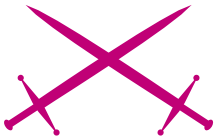

ADS i fantasmi della NTFS

Nanni Bassetti

Grado di difficoltà

Tra i files presenti sui nostri hard disk non è tutto oro quel che luccica, infatti vi sono delle informazioni nascoste all'interno dei più comuni programmi di uso quotidiano. Gli ADS (Alternate Data Streams) sono un ottimo sistema per occultare immagini, virus, spyware nel nostro computer, impariamo a capirli, individuarli e distruggerli.

Sulle case infestate dai fantasmi si potrebbe discutere a lungo, ma pensare che anche nei nostri computers potrebbero albergare degli spettri diventa veramente terrificante. Ebbene sì, purtroppo anche nei PC possono esserci queste oscure presenze, che non si limiterebbero soltanto a spaventarci, ma potrebbero rappresentare una vera e propria minaccia.

Gli hackers hanno un unico desiderio, quello di carpire informazioni dai nostri sistemi e per farlo cercano sempre di istallare del malware sui nostri PC, ci provano continuamente, con gli activex da web, con macro nelle e-mail, ecc. ecc.

Molti dei metodi su indicati sono intercettati dagli anti-virus, dagli anti-spam e specialmente dalla nostra accortezza, però c'è un modo che potrebbe essere difficile da intercettare, perché sfrutta una caratteristica della *NTFS* (*New Technology File System*), ossia il file system dei sistemi Windows XP, NT e 2000, infatti gli ADS furono inseriti nella *NTFS*, per una questione di compatibilità con la *Macintosh Hierarchical File System* (HFS), per mantenere alune informazioni associate ai files, come icone, ecc.

In questo modo i sistemi Mac poterono operare in modo trasparente sui dati presenti sui server NT. I sistemi basati su NTFS hanno gli strumenti per creare gli ADS (*Alternate Data Streams*) ma non sono muniti di strumenti per eliminarli, ma cosa sono gli ADS?

Prima di addentrarci nell'argomento facciamo un breve ripasso di informatica di base parlando del filesystem, ossia il sistema tramite il quale i file sono conservati ed organizzati sulle memorie di massa (hard disk, floppy, ecc.).

Il filesystem scrive i files sui settori dei dischi e li visualizza linkandoli ai nomi dei files stessi tramite una tabella di allocazione la FAT (*File Allocation Table*), questa tabella contiene il nome file e l'indirizzo fisico del file sul disco (per semplificare), e grazie ad essa i files possono essere mostrati in maniera gerarchica ed

Dall'articolo imparerai...

- A creare e distruggere gli ADS (*Alternate Data Streams*) e capirne la pericolosità

Cosa dovresti sapere...

- Un minimo di comandi DOS e sistema Windows

organizzati in directories (in modo testuale come nel DOS) oppure in cartelle (modo grafico come nei sistemi a finestre o interfacce grafiche).

La storia della FAT affonda le sue radici nel lontano 1980 con la prima versione di QDOS di Tim Paterson, il predecessore del PC-DOS e di MS-DOS della Microsoft, con questa innovazione si poteva tener traccia delle aree di disco usate e di quelle libere, in seguito la FAT assunse nuovi nomi, come FAT12, FAT32, VFAT e NTFS, la differenza tra loro consisteva in quanti bit sono allocati per numerare i cluster del disco, ad esempio con 32 bit si potevano gestire 232 = 4.294.967.296 cluster e così via...

La FAT è sostanzialmente composta di quattro aree: Area riservata, Tabella di Allocazione dei File, Directory radice ed Area dei File, le informazioni per gestire il disco (*boot sector*) sono immagazzinate nell'area riservata che parte dal settore logico zero.

