Difesa

Steganografia, l'arte della scrittura occulta...

Francesco Arruzzoli

Grado di difficoltà

Parlare di Steganografia in modo esauriente vorrebbe dire scrivere un trattato di migliaia di pagine sia per le sue enormi potenzialità ed applicazioni sia perchè la sua storia è molto antica.

Infatti al contrario di quanto si possa pensare è riconducibile al tempo degli antichi greci e la parola stessa deriva dal greco, dalle parole *stèganos*, che significa nascosto, e *gràfein*, che significa scrivere; ho scritto questo articolo per fare una breve introduzione a quest'arte, dare una panoramica sulle sue principali applicazioni nel campo informatico e porre una base di partenza per successivi approfondimenti. La storia è piena di applicazioni steganografiche, i greci ad esempio, usavano incidere del testo (il messaggio segreto) su tavolette di legno e successivamente lo occultavano ricoprendolo di cera, infine scrivevano sulla cera un messaggio generico, magari una poesia d'amore per non destare sospetti; per leggere il vero messaggio il destinatario doveva grattare via la cera dalla tavoletta. Gli antichi romani , invece, usavano spesso scrivere tra le righe di una generica lettera usando come inchiostro il succo di limone (ma anche aceto o latte); questo una volta asciutto diviene invisibile ma se si pone la lettera in prossimità di una fiamma il succo di limone si brucia più rapidamente della carta e fa apparire la scritta; a volte usavano il componimento acrostico (dal greco akròstichon - ciò che si trova all'inizio del verso), versi poetici nei quali l'unione delle lettere iniziali di ciascun verso forma una parola o una frase. Ma solo nel 1500 d.c. la scienza della steganografia fù ufficializzata grazie ai trattati (*Steganographia* e *Clavis Steganographiae*) dell'abate Giovanni Tritemio, che definì la steganografia come una disciplina il cui scopo è quello di nascondere un' informazione in modo tale che la sua presenza non possa essere determinata. Sono oltremodo famose le griglie di Gerolamo

Dall'articolo imparerai...

- Cos'è la steganografia e le sue principali applicazioni
- Steganografare le informazioni con le immagini e con gli Alternate Data Streams di Microsoft

Cosa dovresti sapere...

- Dovresti avere la conoscenza di base del sistema operativo Windows XP
- Dovresti avere dimestichezza con la console del DOS in Windows XP

Cardano matematico e stregone quasi contemporaneo di Tritemio che applicando dei cartoncini con ritagliati rettangoli in posizioni irregolari scriveva sui fogli messaggi segreti che confondeva aggiungendo successivamente altro testo (Fig.1).

La steganografia è differente dalla crittografia, quest'ultima pone come fattore di sicurezza il contenuto dell'informazione, dove tutti possono leggere il messaggio criptato ma soltanto chi possiede la chiave per decodificarlo è in grado di leggere il messaggio in chiaro, va da sè, che una volta conosciuta la chiave di decodifica il messaggio crittografato non è più sicuro. La steganografia pone come fattore di sicurezza l'esistenza stessa dell'informazione, nascondendo il messaggio segreto in maniera tale che nessuno possa trovarlo. La metodologia per *rompere* (in gergo tecnico) i messaggi steganografati è sostanzialmente differente, infatti la crittanalisi cerca di decodificare e rompere messaggi criptati, mentre la steganalisi cerca di determinare l'esistenza di eventuali informazioni nascoste. Anche la risoluzione è diversa, la prima può partire dal confronto di porzioni di testo in chiaro e parti di testo cifrato, la seconda deve innanzitutto rendersi conto che è in presenza di un' informazione steganografata e dopo tentare la decodifica analizzando il testo di copertura, il suo contenitore e qualsiasi altro elemento collegato al messaggio nascosto. La steganografia quindi offre grande spazio alla creatività ed alla capacità di inventare metodi e tecniche sempre diverse per trasmettere informazioni nascoste. Tuttavia possiamo dividere le tecniche steganografiche in tre tipi:

- Steganografia sostitutiva,
- Steganografia selettiva,
- Steganografia costruttiva.

