גירסה 1.00 - 4.5.2003

NTFS Alternate Data Streams

ניר אדר

Nir Adar

Email: underwar@hotmail.com

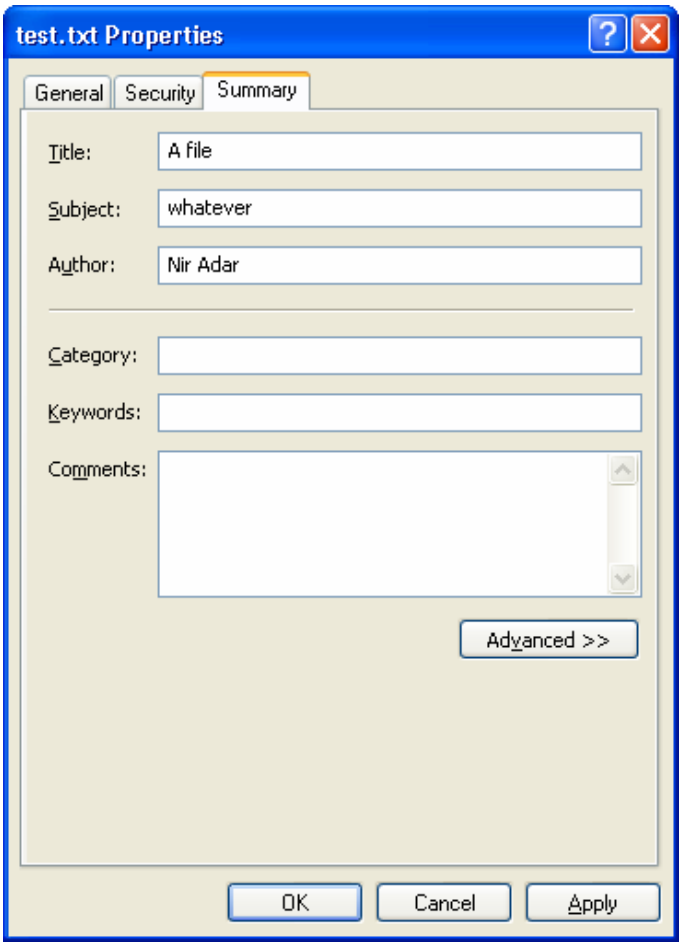
Home Page: http://underwar.livedns.co.il

אנא שלחו תיקונים והערות אל המחבר.

NTFS Alternate Data Streams

רקע

Alternate Data Streams – ערוצי מידע חלופיים – הוצגו על ידי חברת מיקרוסופט בשנת 1990.
בעזרתם יכולה מערכת הקבצים NTFS לשמש כשרת קבצים עבור מחשבי מקינטוש על ידי מתן שירותים הדרושים למקינטוש לניהול קבציו. מחשבי מקינטוש משתמשים בערוצים חלופיים בשם resource forks כדי לשמור מידע מיוחד הקשור לתוכניות, כגון סמלים (icons) וכו'.
Windows 2000 משתמשת בערוצי מידע חלופיים כדי לשמור "תקציר מידע" עבור קבצים.
ניתן להגדיר לקובץ תקציר מידע על ידי שימוש באפשרות "מאפיינים" בחלונות Windows Explorer.
כאשר נבחר מאפיינים עבור קובץ ונגיע אל המסך הבא, הנתונים ישמרו ב-ADS לצד הקובץ:



ערוצי מידע חלופיים הם אפשרות שימושית ב-Windows. הם מאפשרים לשמור מידע נוסף עבור כל קובץ שצמוד אל הקובץ אך לא נראה במערכת הקבצים כקובץ נפרד.
עקב העובדה ש-Alternate Data Streams לא ניתנים לאיתור בקלות, הם מציגים בעיית אבטחה חמורה אותה נציג במסמך זה.

יצירת ADS

כיצד יוצרים ADS? מה ניתן לשמור בו? התשובה – מפתיעה – אנחנו יכולים להתייחס אל Alternate Data Stream כאל קובץ לכל דבר. אנחנו יכולים ליצור ADS, לשים בו כל תוכן, ובהמשך נראה שאנחנו יכולים אף להריץ תוכניות, שנשמרו כ-ADS.