La NTFS nasce negli anni '90 ed è un sistema a 64 bit portando i computer a poter indicizzare hard disk enormi, inoltre possiede caratteristiche di affidabilità (se un processo è interrotto brutalmente il filesystem non si corrompe), di sicurezza (si possono impostare dei permessi di accesso su files e cartelle) e di supporto dei nomi lunghi dei files fino a 255 caratteri grazie alla codifica *Unicode*.

Nella NTFS le informazioni su file e cartelle sono memorizzate in una tabella chiamata *Master File Table* (MFT). In questa regione del disco ogni file è identificato da una collezione di oggetti chiamati attributi.

Tra questi troviamo, per esempio, il nome assegnato al file, la data di creazione, la data dell'ultima modifica, i descrittori di protezione e, ovviamente, i dati che ne rappresentano il contenuto, però a questi dati *ufficiali* si affiancano dei dati di contenuto *alternativi*, gli ADS appunto, che permettono, come in un allegato e-mail, di agganciare ad un file noto es.: notepad.exe, un altro file di qualsiasi tipo.

Penso che si cominci ad intuire la pericolosità rappresentata da questi *depositi* virtuali di informazioni, ma non è tutto, infatti gli ADS sono invisibili, (come i fantasmi) e non alterano la dimensione del file originale, se per esempio inseriamo un file di 3Mb nel notepad.exe (70Kb), il nostro beneamato blocco note continuerà a mantenere la dimensione di 70Kb, l'unico campanello d'allarme sarà raffigurato dalla modifica della data di creazione del file, ma come è facilmente immaginabile, è un problema facilmente aggirabile. Ecco due semplici utilities per cambiate il date-time stamp dei files:

- Attribute Magic – Download *http://www.elwinsoft.com/atm.html,*
- fileTweak – Download *http://www.febooti.com/products/filetweak/.*

Proprio come le inconsolabili anime dei defunti gli ADS non solo infestano gli oggetti ma anche le stanze, infatti questi ospiti sgraditi possono essere presenti nelle cartelle (*directories*) e rimanere invisibili, fino a quando, qualcuno, che non è un medium, li chiamerà per appalesarli e lì saran dolori.

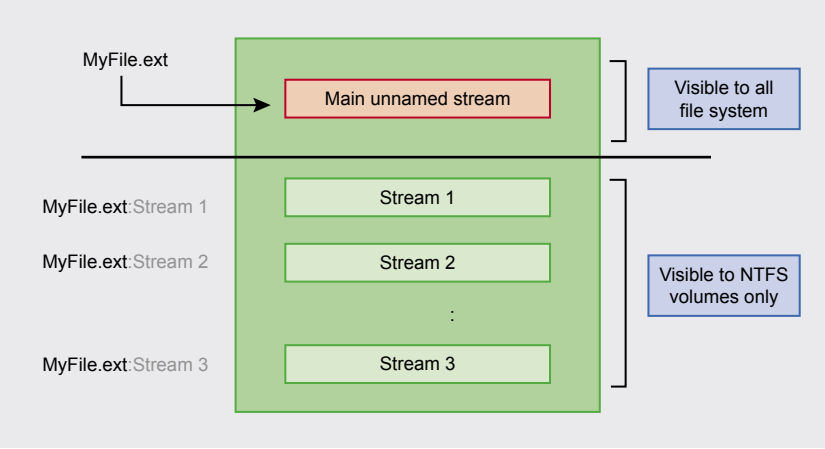

Fig. 1: *Streams del file*

```
C:\ads1>dir
 Il volume nell'unità C non ha etichetta.
 Numero di serie del volume: 5492-D9EE

 Directory di C:\ads1

27/09/2006  15.47    <DIR>          .
27/09/2006  15.47    <DIR>          ..
27/09/2006  15.47           644.154 biglietto.bmp
16/09/2006  19.45            70.144 notepad.exe
               2 File         714.298 byte
               2 Directory  63.164.387.328 byte disponibili
```

