Alternate Data Streams

Het verbergen van malware via een verborgen 'feature' van NTFS

Ir. M. Paques
is als junior adviseur werkzaam binnen de business unit IT Security en control van KPMG IT Advisory in Amstelveen. Hij houdt zich onder meer bezig met security testing, social engineering, technische security reviews en de beveiliging van nieuwe technologieën.

paques.matthieu@kpmg.nl

Ir. Matthieu Paques

Het NTFS-bestandssysteem dat door Windows gebruikt wordt, biedt de mogelijkheid om meerdere 'data streams' op te nemen in één bestand. Dit concept, aangeduid met Alternate Data Streams (ADS), is relatief onbekend en biedt de mogelijkheid om data of kwaadaardige software op het systeem te verbergen zodat die zonder speciale tools haast onmogelijk gedetecteerd kunnen worden. Hackers maken op verschillende manieren dankbaar gebruik van deze feature, bijvoorbeeld om hun tools of malware ongezien op het systeem achter te laten, waardoor ze later eenvoudig op het systeem kunnen terugkeren of door met een keylogger (een vorm van spyware die alle toetsaanslagen registreert) onderschepte gebruikersinvoer (als wachtwoorden en creditcardnummers) in een ADS weg te schrijven, zodat deze onvindbaar is voor de gebruiker zelf en later door de hacker kan worden uitgelezen. In dit artikel wordt beschreven hoe ADS misbruikt kan worden en daarnaast hoe in ADS verborgen bestanden opgespoord en verwijderd kunnen worden.

Inleiding

Vanaf Windows NT maakt Microsoft Windows gebruik van het NTFS (New Technology File System), dat het oude FAT(32) filesysteem vervangt. Eén van de kenmerken van NTFS is de aanwezigheid van Alternate Data Streams. Alternate Data Streams zijn oorspronkelijk opgenomen in alle versies van NTFS om compatibiliteit met Macintosh Hierarchical File System (HFS) te verzorgen. Het Macintosh filesystem maakt gebruik van verschillende zogehete 'forks' voor het opslaan van data (voor de inhoud van documenten) en metadata (voor het vastleggen van het bestandstype en andere relevante details over het bestand). ADS wordt tevens door Windows gebruikt om bestandsinformatie als metadata en tijdelijke gegevens op te slaan. De applicatie *WordPad* gebruikt dit bijvoorbeeld om metadata over een bestand op te slaan.

Karakteristiek voor het gebruik van ADS is dat de gegevens die hierin worden weggeschreven niet in de Windows Verkenner of via bijvoorbeeld een DOS-prompt zichtbaar zijn. Bij het openen van een bestand wordt de hoofdstroom van gegevens geraadpleegd. Eventuele andere aanwezige data streams zijn onzichtbaar. Zo kan er bijvoorbeeld een .zip-bestand van 10 MB in de stream van een tekstbestand van slechts 1 kb worden opgenomen. Windows zal hierna nog steeds de bestandsgrootte van 1 kb weergeven. Deze

'feature' biedt hiermee vanuit het perspectief van een hacker interessante mogelijkheden om bijvoorbeeld tools (een zogenaamde 'rootkit') op een gecompromitteerd (reeds geïnfiltreerd) systeem te verbergen die gebruikt kunnen worden voor verdere aanvallen. Ook worden ADS gebruikt om virussen en andere malware in te verbergen (bijvoorbeeld W2k.stream, het eerste virus dat gebruikmaakt van ADS om zichzelf in te verbergen). Gelukkig, voor gebruikers van Windows, gaat een stream van een bestand verloren wanneer dit via een browser of FTP wordt binnengehaald. Dit betekent dat streams feitelijk niet gebruikt kunnen worden voor het verspreiden van malware maar slechts om bestanden te verbergen nadat malware het systeem reeds heeft gecompromitteerd.

ADS in de praktijk, een kleine workshop ...

Een typisch scenario waarin een hacker gebruikmaakt van een ADS zou er als volgt uit kunnen zien:

Allereerst wordt op een gecompromitteerd systeem een ADS aangemaakt onder een bestaande file of directory, vervolgens wordt hier een executable naartoe geschreven en wordt ervoor gezorgd dat dit bestand automatisch door de gebruiker wordt opgestart bij het opstarten van Windows. Deze stappen worden in de volgende paragrafen in detail beschreven.