La Steganografia sostitutiva è indubbiamente la più diffusa e parte dal principio che in genere il canale di comunicazione (ad es. La radio, il telefono, la televisione, ecc.) trasmettono segnali che a causa di interferenze ambientali, generate dagli stessi conduttori, apparati trasmissivi e/o di ricezione si sporcano acquisiscono cioè del segnale di fondo in gergo detto *rumore*; la tecnica è quella di inserire un messaggio segreto facendolo apparire come rumore e che quindi solo con un appropriato filtro può essere recuperato. Il limite di questa tecnica è quello che una volta che si conosce il mezzo di trasmissione si conosce anche il rumore che in genere si crea e se ne può realizzare un modello. Si può quindi utilizzare tale modello per controllare le trasmissioni, confrontando il rumore ed evidenziando quello sospetto. La steganografia selettiva e quella costruttiva sono state pensate proprio per eliminare questo limite della steganografia sostitutiva. La Steganografia selettiva in realtà non ha molte applicazioni in quanto è estremamente dispendiosa in termini di tempo e di risorse. La tecnica utilizzata nella steganografia selettiva è sostanzialmente quella empirica cioè ripetere il processo fino a quando non viene soddisfatta una certa condizione. Cerchiamo di fare un esempio estremamente semplice ma poco realistico e al limite della stupidità. Supponiamo di voler inviare dei messaggi di risposta si/no in segreto ad un nostro amico e per farlo decidiamo di usare delle immagini e un programma (filtro) steganografico che abbiamo precedentemente preparato e che utilizzano entrambi le parti. Il programma analizza le immagini inviate e se il numero totale dei bit uguali a 0 è maggiore di quelli uguali a 1 allora la risposta è si in caso contrario no. Per acquisire l'immagine usiamo uno scanner e questo comporta che ad ogni acquisizione un diverso *rumore naturale* di fondo venga inserito nell'immagine, provando e riprovando alla fine si riuscirà a trovare l'acquisizione con il numero di bit maggiori che ci serve. L'immagine è stata selezionata tra diverse prove (da qui deriva il nome tecnica selettiva) e il risultato è che non viene effettuato sull'immagine nessun artifizio che possa essere analizzato e individuato quindi permette di superare il confronto con un eventuale modello statistico di rumore perchè rientra pienamente nei suoi parametri. La Steganografia costruttiva potremmo dire che aumenta il livello di qualità e di *invisibilità* della tecnica in quanto si propone di utilizzare un modello di rumore originale per adattare il messaggio segreto, in modo che il risultato sia un falso rumore che però ha tutte le caratteristiche ed i parametri del modello naturale.

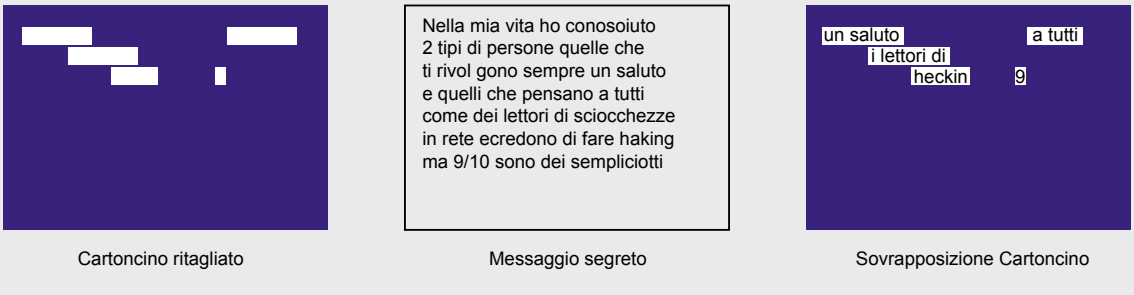

Fig. 1: *Griglia di Cardano*

A parte la maggiore complessità nel realizzare una simile tecnica i problemi principali sono sostanzialmente due: se chi ascolta ha più tempo a disposizione può costruire un modello sempre più perfetto in grado alla fine di scoprire il falso rumore; se il modello utilizzato per creare i messaggi steganografici fosse scoperto potrebbe essere utilizzato come filtro per individuare i messaggi (ad es. Potrebbe essere inserito come firma in un IDS). Oggi la steganografia è più che mai viva ed ha dato vita ad altre forme e tecniche di occultamento, esistono ad esempio alcune tecniche come la codifica *Line-shift, word-shift* e *feature* dove le parole cifrate vengono nascoste modificando alcune caratteristiche del documento che le contiene, come lo spostare leggermente le parole segrete verticalmente sulla riga o modificandone in maniera quasi impercettibile i caratteri che le compongono. Ma è proprio nell' ambito informatico che la moderna steganografia ha trovato una sua rinascita divenendo un argomento estremamente scottante. In diverse occasioni, ad esempio, il governo Americano ha ipotizzato l'idea che Osama Bin Laden per impartire ordini ai suoi fedeli abbia trasmesso del testo nascosto facendo uso della steganografia nei suoi video televisivi. In ogni caso, tralasciando eventi tragici e disastrosi come quelli dell'11 settembre, a mio parere, uno degli esempi più affascinanti della steganografia e che meglio fà capire le sue immense potenzialità di impiego, è quello di nascondere del testo (ma anche un programma o un qualsiasi altro file) all'interno di una immagine (bitmap, Jpeg, ecc.).