Fig. 2: *Finestra DOS con i 2 files da usare*

In pratica

Vediamo come creare velocemente un ADS. Prima creiamo una cartella c:\ads1, clicchiamo su START, quindi su ESEGUI, quindi digitiamo `CMD`, scriviamo `cd \ads1`, e poi scriviamo `copy %windir%\notepad.exe c:\ads1`. Così copiamo il file notepad.exe (il BloccoNote) nella cartella ads1. Poi copiamo un'immagine esemplare, in nostro caso: *biglietto.bmp* nella cartella c:\ads1. Adesso procediamo alla grande alchimia, inseriamo l'immagine *biglietto.bmp* nel file *notepad.exe* e scriviamo: `type biglietto.bmp -> notepad.exe:biglietto.bmp` ed il gioco è fatto!

Notiamo subito che *notepad.exe* è di 70Kb e biglietto.bmp è di 3.3Mb

Dopo aver cancellato *biglietto.bmp*, notiamo che *notepad.exe* è ancora di 70Kb, però la data è cambiata, dal 19/08/2004 al 16/09/2006 ed anche l'ora.

Che succede se digitiamo notepad.exe e premiamo INVIO?

Ecco la risposta: parte il Blocco Note, ma se digitiamo `start ./notepad.exe:biglietto.bmp` Accade un'altra cosa: appare un innocentissimo biglietto da visita, ma se fosse stata un'immagine pedo-pornografica? Oppure un video hard? Un messaggio terroristico? O un eseguibile (*exe*) malevolo? Virus, spyware, ecc.

Facciamo finta che il programma *calc.exe* (la calcolatrice di windows) sia un pericolo trojan virus:

```
type %windir%calc.exe >
notepad.exe:calc.exe
```

Adesso abbiamo inserito il file *calc.exe* nel blocco note ergo se digitiamo: `start ./notepad.exe:calc.exe` Ecco che appare la calcolatrice di Windows.

La peculiarità degli ADS è che possono inglobare dei file eseguibili da altri programmi, come ad esempio uno script PERL o VBS o PHP ed essere eseguiti dal programma relativo, per esempio: `perl notepad.exe:prova.pl`

ADS e cartelle

Similarmente possiamo allegare dati alternativi ad una cartella.

Col seguente comando si aggiunge uno stream alla cartella corrente cioè a *c:\ads2* (nuova cartella vuota):

```
c:\ads2> type c:\immagini\
pippo.jpg > :ppp.jpg
```

Se si lancia il comando `c:\ads2\dir` vediamo che la cartella ads2 è vuota...ma sappiamo che non è vero. L'eliminazione di stream da una cartella è chiaramente un problema più complesso, poiché siamo costretti ad usare utilities specifiche.

Riepilogando

Lo stream può essere eseguito solo se chiamato direttamente da un programma col percorso completo del file inquinato, quindi è impossibile che sia eseguito accidentalmente, inoltre nessuno dei protocolli di Internet come SMTP (posta elettronica), FTP ecc. può trasportarli, perchè non supportano gli streams, quindi gli ADS non possono essere inviati via Internet.

Comunque, i files contenenti ADS possono viaggiare attraverso le LAN a patto che si vadano a copiare su sistemi che hanno l'NTFS.

In alcuni casi, gli streams sono stati usati per effettuare degli exploit sui web server che erano suscettibili a mostrare il codice sorgente attraverso il: $DATA stream, questa era una grave minaccia per gli script in PHP o ASP, per fortuna la gran parte dei server è stata patchata, comunque l'exploit consisteva in questo, bastava digitare un URL così:

- *http://www.xyz.com/default.asp::$DATA*

Fig 4. *Biglietto.bmp*

```
C:\ads1>dir
 Il volume nell'unità C non ha etichetta.
 Numero di serie del volume: 5492-D9EE

 Directory di C:\ads1

27/09/2006  15.49    <DIR>          .
27/09/2006  15.49    <DIR>          ..
16/09/2006  19.45            70.144 notepad.exe
               1 File         70.144 byte
               2 Directory  63.164.350.464 byte disponibili
```