Het is mogelijk onderstaande voorbeelden op het eigen systeem uit te proberen. De gebruikte commando's zijn ter verduidelijking weergegeven in lichtblauwe boxen. Vooraf zijn de bestanden *calc.exe* en *notepad.exe* uit Windows naar de nieuwe map *C:\ADS* gekopieerd. Tevens wordt gebruikgemaakt van de toolset *Unxutils* ([Unx]). De in de voorbeelden genoemde commando's worden alle in een DOS-prompt uitgevoerd, tenzij dit anders aangegeven is.

Het aanmaken van een ADS

Een ADS wordt aangeduid met de naam van het bestand waarin de stream is ondergebracht, een dubbele punt en vervolgens naam van de ADS.

Bijvoorbeeld:

C:\ADS\bestandsnaam.txt:streamnaam.txt

Hierin is '*bestandsnaam.txt*' de naam van het 'gastheer'bestand en '*streamnaam.txt*' de naam van de ADS. Het gastheerbestand kan een bestaand of een nieuw bestand zijn. Door het volgende commando in een DOS-prompt uit te voeren wordt een nieuw bestand *testfile.txt* aangemaakt:

```
echo Dit is een testfile > testfile.txt [ENTER]
```

Zoals door middel van een '*dir*'-commando kan worden vastgesteld, heeft het nieuwe tekstbestand *testfile.txt* een bestandsgrootte van 22 bytes (zie figuur 1). Dit bestand bevat de tekst 'Dit is een testfile' en kan via het DOS-commando '*type testfile.txt*' worden uitgelezen.

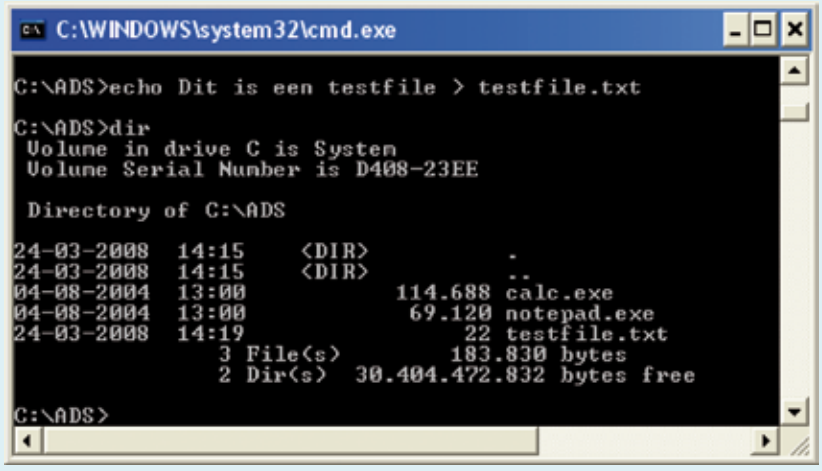
Met het volgende commando wordt tekst toegevoegd aan de ADS van het bestand *testfile.txt*:

```
echo secret information > testfile.txt:datastream.txt
[ENTER]
```

De tekst '*secret information*' is hiermee toegevoegd aan de ADS met de naam '*datastream.txt*'. Merk op dat de bestandsgrootte (zie figuur 2) van het bestand *testfile.txt* gelijk is gebleven; deze is nog steeds 22 bytes (de tijd is echter wel veranderd). Het toevoegen van een ADS aan een bestand verandert niets aan de werking of inhoud van het oorspronkelijke bestand.

Een .jpg-bestand (plaatje) kan worden toegevoegd aan een stream met het volgende commando:

```
type c:\windows\Greenstone.bmp >
testfile.txt:Greenstone.bmp [ENTER]
```



Figuur 1. **Het aanmaken van een tekstfile van 22 bytes.**

Om vast te stellen of het plaatje daadwerkelijk in de stream is opgenomen, kan de stream worden geopend met het volgende commando:

```
mspaint testfile.txt:Greenstone.bmp [ENTER]
```

Gegevens benaderen in een ADS

Wanneer getracht wordt de data in de ADS te benaderen via het commando '*type testfile.txt:datastream.txt*', wordt een foutmelding getoond. Ditzelfde gebeurt indien via het '*Open*'-commando in Notepad wordt geprobeerd de stream te wijzigen. Een stream kan aangepast worden door Notepad via de commandprompt aan te roepen:

```
notepad testfile.txt:datastream.txt [ENTER]
```

Nu wordt Notepad gestart en de inhoud van de ADS getoond. Wanneer er nu aanvullende tekst wordt toegevoegd aan de ADS zal de bestandsgrootte van het bestand '*testfile.txt*' zoals dat door Windows wordt weergegeven, niet gewijzigd zijn.