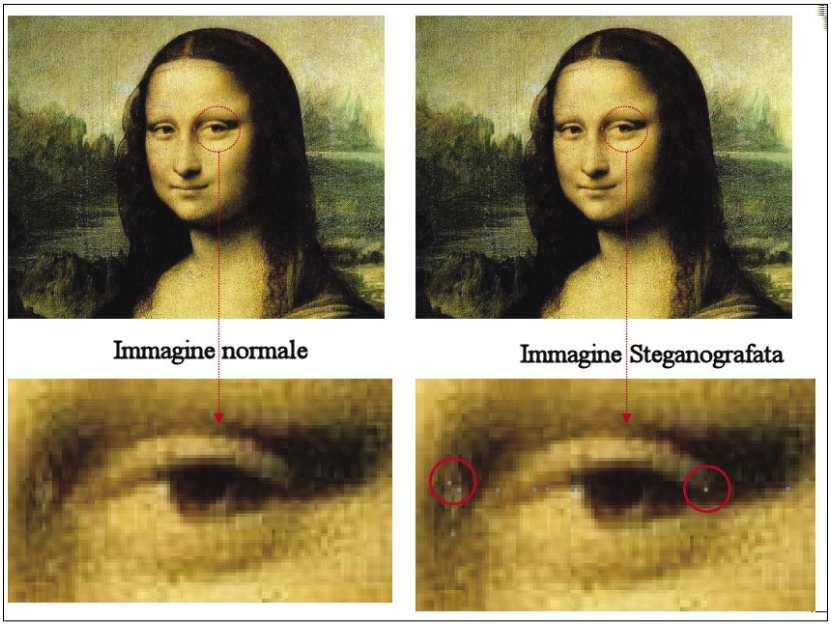

Fig. 2: *Confronto Immagine normale e steganografata*

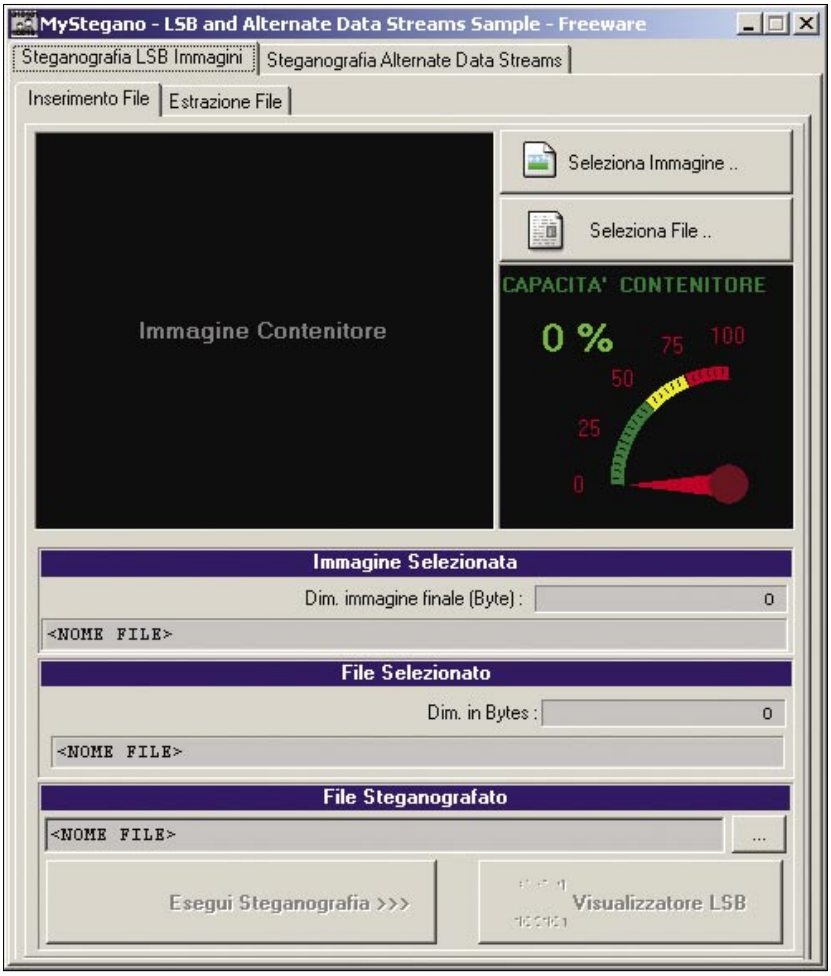

Fig. 3: *Programma MyStegano in esecuzione*

La steganografia delle immagini

Per un computer un'immagine è un insieme di pixel ovvero un insieme di numeri. Un pixel è l'unità grafica più piccola che un computer può gestire su un monitor. Ogni pixel può avere varie intensità di luce e colore. Queste informazioni vengono con l'uso di tre colori primari il Rosso, il Verde ed il Blu (RGB – Red Green Blue). Ogni Pixel ha quindi queste tre informazioni ed ognuna di queste è rappresenta da un Byte. Le immagini più comuni hanno dimensioni 640x480 pixel e sono a 16 Milioni di colori (24 Bit per ogni pixel),

Maggiori sono i Bit a disposizione di un Pixel maggiore è la capacità di nascondere dei dati. Dato che i file contenenti testo, programmi, ecc. sono anche loro un inseme di byte la tecnica usata è quella di prendere un file immagine e un file generico ed inserire quest'ultimo nel file immagine tramite un particolare algoritmo che distribuisce i byte del file generico all'interno del file immagine in maniera che le variazioni che appaiono, quando successivamente si visualizza l'immagine, risultano minime se non impercettibili e la cosa più interessante è che queste "imperfezioni" possono essere tranquillamente scambiate per del *rumore* cioè imperfezioni generate dal sistema di acquisizione come ad esempio uno scanner. L'algoritmo utilizzato per inserire un file generico dentro immagini Bitmap è detto LSB (Least Significant Bit) *algoritmo di inserimento nel bit meno significativo*. Per