Fig. 3: *Notepad.exe che mantiene la stessa dimensione*

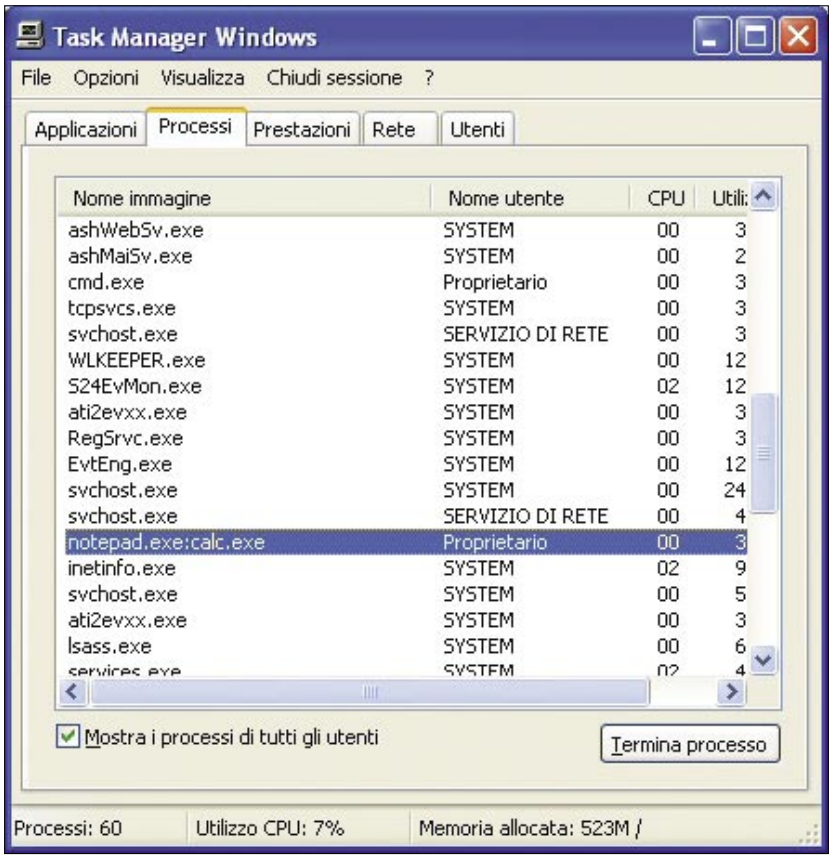

Fig. 5: *Task manager mostra il processo notepad.exe:calc.exe*

Diventiamo GHOSTBUSTERS

Diventare *Ghostbusters* significa imaparare ad acchiappare i fantasmi, quindi i nostri ADS, cominciamo con una semplice tecnica:

- premiamo ctrl + Alt + Canc

Vediamo nel task manager che esiste il processo notepad.exe:calc.exe, il quale ha mandato in esecuzione la calcolatrice di Windows, chiaramente se al posto di notepad.exe: calc.exe ci fosse stato notepad.exe: SonoUnSuperVirus.exe, chiunque potrebbe sgamare facilmente l'intruso.

Allora un hacker furbo può fare questo:

```
type c:\nc.exe > C:\windows\
system32\notepad.exe:svchost.exe
```

Questa operazione non fa altro che nascondere nello spazio ADS del file notepad.exe il file nc.exe (pericolosissimo) nominandolo svchost.exe, nome che non desterebbe sospetti nella maggior parte degli utenti di Windows, se poi l'hacker ha digitato questo (l'opzione /B serve a non far comparire la finestra DOS):

```
start /B C:\windows\notepad.exe:
svchost.exe -d -L -p 2222 -e cmd.exe
```