יצירת ערוצי מידע חלופיים היא פעולה פשוטה. נדגים למשל יצירת ערוץ מידע חלופי שישויך עם הקובץ myfile.txt. כל שעלינו לעשות הוא להפריד שם הערוץ הראשי משם הערוץ האלטרנטיבי על ידי נקודתיים, ובכך להגדיר את ערוץ המידע החלופי של הקובץ.

דוגמא:

נניח שהקובץ myfile.txt קיים בספריה c:\ads. נפתח חלון DOS, ונכתוב:

```
C:\ADS> echo ADS Example > myfile.txt:hidden
```

הנתונים ישמרו ב-ads ששמו hidden.

ניתן גם לשמור קבצים שלמים, ולאו דווקא שורה אחת כ-ADS:

```
C:\ADS> echo ADS Example > file.txt
C:\ADS> type file.txt > myfile.txt:hidden
```

כמו כן איננו מוגבלים לקובצי טקסט בלבד. ניתן לשמור גם קבצים בינאריים כערוצים חלופיים:

```
C:\ADS> type c:\windows\notepad.exe > myfile.txt:sol.exe
```

ניתן לשמור קבצי הרצה, קבצי תמונה, קבצי מוסיקה או כל סוג מידע אחר.

האם העובדה ששמרנו מידע נוסף לצד הקובץ משנה את גודלו?
אם נביט בקובץ myfile.txt נראה כי לפי הנתונים אותם מספקת מערכת ההפעלה למשתמש, לא חל שינוי כלשהו בגודלו של הקובץ.

לערוצי מידע חלופיים אין מאפיינים משל עצמם. זכויות הגישה אל הערוץ הראשי הינן גם זכויות הגישה אל הערוצים החלופיים. במילים אחרות – אם איננו יכולים לשנות קובץ כלשהו, איננו יכולים להוסיף אליו ערוצים חלופיים. עם זאת, למרות ש-Windows אינה מרשה למשתמש למחוק קבצי מערכת מוגנים, היא מרשה, למשתמש עם מספיק זכויות, להוסיף אליהם ערוצי מידע נוספים.
בודק קבצי המערכת (sfc.exe), הבודק האם קבצי המערכת שונו, אינו מסוגל לגלות ערוצי מידע חלופיים.

ניתן להוסיף ADS גם לספריות, בצורה הבאה:

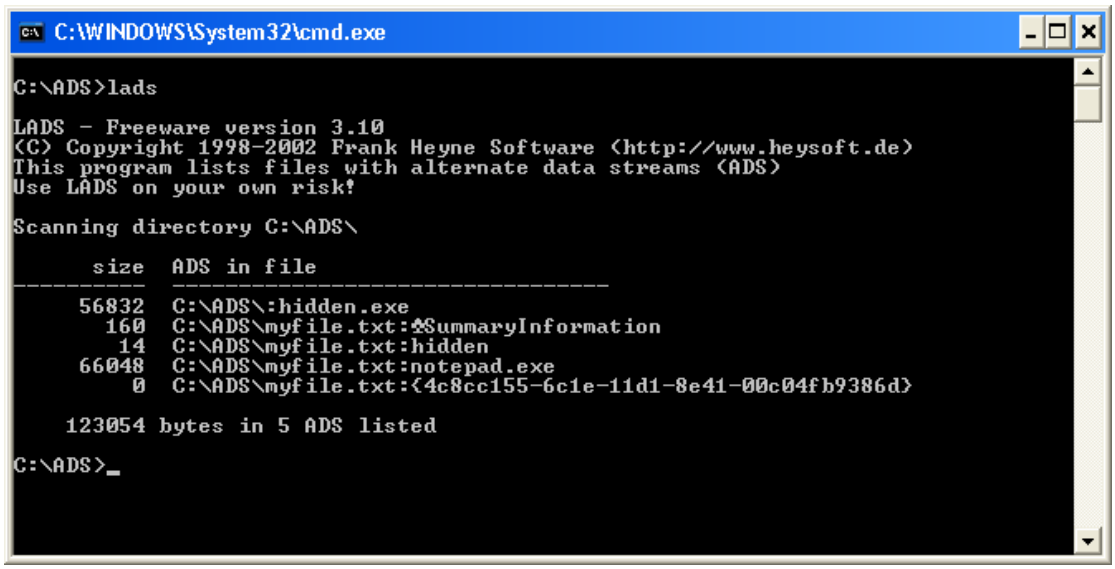
```
C:\ADS> type c:\windows\system32\sol.exe > :hidden.exe
```