In principe kan elk type file in een ADS worden opgeslagen. In plaats van gewone tekst kan ook uitvoerbare code of een geheel programma in een ADS geplaatst worden. Zo'n programma is dan voor de gebruiker van het systeem onzichtbaar aanwezig. Een ADS kan niet alleen aan files worden toegevoegd, maar ook aan directories, bijvoorbeeld door de onderstaande commando's uit te voeren:

```
mkdir ads2dir [ENTER]
type calc.exe > c:\ads\ads2dir:calctest.exe [ENTER]
```

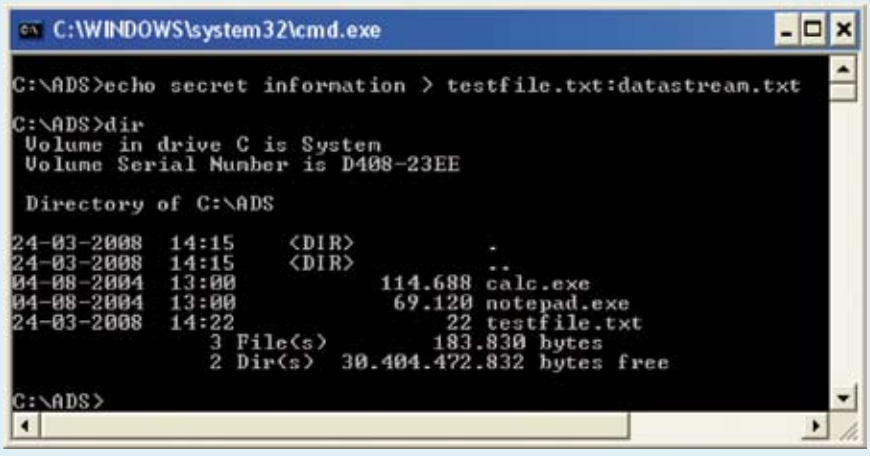
Met het eerste commando is een nieuwe directory '*ads2dir*' aangemaakt. Het tweede commando zorgt ervoor dat een kopie van het programma *Calculator* gekopieerd wordt naar de ADS '*calctest.exe*' van deze directory.

Indien nu in de Windows-verkenner de eigenschappen van de folder '*C:\ADS*' worden opgevraagd, zal de Verkenner aangeven dat de folder 0 bytes groot is. De ADS van de folder bevat echter het bestand '*calc.exe*'. De hoeveelheid data die in een ADS opgeslagen kan worden, is bijzonder groot. Tevens kan een oneindig aantal streams aan een bestand worden toegevoegd.

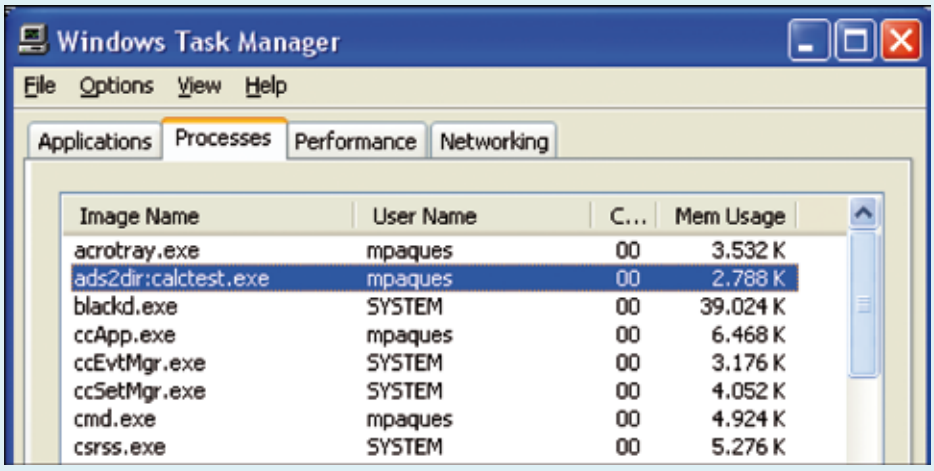
Het verborgen '*calctest.exe*'-bestand kan worden uitgevoerd met het onderstaande commando. Merk op dat het volledige directory path gebruikt wordt om de locatie van het bestand aan te geven.

```
start c:\ads\ads2dir:calctest.exe [ENTER]
```