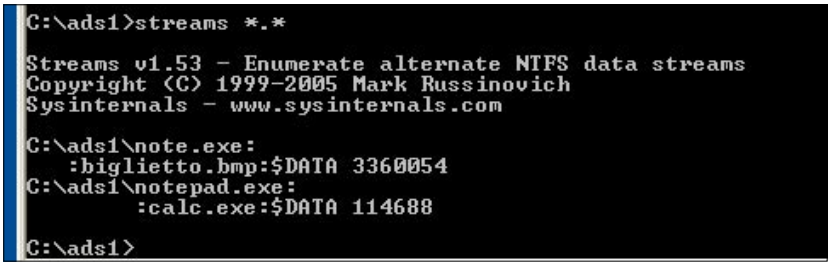

Fig. 6: *Streams ci fa vedere biglietto.bmp contenuto in note.exe*

In Rete

- *http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnfiles/html/ntfs5.asp,*
- *http://www.diamondcs.com.au/index.php?page=archive&id=ntfs-streams,*
- *http://www.auditmypc.com/freescan/readingroom/ntfsstreams.asp,*
- *http://www.securityfocus.com/bid/149/info,*
- *http://www.forensicfocus.com/dissecting-ntfs-hidden-streams,*
- *http://www.windowsecurity.com/articles/Alternate_Data_Streams.html,*

Utilities freeware che si possono usare:

- Lads.exe (*www.heysoft.de*),
- AdsCheck.exe (*http://www.diamondcs.com*),
- LNS - List NTFS Streams (*http://ntsecurity.nu/toolbox/lns/*),
- Ads Spy (*http://www.spywareinfo.com/~merijn/files/adsspy.zip*),
- Streams.exe (*http://www.sysinternals.com/utilities/streams.html*),
- SFind (*http://www.foundstone.com*).

Cenni sull'autore

L'autore lavora dal 1998 nella IBOL S.r.l. come sviluppatore di applicazioni web e system administrator e dal 2004 si occupa di sicurezza informatica con la sua ditta NBS *http://www.nannibassetti.com.*

Ha scritto un libro sulla sicurezza del web ed un thriller informatico *Onphalos* ed ha collaborato con la procura del Tribunale di Bari per un indagine informatica su un computer sequestrato (Digital Forensics).

Succede che il programma NetCat (*nc.exe*) si mette in ascolto sulla porta 2222 permettendo all'intruso di introdursi da remoto nel computer vittima.

Adesso è tempo di cominciare a difendersi!

Se siamo stati così fortunati da scoprire un file con ADS sospetto possiamo pulirlo *a mano* così:

- `ren notepad.exe note.exe` (rinominiamo il file *notepad.exe* come ci pare),
- `type note.exe -> notepad.exe` (riscriviamo il file *notepad.exe* col comando type, che non si porta appresso l'ADS),
- `del note.exe` (cancelliamo *note.exe*)

E così abbiamo un notepad nuovo di pacca e, specialmente, pulito.

Un altro sistema semplice ed efficace è quello di copiare i files infestati su una chiavetta USB o un floppy o un hard disk non NTFS e poi ricopiarlo nel vostro hard disk, infatti la copia su altri file system distrugge gli ADS, perchè non supportati.

Streams o ADS Spy permettono la cancellazione degli ADS oltre che la scoperta. Per pulire i files dagli ADS basta digitare: `streams -s -d *.*` dove *-s* è per le sottodirectories e *-d* per cancellare gli ADS.

Per concludere ci sono anche ADS buoni come le informazioni che il browser inserisce in questi spazi, come la [Zone Transfer] che identifica da che zona di internet un file è stato scaricato....qual'è l'utilità?

Poi c'è la Systeminformation ossia la peculiarità che per ogni documento, è possibile memorizzare informazioni aggiuntive quali titolo, oggetto, autore, parole chiave ecc. attraverso la scheda Riepilogo presente nelle Proprietà del relativo file.

Ed infine c'è Encriptable sempre presente nei file nascosti thumbs.db contenenti la cache delle anteprime delle immagini.

Queste meta-informazioni vengono salvate in appositi ADS di sistema, ma non sono questi gli spettri che ci spaventano. ●