גילוי, צפייה ומחיקת ADS

הבעיה המרכזית בנושא ערוצי המידע החלופיים, הוא שמערכת ההפעלה Windows איננה כוללת אף כלי היכול לשמש לגילוי ADS.
ערוצי המידע קיימים, תופסים מקום בכונן וניתן להשתמש בהם, אולם מערכת ההפעלה איננה מאפשרת למשתמש הפשוט לדעת זאת.

מספר כלים מצויים ברשת המאפשרים לעבוד עם ADS.
אחד מהם, אותו נציג, הוא תוכנה בשם LADS שנכתבה על ידי Frank Heyne, וניתנת להורדה מהאתר http://www.heysoft.de. תוכנה זו היא תוכנה המופעלת מה-Command Line, והיא מציגה את הערוצים החלופיים הקיימים בספרייה הנוכחית, או בספריה אחרת, בהתאם לפרמטרים המועברים אליה.

התמונה הבאה מציגה דוגמא לפלט שתוכנה זו מוציאה:



לאחר שגילינו את קיומם של ה-ADS, נרצה לצפות בהם.

ננסה לכתוב את השורה הבאה:

```
C:\ADS> notepad myfile.txt:hidden
```

נקבל הודעת שגיאה – כאילו הקובץ לא קיים, ו-Notepad ישאל אותנו אם אנו רוצים ליצור קובץ חדש.

זו איננה ההתנהגות לה ציפינו, מכיוון שקודם לכן יצרנו את הערוץ הנ"ל.

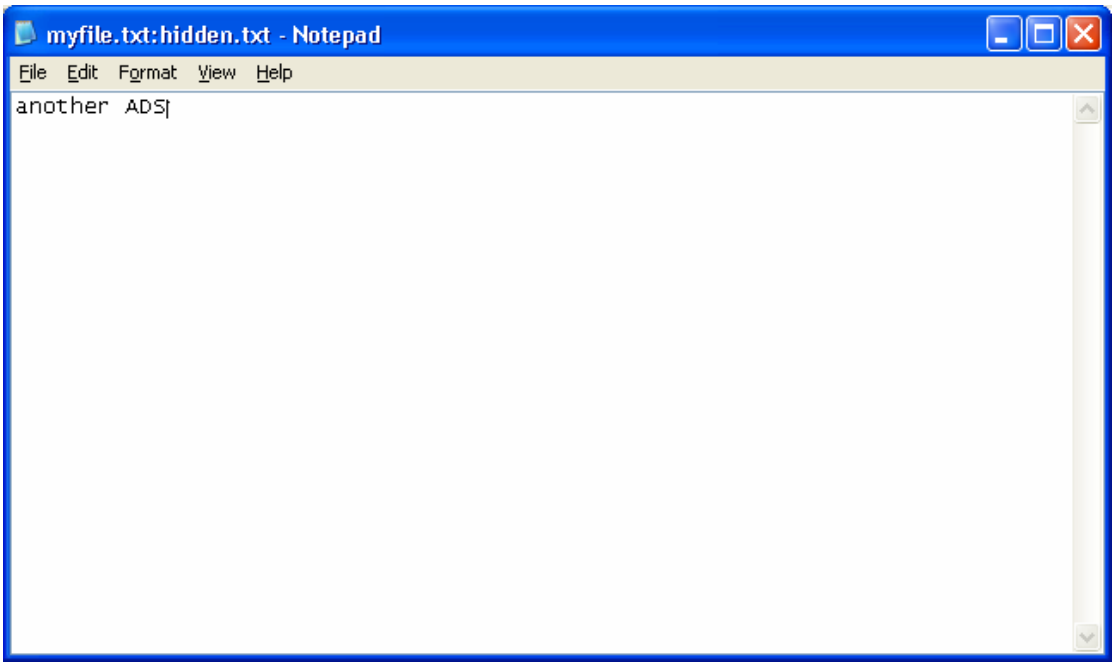
כדי להבין את הבעיה, נבצע את הפעולה הבאה. ניצור ערוץ נוסף כך:

```
C:\ADS> echo another ADS > myfile.txt:hidden.txt
```