Met dit commando wordt de Windows-rekenmachine vanuit de ADS gestart. (Dit werkt niet voor Windows Vista, daar Vista het opstarten van applicaties in streams via het 'start'-commando niet ondersteunt.) In Windows 2000 en eerdere versies van Windows wordt een ADS-executable in proces viewers zoals Windows Task Manager weergegeven als het gastheerbestand waar deze aan gekoppeld is. Zouden we dus '*calc.exe*' opnemen in een ADS van '*explorer.exe*' en vervolgens '*calc.exe*' uitvoeren, dan wordt '*explorer.exe*' in deze Windows-versies als actief proces aangegeven. Dit betekent dat naast de aanwezigheid van de file ook het uitvoeren hiervan verborgen plaatsvindt. In Windows XP is een programma dat actief is in ADS, wel in taakbeheer zichtbaar, zoals te zien is in figuur 3.



Figuur 2. **Het schrijven van data naar een ADS.**



Figuur 3. **Taakbeheer in Windows XP.**

Met de tool 'cat' (onderdeel van de toolset UnxUtils) kan een programma uit een ADS terug naar een normale file (hier '*calcnew.exe*') worden geschreven.

```
Cat c:\ads\ads2dir:calctest.exe > calcnew.exe [ENTER]
```

Het bestand '*calcnew.exe*' bevat nu de calculator die we aan de directory hadden gekoppeld.

Misbruik maken van ADS

Zoals eerder opgemerkt kan praktisch elk type bestand in een ADS worden opgenomen. Een typisch scenario waar een virus (of ander type malware) gebruik van maakt, ziet er als volgt uit:

Scenario 1

Een hacker vervangt de originele executable met de viruscode, hernoemt het virus naar de oorspronkelijke bestandsnaam en voegt vervolgens de oorspronkelijke executable toe in de ADS. Wanneer de gebruiker het executable-bestand uitvoert wordt de viruscode gestart en start het virus vervolgens het oorspronkelijke programma dat zich in de ADS bevindt (figuur 4).

Scenario 2

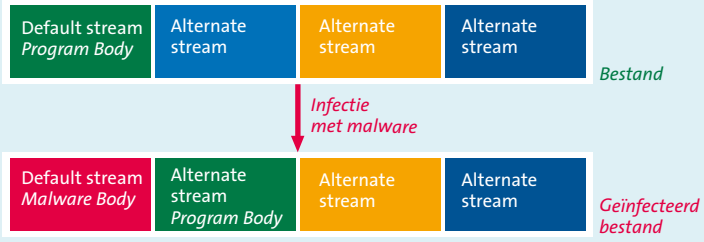
In een ander scenario wordt de viruscode zelf in de ADS verborgen. De viruscode kan nu automatisch worden uitgevoerd via bijvoorbeeld het Windows-register tijdens het opstarten van Windows of door in de oorspronkelijke executable een beperkt stuk code toe te voegen dat het virus in de ADS aanroept. Voordeel van deze aanpak is dat de bestandsgrootte van de oorspronkelijke file (nauwelijks) verandert, wat de kans op detectie verkleint.

Het volgende voorbeeld illustreert hoe een bestand in een ADS automatisch kan worden opgestart.

Let op: De volgende commando's brengen wijzigingen aan in het register. Het is aan te raden om voor het uitvoeren van deze commando's een back-up van het Windows-register te maken. (Voor het uitvoeren van registerwijzigingen zijn beheerdersrechten op het systeem nodig.)

```
reg delete HKCR\txtfile\shell\open\command /f [ENTER]

reg add HKCR\txtfile\shell\open\command /ve /t REG_
EXPAND_SZ /d c:\ads\ads2dir:calctest.exe /f [ENTER]
```



Figuur 4. **Infectie van een bestaand programma met malware.**

Wanneer nu een willekeurige tekstfile wordt geopend zal Windows de rekenmachine (uit de ADS) in plaats van Notepad starten. Uiteraard kunnen deze commando's ook in een batchbestand, VB-script of andere programmeertaal worden opgenomen (om door een nietsvermoedende gebruiker te worden uitgevoerd). In dit voorbeeld wordt het onschuldige programma calculator gestart. Op dezelfde wijze kan met slechts twee regels code elke keer dat er een tekstfile wordt geopend onmerkbaar elk mogelijk bestand worden gestart.