creare un pixel nero i byte dei tre colori devono essere a 0 (R=0, G=0, B=0) per crearne uno bianco i byte devono avere il valore 255 (R=255, G=255, B=255), variando questi valori è possibile ottenere tutte le sfumature di grigio presenti tra il bianco ed il nero. Ad esempio consideriamo la rappresentazione binaria di un pixel bianco:

```
1111 1111   (Rosso)
1111 1111   (Verde)
1111 1111   (Blu)
```

Adesso consideriamo la rappresentazione binaria di una tonalità di grigio (possiamo ottenerne fino a 256) manipolando il valore del pixel:

```
1001 1100   (Rosso)
1011 0001   (Verde)
1000 0100   (Blu)
```

Variando il Bit meno significativo (il primo gruppo di numeri a destra) nelle tre componenti di colore le caratteristiche del Pixel rimangono sostanzialmente invariate e quindi possiamo utilizzare proprio i Bit meno significativi per *nascondere* Byte del file generico da occultare.

Ecco ad esempio il Pixel precedente modificato :

```
1001 0001   (Rosso)
1011 1111   (Verde)
1000 1001   (Blu)
```

Nella Figura 2 si può vedere un particolare dell'immagine della Gioconda prima di essere steganografata e subito dopo la steganografia, i piccoli punti in grigio (evidenziati con i cerchi rossi) che appaiono rappresentano i byte inseriti ma si notano solo con un ingrandimento dell'immagine e possono essere facilmente scambiate per rumore. Effettuando delle semplici personalizzazioni all'algoritmo come aumentare o dimunire la distanza dei byte modificati nell'immagine è possibile ad esempio rendere più difficile il riconoscimento da parte di un sistema di analisi basato su firme (modelli da utilizzare come campione).