ננסה כעת לצפות ב-ADS זה:

```
C:\ADS> notepad myfile.txt:hidden.txt
```

כעת הפעולה תצליח. Notepad יפתח והקובץ שלנו יוצג:



נוכל לגשת גם לקבצים נוספים בעלי סיומת, למשל, הפקודה הבאה תפתח את קובץ ה-EXE של Notepad:

```
C:\ADS>notepad myfile.txt:notepad.exe
```

ערוצי מידע חלופיים הם חלק ממערכת הקבצים NTFS. לפיכך, אם קובץ עם ADS מועבר אל מערכת קבצים אחרת שאיננה תומכת בהם, כגון FAT או FAT32, ערוצי המידע נמחקים.

כאשר קובץ מועבר/מועתק מערכת קבצים NTFS למערכת קבצים אחרת שגם היא NTFS, מועתקים/מועברים כל הערוצים ביחד עם הקובץ.

מחיקת ADS יכולה לעשות בפשטות על ידי רצף הפעולות הבא:

```
C:\ADS> type myfile.txt > temp.txt
C:\ADS> del myfile.txt
C:\ADS> ren temp.txt myfile.txt
```

הרצת ADS

בדוגמאות הקודמות ראינו כי ניתן לשמור קבצי הרצה בתוך ADS.
נרצה להריץ את הקבצים ששמרנו, ונרצה לעשות זאת בצורה ישירה – כלומר, ללא צורך להעתיק ראשית את הקובץ אל מחוץ ל-ADS, ואז להריצו.

במערכת ההפעלה Windows NT ניתן לבצע זאת בקלות בצורה הבאה:

```
C:\ADS> start myfile.txt:notepad.exe
```

עם זאת, ב-Windows 2000 וב-Windows XP נקבל הודעה כי הפרמטר אינו מספק.
הפתרון: שימוש באחת משתי צורות הכתיבה הבאות:

```
C:\ADS> start .\myfile.txt:notepad.exe
```

```
C:\ADS> start c:\ads\myfile.txt:notepad.exe
```

עובדה מעניינת היא שאם נביט ב-Task Manager, תחת Windows NT, 2000, נראה כי הקובץ שרץ הוא myfile.txt. תחת ה-Task Manager של Windows XP, נראה כי הקובץ שרץ הוא myfile.txt:notepad.exe.

דרך נוספת להרצת ADS העובדת ב-Windows 2000 וב-Windows XP היא יצירת shortcut (קיצור דרך).
נעשה זאת על ידי יצירת קיצור דרך שיצביע אל c:\ads\myfile.txt.
לאחר מכן נלחץ על קיצור הדרך שיצרנו בעזרת המקש הימני של העכבר, נבחר properties, ונשנה את הקובץ אליו הוא מצביע ל-c:\ads\myfile.txt:notepad.exe. לאחר מספר שניות, נשים לב לשינוי הסמל של הקובץ. לחיצה כפולה עליו תפתח את ה-ADS.

ניתן להריץ קובץ הנמצא ב-ADS עם הפעלת Windows על ידי הוספתו ל-Registry אל HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVerssion\Run, וכתיבת המסלול המלא אל הקובץ הנסתר.