Het register kan worden hersteld met het volgende commando:

```
reg add HKCR\txtfile\shell\open\command /ve /t REG_
EXPAND_SZ /d "%SystemRoot%\system32\notepad.exe
%1" /f [ENTER]
```

Andere manieren waarop een executable in een ADS kan worden gestart, zijn onder meer:

- het automatisch laten starten met Windows;
- via de task scheduler;
- door toevoeging aan de Windows-startup folder;
- door het toevoegen van instructies in de winstart.bat file in de Windows-map;
- door het plaatsen van een file explorer.exe in de map c:\. Doordat de map :\ eerder in het zoekpad van Windows voorkomt zal indien hier een bestand explorer.exe staat, dit automatisch door Windows worden uitgevoerd in plaats van het oorspronkelijke bestand in de map c:\windows\.

Detecteren en verwijderen van Alternate Data Streams

Gezien de eenvoud waarmee bestanden in een stream verborgen worden is het aan te raden om kritische systemen periodiek te controleren op de aanwezigheid van deze streams. Deze controle zou bijvoorbeeld deel kunnen uitmaken van een periodieke technische audit op security-instellingen.

In Windows Vista is het 'dir'-commando voorzien van een nieuwe optie (/r) waarmee files met verborgen streams getoond worden. Voor eerdere Windows-versies zijn er verschillende gratis tools voor het detecteren van ADS beschikbaar als '*lads*' ([Lad]), '*lns*' ([Lns]), '*streams*' ([Mic]) en '*adsspy*' ([Ads]).

```
C:\WINDOWS\system32\cmd.exe

C:\ADS>lads

LADS - Freeware version 4.10
(C) Copyright 1998-2007 Frank Heyne Software (http://www.heysoft.de)
This program lists files with alternate data streams (ADS)
Use LADS on your own risk!

Scanning directory C:\ADS\

      size  ADS in file
----------  ---------------------------------
    114688  C:\ADS\:calctest.exe
    114688  C:\ADS\ads2dir\:calctest.exe
        26  C:\ADS\cat.exe:Zone.Identifier
        26  C:\ADS\lads.exe:Zone.Identifier
    114688  C:\ADS\notepad.exe:calc.exe
        38  C:\ADS\testfile.txt:datastream.txt

    344154 bytes in 6 ADS listed

C:\ADS>_
```

Figuur 5. **Het opsporen van een ADS met lads.**

Een typische output van de tool '*lads*' is opgenomen in figuur 5. Hier is te zien dat zowel de naam van de ADS als de afmeting van deze ADS zichtbaar kan worden gemaakt.

Voor diegenen die de voorkeur geven aan een grafische interface biedt de Tool '*Adsspy*' (figuur 6) uitkomst.

Wanneer het bestand of de directory waaraan een ADS is gekoppeld wordt verwijderd, wordt daarmee ook de ADS verwijderd. Ook kunnen de tools '*streams*' en '*ADS spy*' worden gebruikt om de ADS uit de file te verwijderen.

Een andere wijze om de ADS te verwijderen is door de file waaraan deze is gekoppeld naar een bestandssysteem dat geen ADS ondersteunt (bijvoorbeeld FAT32) te verplaatsen en weer terug.

