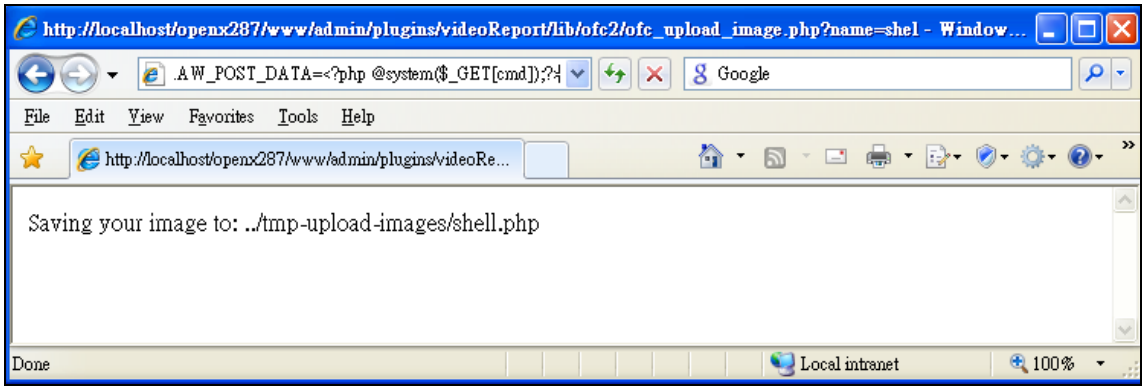
במידה וכן- הדבר מעיד כי הפלאגין מותקן על השרת.

לאחר מכן, התוקף היה שולח את הבקשה הבאה:

```
http://victim.com/www/admin/plugins/videoReport/lib/ofc2/ofc_upload_imag
e.php?name=shell.php&HTTP_RAW_POST_DATA=<?PHPCODE?>
```

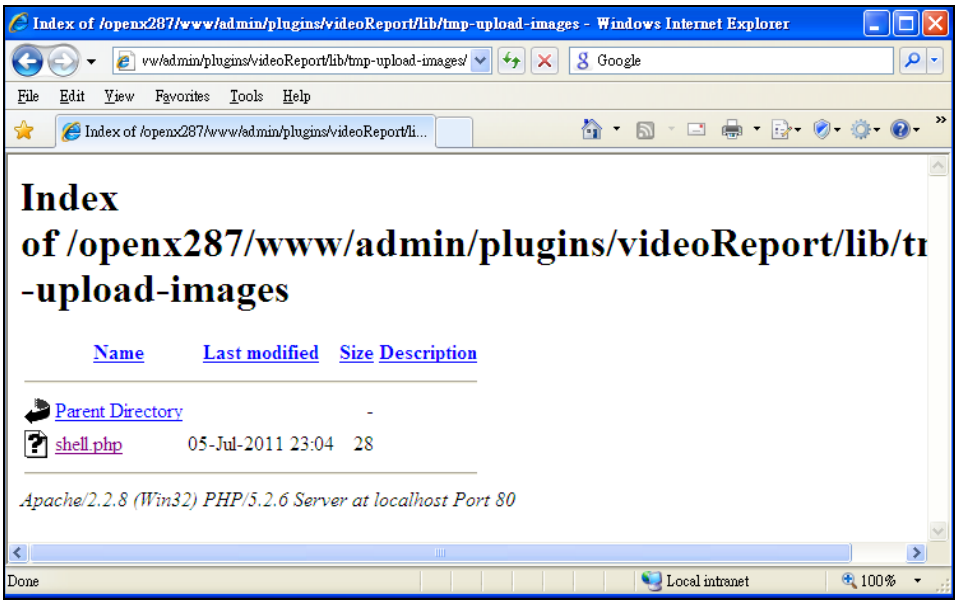
תפקידה היה להשתמש בפלאגין להעלת התמונות (שא'- לא היה דורש הזדהות, וב'- לא היה מוודא כי אכן מדובר בתוכן המרכיב תמונה) לטובת העלאת WebShell לשרת ה-OpenX.

במידה ואכן מדובר בפלאגין החשוף לחולשה זו, ההודעה הבאה הייתה מתקבלת:



[במקור: http://blog.armorize.com/2011/07/openx-hacked-by-dyndns-malvertising.html]

ואכן, הפלאגין היה יוצר "תמונה" בתיקיה שנקבעה:



[במקור: http://blog.armorize.com/2011/07/openx-hacked-by-dyndns-malvertising.html]

לאחר העלאת ה-WebShell, התוקף היה יכול לשלוף את סיסמאותיהם של מנהלי המערכת, להתחבר בשמם ולהכניס את התוכן המפנה ל-Exploits Kit בפרסומות המוצגות באתר. בגל תקיפות אלו, נתקפו עשרות אתרים של חברות שונות, וכולן הופנו את הגולשים באתרים הנגועים לערכות התקיפה של קבוצת ההאקרים העומדת מאחור תקיפות אלו.