L'algoritmo LSB funziona però solo con formati di immagini tipo Bitmap (BMP) non compresse (quindi hanno dimensioni spesso significative), mentre per formati compressi come ad esempio il JPEG, si usano altre tecniche che sfruttano degli *spazi* all'interno del formato del file. La steganografia in combinazione alla crittografia è uno dei modi più sicuri per trasmettere informazioni (ad es. un file viene prima crittografato e dopo inserito in un file immagine). Recentemente ha fatto scalpore la notizia che i servizi segreti americani siano in grado di rintracciare dal documento cartaceo, le più comuni stampanti laser a colori in commercio, grazie ad uno stratagemma software inserito nel firmware della macchina che stampa sui bordi della pagina minu-

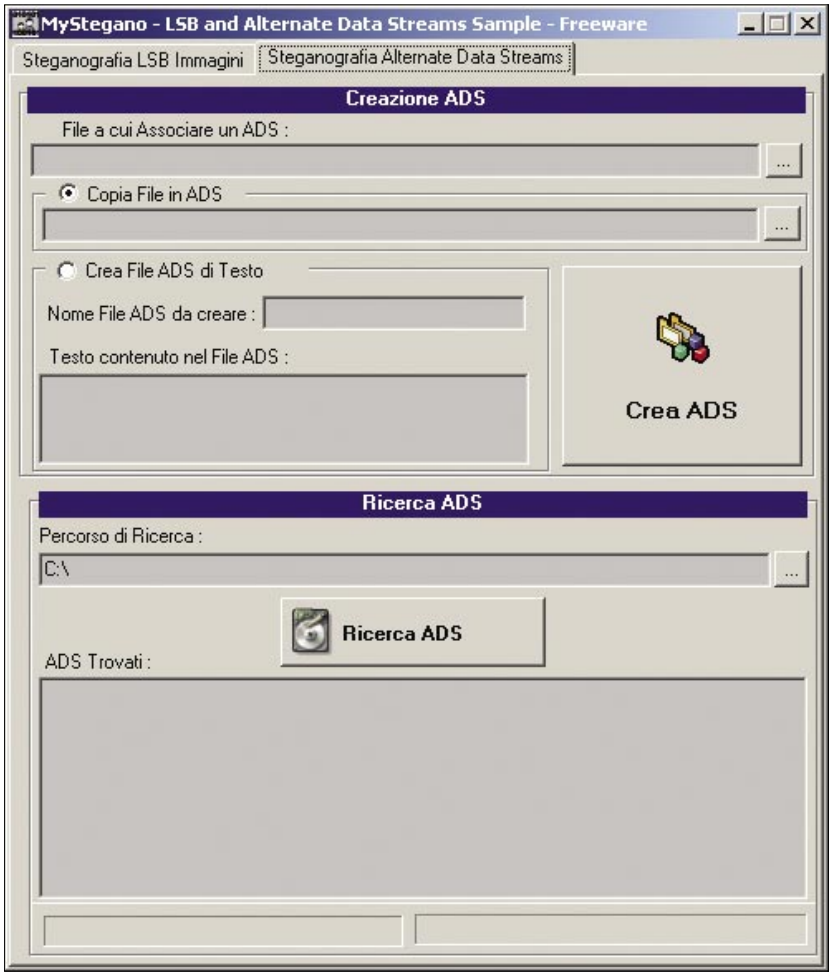

Fig. 4: *Programma MyStegano – Sezione Alternate Data Streams*

scoli puntini gialli quasi invisibili che in maniera codificata contengono data ora e numero di serie della stampante. Un utilizzo interessante della steganografia sulle immagini è quello di difendere la paternità delle proprie opere digitali. Nelle immagini pubblicate su Internet si possono inserire con tecniche di steganografia delle informazioni personali (*watermark*) o dei codici di serie (*fingerprint*) che permettono al proprietario di riconoscere immediatamente se qualcun'altro ha pubblicato o utilizzato su altri siti le sue immagini senza autorizzazione. Per darvi un esempio pratico di come si possa realizzare la steganografia di file generici con file immagini ho relizzato per questo articolo una piccola utility (mystegano.zip) contenuta nel cd rom allegato alla rivista, oppure disponibile al seguente indirizzo: *http://www.arruzzoli.it/hackin9/mystegano.zip*. Lo scopo è puramente didattico e l'utilizzo è molto semplice, scompattate il file mystegano.zip ed eseguite il programma *mystegano.exe* (Fig.3).