ADS כבעיית אבטחה

ממבט ראשון ערוצי המידע החלופיים נראים כרעיון טוב – הם מאפשרים תמיכה במקינטוש, ומאפשרים ל-Windows לשמור מידע נוסף על קבצים.
אם זאת, האפשרות לשמור קבצים בתור ADS מתחילה להעלות חשד לגבי בטיחות ונחיצות השיטה.
האפשרות להסתיר קבצים בערוצים חלופיים מאפשרת יצירת וירוסים וסוסים טרוינים הקשים לאיתור.
כבר בשנת 2000 יצא וירוס בשם W2K.Stream שניצל את ערוצי המידע החלופיים.

אנטי-וירוסים אמורים להיות הכלי שיאתר מידע מוסתר בערוצים חלופיים. מקובל כיום שתוכנת אנטי-וירוס רצה ברקע, ומנטרת את כל הגישות לקבצים.
חלק מהאנטי-וירוסים סורקים כל קובץ, ללא התייחסות לשמו, וחלק מהם מתייחסים לשם הקובץ. הסוג השני של האנטי-וירוסים נוטה לפספס וירוסים המצויים ב-ADS, מכיוון שהוא מתייחס לשם קובץ עם נקודתיים באמצע כשם קובץ לא חוקי, ולכן הוא איננו סורק אותו.

ישנם אנשים אבטחה הטובים כי תוכנות אנטי-וירוס אינן צריכות לבדוק ADS עבור וירוסים. לטענתם, מכיוון ש-Windows מריצה באופן אוטומטי את הערוץ הראשי כאשר המשתמש פותח קובץ, תוקפים צריכים לשנות את התחלת הקובץ כדי שיריץ את התוכנית שנמצאת בערוץ החלופי. אנשי אבטחה אלו טוענים כי תוכנת האנטי-וירוס ללא התמיכה ב-ADS תזהה את שינוי תחילת הקובץ, וכך יתגלה הווירוס.

לטענה זו מספר בעיות:

1. אנטי וירוס ללא תמיכה בערוצי משנה לא יוכל לנקות את ערוצי המשנה מוירוסים – הוא יוכל רק להתריע שהם קיימים.
2. מכיוון שווירוסים יכולים לתת שמות אקראיים לערוצי המשנה סריקת הערוץ הראשי הינה בעייתית – תוכנת האנטי-וירוס הממוצעת תתקשה להחליט האם פנייה לערוץ חלופי היא פנייה לגיטימית או פנייה אל קוד זדוני של ווירוס.
3. קיימות לפחות 5 שיטות להפעיל קוד המצוי ב-ADS בלי לשנות את הערוץ הראשי. בעזרת שיטות אלו משתמשים זדוניים יכולים לחמוק מאיתור על ידי תוכנות אנטי-וירוס.

העובדה שהכלים הסטנדרטים לצפייה בקבצים מדווחים כי גודל הקובץ אינו משתנה כאשר אנו מוסיפים ערוצי משנה מקשה אף היא על איתור ה-ADS.

סיכום

ערוצי מידע חלופיים הם חלק ממערכת הקבצים NTFS המיועד לתת תמיכה עבור HFS – מערכת הקבצים של מחשב המקינטוש.
למרות שניתן ליצור ערוצים חלופיים ולפנות אליהם בקלות על ידי מערכת ההפעלה, לא קיימים ב-Windows כלים כדי לגלות ADS לא רצויים. יתר על כן, מערכת ההפעלה מספקת למשתמש מספיק פונקציונאליות כדי שיוכל ליצור ערוצים חלופיים ולהריץ קוד המוסתר בהם.
המחסור בכלים לגישה אל ערוצים אלו הופכים אותם לבעיית אבטחה. וירוסים המנצלים ערוצים אלו קיימים כבר כ-3 שנים.

הפתרון לבעיה אינו הפסקת השימוש ב-NTFS. מערכת קבצים זו מספקת יתרונות רבים בתחום האבטחה והאמינות. פתרון לבעיה הוא קביעת הרשאות מתאימות עבור קבצי המערכת החשובים, וסריקת המערכת תקופתית בעזרת כלים כגון LADS. כמו כן, אנטי-וירוסים צריכים להתעדכן ולבדוק גם את הערוצים החלופיים עבור וירוסים.

EOF