Malvertising בחסויות לתוספים לדפדפנים

כיום כמעט לכל דפדפן קיימים תוספים אשר מאפשרים למפתחים השונים להרחיב את יכולות הדפדפן, תוספים אלו לעיתים מפותחים תחת חסותה של חברה זו או אחרת, הדבר בדרך כלל מתבטא בפרסומות שיופיעו בעת השימוש בתוסף באתרים מסויימים. הדבר כמובן תלוי בתוסף, אך ברב המקרים הפרסומות יופיעו במקום הפרסומות באתרים אליהם גלשנו ולעיתים בנוסף אליהן.

פעולה זו מתבצעת על ידי התוסף, המכיל קוד שתפקידו לזהות את הגלישה לאתר שנקבע מראש, לזהות את הקוד שאחראי על הצגת הפרסומת ולהחליפו בקוד שיטען פרסומת משרת הפרסומות של נותנת החסות. בכדי לא לפגוע בתצורתו המקורית של העמוד, הפרסומת תופיע במקום הפרסום המקורי באתר אליו גלשנו - דבר שבפירוש פוגע בהן, מבחינת המפרסם באתר המקורי, הפרסומת שלו לא נטענה, והגולש לא צפה בה, כך שכסף לא יזרום לחברה המפרסמת. ובמקום זאת יזרום ליותר התוסף או לחברה נותנת החסות.

נכון לכתיבת שורות אלו, לא נצפה שום ניצול של מנגנון זה בכדי לטעון תוכן זדוני, אך מדובר במנגנון שאם השימוש בו יצבור תאוצה, ומפיצי התוכנות הזדוניות יראו כי שווה להשקיע בניצולו, קיים סיכוי שתוספים תמימים יתהפכו, ואז גם השימוש בתוסף תמים יוכל להיות קטלני ביותר.

דוגמא פעולה זו עובדה ניתן לראות בקישור הבא:

http://stopmalvertising.com/malvertisements/firefox-add-on-and-google-chrome-extensions-hijacked-by-sponsored-ads.html

Malvertising לצרכים נוספים

עד כאן ראינו כי ארגוני פשיעה שונים עושים שימוש בפרסומות בכדי להתקין מזיקים על מחשבי הגולשים, במקרים שונים נצפו מטרות בעלי אופי דומה, אך שונות לחלוטין, כגון שימוש בפרסום בכדי לבצע מתקפות DDoS על אתרים שונים.

פעולה זו מתבצעת כמו שראינו על ידי החלפת הפרסומות הטבעיות באתר בפרסומות שונות, אך במקום לנסות להתקין על הקורבן קוד זדוני פרסומות אלו מכילות קוד זדוני (קוד Flash בעיקר) שתפקידו לגרום מתקפת DoS אל מול אתרים שונים, במידה ומדובר באתר בעל תעבורה נרחבת, האתר שהוצב כמטרה יהיה תחת מתקפת DDoS כאשר התוקפים הם גולשים תמימים שאינם יודעים שנוצלו בכדי לבצעה.

דוגמא טובה למקרה כזה הוא האתר stopmalvertising.com (שבאופן אירוני מתעסק בניסיון לאיתור לעצירה של מתקפות מבוססות פרסום), שבתאריך ה-21/07/11 היה נתון תחת מתקפת DDoS משלושת הכתובות הבאות:

- data-ero-advertising.com
- flatfee.ero-advertising.com
- www.ero-advertising.com

נושא זה לא נבדק, אבל ככל הנראה לשלושת האתרים הללו מאגר פרסומות משותף, כך שבמידה והוא נפרץ ניתן להבין למה שלושתם השתתפו במתקפה זו.

סיכום

כמו שניתן לראות, מדובר בנושא בעל פוטנציאל נזק לא קטן, נכון להיום מדובר תמיד בגלים קטנים, אך נראה כי גם אלו מספיקים בכדי ליצור רעש ונזק רב. נראה כי ארגונים רבים לא מודעים לנושא זה, וארגוני פשיעה רבים עושים שימוש בו לצרכיהם האישיים. נקווה שבעתיד הקרוב המודעות לנושא זה תגבר ונראה כי השימוש בפרסום באינטרנט ינותב לטובה.

מקורות

- http://stopmalvertising.com
- http://blog.armorize.com
- http://www.zdnet.com
- http://cve.mitre.org
- http://news.cnet.com