Selezionate la linguetta *Steganografia LSB immagini* e *quindi Inserimento File*, con il pulsante *Seleziona immagine.*. selezionate il file immagine (contenitore) che dovrà ospitare il file generico e con il pulsante *Seleziona file*.. selezionate il file generico da nascondere; quindi premete il pulsante *Esegui steganografia*. Il pulsante Visualizzatore LSB vi permetterà di vedere come il file è stato distribuito all'interno dell'immagine. Per estrarre il file selezionate la linguetta *Steganografia LSB immagini* e *Estrazione File*, premete il pulsante *Seleziona immagine* selezionando l'immagine steganografata quindi premete il pulsante *Estrai File Contenuto*. Su Internet ci sono diverse applicazioni che effetuano steganografia come S-Tools o la completa Stegano Security Suite 2006. In modo molto simile alle immagini può essere applicata la tecnica della steganografia anche ai file musicali MP3, utilizzando cioè i file audio come *contenitori* per nascondere file generici, un esempio interessante può essere il programma *mp3stego che* trovare a questo indirizzo: *http://www.petitcolas.net/fabien/steganography/mp3stego/index.html* dove tra l'altro è disponibile anche il codice sorgente. Per i video la tecnica si ripete ed è molto simile alle precedenti (parliamo sempre di steganografia sostitutiva), su internet trovate programmi come StegoVideo che in maniera molto semplice vi permette di inserire file generici in video con formato AVI, è disponibile anche come plugin per il software di video editing Virtual DUB. Un'altra interessante applicazione a cui diversi gruppi di sviluppatori stanno lavorando in tutto il mondo è la steganografia di internet (network steganography è un bel esempio che trovate all'indirizzo: *http://stegano.net/*), utilizzando ad esempio i pacchetti dei servizi ICMP del protocollo TCP-IP per trasmettere informazioni steganografate, oppure di un sito WEB che solo grazie ad un particolare plugin installato sul proprio browser, mostri i contenuti nascosti, completamente diversi da quelli visibili da un normale browser. Un aspetto inquietante che viene spesso sottovalutato è che la steganografia può essere un problema anche per sistemi come gli Intrusion Detection System (IDS) e per i più evoluti Intrusion Detection and Prevention (IDP) in quanto le sue applicazioni sono nella maggior parte dei casi artigianali, realizzate ad hoc, non seguono algoritmi o tecniche particolarmente conosciute e quindi le firme degli IDS come pure i sistemi euristici degli IDP, spesso, non sono in grado di *vederle*.

La steganografia del FileSystem

Altri scenari di applicazioni steganografiche sono ad esempio i filesystem steganografati dove i veri file sono celati all'interno di un altro file system di copertura e possono essere resi visibili solo grazie ad una particolare password. Eppure un filesystem dotato di capacità steganografiche è oggi proprio sotto i nostri occhi e probabilmente, paradossalmente, molti di noi non lo sanno. Mi riferisco al filesystem del sistema operativo più diffuso al mondo quello di Microsoft. L'NTFS (*New Technology File System*) utilizzato in modo particolare dai sistemi operativi windows 2000 e superiori è dotato di una categoria di oggetti detti *Alternate Data Streams (ADS)* nota da molto tempo tra gli addetti ai lavori, ma sconosciuta ai più.

Gli ADS inizialmente sono stati implementati da Microsoft per consentire a Windows NT di essere utilizzato come file-server anche da sistemi Macintosh basati su un altro tipo di filesystem (HFS). Il problema principale è che HFS a differenza di NTFS memorizza per ogni file informazioni supplementari (ad es. Icone, metadati, ecc.) utilizzando una struttura simile ad un ADS. Nel filesystem di Microsoft (NTFS) le informazioni su file e cartelle sono memorizzate in una tabella chiamata Master File Table (MFT). In questa parte del disco ogni file è identificato da un insieme di oggetti detti attributi (il nome assegnato al file, la data di creazione, la data dell'ultima modifica, ecc.), gli ADS permettono di creare e salvare una estensione di questi attributi/meta-informazioni con una elevata possibilità di personalizzazione, in questo modo i sistemi Mac possono operare in modo trasparente sui dati presenti sul server NT. Gli ADS sono quindi un vero e proprio flusso alternativo a quello del file system principale, possono essere file di qualsiasi genere ma anche cartelle, sono invisibili agli utenti ed ai programmi che non li supportano e possono essere eseguiti direttamente. E' bene ricordare che gli ADS sono proprietà di NTFS e che l'associazione ad un file del flusso primario riamane in questo ambito, quindi se si spostano i file del flusso principale su altri filesystem come ad esempio la vecchia FAT32 gli ADS associati verrano persi. In realtà gli ADS sono diventati famosi non