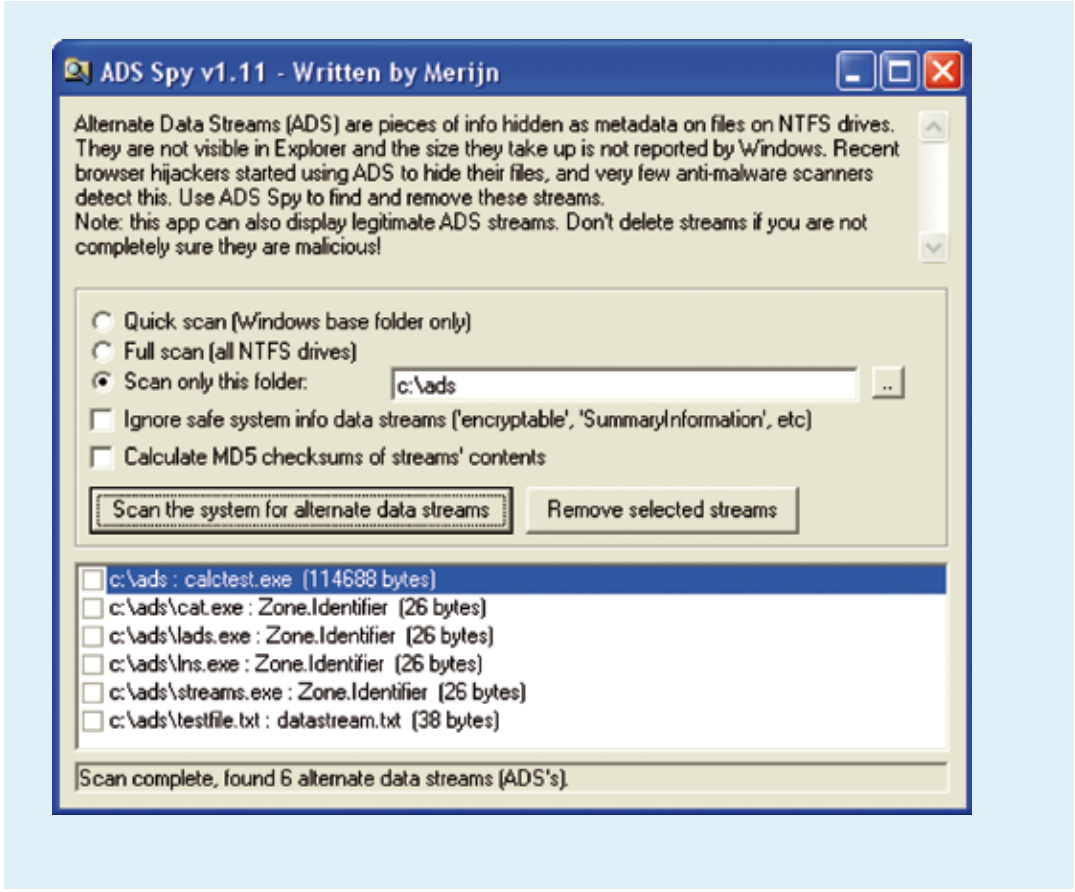
Een derde mogelijkheid voor het verwijderen van een ADS is om de inhoud van het oorspronkelijke bestand naar een nieuw bestand te schrijven en het nieuwe bestand te hernoemen naar de oorspronkelijke bestandsnaam. Bijvoorbeeld:

```
type notepad.exe>tempfile.exe [ENTER]
del notepad.exe [ENTER]
ren tempfile.exe notepad.exe [ENTER]
```

Aanvullend op het controleren op de aanwezigheid van een ADS op het filesysteem met bovenstaande tools kunnen we alle programma's die automatisch met Windows worden gestart, nalopen op verdachte patronen. Een ':' in het path wijst mogelijk op de aanwezigheid van een verborgen ADS.

Conclusie

De ADS-feature van NTFS geeft de mogelijkheid om files op te slaan op een manier onzichtbaar voor Windows en standaard file handling applicaties. Een hacker kan misbruik van deze eigenschap maken door virussen of malware in een ADS te verbergen. Met ADS kan data in bestaande files worden toegevoegd zonder hun afmeting of werking te beïnvloeden. Er kan een grote hoeveelheid data in een ADS worden opgenomen (ideaal voor keyloggers). Hiernaast zijn ADS eenvoudig te maken en bijzonder lastig te detecteren zonder het gebruik van speciale tools. Files in een ADS kunnen worden aangeroepen op allerlei verschillende manieren waaronder het gebruik van batch files of via het Windows-register. Met deze combinatie van eigenschappen kan ADS een serieuze bedreiging vormen voor de beveiliging van een systeem. Het is dan ook aan te raden om kritische systemen periodiek te controleren op de aanwezigheid van alternate data streams. Deze controle zou bijvoorbeeld deel kunnen uitmaken van een periodieke technische audit op security-instellingen.



Figuur 6. **ADS spy: een grafische tool om ADS op te sporen.**

Literatuur

[Ads] *adsspy*, http://www.bleepingcomputer.com/files/adsspy.php.
[Lad] *lads*, http://www.heysoft.de/Frames/f_sw_la_en.htm.
[Lns] *lns*, http://ntsecurity.nu/toolbox/lns/.
[Mic] *streams*, http://www.microsoft.com/technet/sysinternals/FileAndDisk/Streams.mspx.
[Micro6] Microsoft, *Alternatieve NTFS-gegevensstromen gebruiken*, http://support.microsoft.com/kb/105763, 24 mei 2006.
[Park05] Don Parker, *Windows NTFS Alternate Data Streams* http://www.securityfocus.com/infocus/1822, 2005-02-16.
[Unx] *GNU utilities for Win32*, http://unxutils.sourceforge.net/.
[Wiki] Wikipedia, *Fork (filesystem)*, http://en.wikipedia.org/wiki/Fork_(filesystem).