tanto per la loro possibilità di comunicare con i sistemi MAC ma perchè recentemente sono stati scoperti virus, trojan e malicious script che utilizzavano questa tecnologia per rendersi *invisibili*, riuscendo così ad eludere i sistemi di sicurezza come antivirus e anti spyware. Il problema fondamentale è che Microsoft non ha dato nessuno strumento di supporto agli utenti a livello di sistema operativo per verificare la presenza di ADS nei file, per analizzarli e per eliminarli. Di fatto gli ADS risultano praticamente invisibili sia da Esplora Risorse sia dal Prompt del DOS, così ad esempio potremmo trovarci in situazioni dove, un file di dimensione apparentemente nulla, è associato ad un ADS di svariati Gbyte (gli ADS non hanno limiti di dimensione). Per meglio comprendere il loro funzionamento facciamo degli esempi pratici.

In un sistema operativo Windows XP dal Prompt del DOS creiamo una cartella: c:<CharStyle: FOREIGN>adsprova

posizioniamoci nella cartella adsprova e digitiamo: notepad visibile.txt; il notepad ci chiederà di creare il nuovo file visibile.txt dove inseriremo il testo *CIAO ADS* quindi salviamo il file. Eseguiamo da console il comando *DIR* per verificare le dimensioni del `file visibile.txt` e confrontarle successivamente. Se vogliamo creare un ADS associato al file visibile.txt dal Prompt del DOS digitiamo: `notepad visibile.txt:nascosto.txt` anche in questo caso il notepad ci chiederà di creare il nuovo file visibile.txt: nascosto.txt e dove inseriremo il testo *123456* quindi salviamo il file. I due punti (:) rappresentano il collegamento tra i due mondi, il file del flusso principale a quello del secondario (ADS). Se dal Prompt del DOS eseguiamo il comando *DIR* e vedremo che del file *nascosto.txt* non c'è traccia e che le dimensioni del file visibile.txt non sono aumentate ma se eseguiamo il comando: `notepad visibile.txt:nascosto.txt` il file ed il suo contenuto riappariranno. A questo punto per poter trovare l'ADS appena creato dobbiamo utilizzare un programma in grado di farlo. Su internet si trovano diverse utility, in ogni caso potete utilizzare sempre mystegano.exe: Selezionate la linguetta *Steganografia Alternate Data Stream* (Fig.4), nella casella di testo *Percorso di ricerca* del riquadro *Ricerca ADS* inserite C:\ADSPROVA e quindi premete il pulsante *Ricerca ADS*. Una volta visualizzati i file ADS nella lista sottostante è possibile aprirli, estrarli o eliminarli premendo il tasto destro del mouse sull'ADS nella lista e scegliendo l'opzione *Apri File, Estrai File* o *Elimina File*.

Per eliminare da console DOS l'ADS collegato al visibile.txt senza perdere i dati in esso contenuto dobbiamo eseguire un'operazione leggermente complessa.

Cenni sull'autore

Francesco Arruzzoli lavora attualmente per una azienda di telecomunicazioni come responsabile della divisione ICT Security. Progettista di sistemi esperti da più di 15 anni si occupa dello sviluppo di applicazioni per il management e la sicurezza di reti TCP-IP, consulenza, auditing, progettazione ed implementazione di soluzioni per la sicurezza di sistemi informativi complessi. Partecipa, in qualità di relatore, a diversi eventi formativi e divulgativi sulla sicurezza informatica, Ethical Hacker certificato all'E-Council americano (International Council of E-Commerce Consultants), ICT Security expert certificato al CompTIA (Computing Technology Industry Association), esperto indipendente dell'ENISA (European Network and Information Security Agency), membro del Clusit (Associazione Italiana per la Sicurezza Informatica) e dell'AICA (Associazione Italiana per l'Informatica ed il Calcolo Automatico) ha ricoperto in passato ruoli di responsabile software, system engineer e ICT security manager presso aziende di informatica e telecomunicazione, società multinazionali e importanti strutture della sanità italiana.

Terminologia

- *Echelon* - è il nome del sistema di sorveglianza globale da parte di alcuni stati, creato durante la Guerra Fredda. È gestito da Stati Uniti, Regno Unito, Australia, Canada e Nuova Zelanda,
- *Carnivore* - è il nome dato ad un sistema implementato dall'FBI (Federal Bureau of Investigation) che è analogo ad un wire tapping. Con tale sistema le e-mail sono controllate così come le conversazioni telefoniche. È una forma di controllo di polizia.

In Rete

- *http://www.arruzzoli.it/hackin9/mystegano.zip* – Utility per steganografare con le immagini,
- *http://www.eff.org/Privacy/printers/docucolor/* – Metodo di decrittazione dei codici delle stampanti,
- *http://www.ol-service.com/sikurezza/crittografia/S-tools4.zip* – Software per la Steganografia S-Tools,
- *http://www.steganos.com/* – Software per la Steganografia Steganos Security Suite 2006,
- *http://compression.ru/video/stego_video/index_en.html* – Software per la Steganografia StegVideo,
- *http://www.heysoft.de/Frames/f_sw_la_en.htm* – Utility per trovare gli ADS,
- *http://unxutils.sourceforge.net* – Utility per estrarre gli ADS,
- *http://www.securityfocus.com/infocus/1822* – approfondimento tecnico su ADS,
- *http://msdn.microsoft.com/library/default?url=/library/en-us/dnfiles/html/ntfs5.asp* – dettagli tecnici dal sito della microsoft.

Rinominiamo il file:

```
ren visibile.txt temp.txt
```

copiamo il contenuto da temp.txt su un nuovo file visibile.txt:

```
type temp.txt > visibile.txt
```

eliminiamo il file temp.txt:

```
del temp.txt
```

Come abbiamo detto in precedenza gli ADS possono essere associati anche a cartelle e se ad esempio volessimo associare un ADS alla cartella adsprova dal Prompt del DOS digitiamo:

```
echo "incredibili ADS" ?adsprova?>
:nascosto.txt
```

Adesso l'ADS è stato associato. L'unico modo per eliminare l'ADS è quello di cancellare la cartella e questo può essere un problema, se l'ADS è stato associato alla cartella root (ad. es. c:\) si deve formattare l'unità logica.

E' inoltre possibile l'esecuzione diretta di ADS eseguibili (file eseguibili collegati magari a file di testo).

Ad esempio creiamo un file test.txt ed inseriamoci il testo *prova* successivamente copiamo nella nostra directory *c:\adsprova*, per sicurezza, il file *c:\windows\notepad*.exe e associamo un ADS *test.txt* contenente notepad.exe semplicemente in questo modo:

```
type notepad.exe>test.txt:notepad.exe
```

Se eseguiamo il comando `DIR` possiamo verificare che le dimensioni del *file text.txt* non sono variate.

Per eseguire direttamente l'ADS possiamo utilizzare il comando start con la seguente sintassi:

```
start c:\adsprova\test.txt:notepad.exe
```

Il comando start esige il percorso completo del file da eseguire.

Sfruttando questa semplice caratteristica dei : punti si potrebbe ad esempio occultare file video con l'ormai classica sintassi:

```
type "c:\windows\clock.avi" >
"visibile.txt:clock.avi"
```

quindi utilizzando il Media Player di Micrsoft per vedere il video:

```
C:\Program Files\Windows Media Player
\wmplayer.exe" "c:\visibile.
txt:clock.avi
```

Se invece volete estrarre il file da un ADS potete utilizzare oltre a Mystegano.exe altre utility freeware disponibili su internet come il porting su windows del famoso comando cat di Unix. Cat.exe lo potete trovare a questo indirizzo: *http://unxutils.sourceforge.net* ed il suo utilizzo è molto semplice, se ad esempio volessimo estrarre clock.avi da `c:\visibile.txt:clock.avi` dovremmo utilizzare il seguente comando:

```
cat "c:\visibile.txt:clock.avi">
"clock.avi"
```

Con l'utility Mystegano.exe potete creare dei file ADS Selezionando la linguetta *Steganografia Alternate Data Stream* (Fig.4), e nel riquadro *Creazione ADS* selezionate il file a cui associare l'ADS nella casella di testo File a cui associare ADS. Quindi potete scegliere di creare un ADS con un file esistente selezionandolo nella casella di testo Copia file in ADS oppure creare direttamente un file di testo selezionando l'opzione *Crea File ADS di testo*, inserendo il nome del file da creare nella casella di testo *Nome file ADS* da creare e il testo contenuto nella casella di testo *Testo contenuto nel file ADS per creare* l'ADS premete Crea ADS. E' bene ricordare che gli ADS sono stati concepiti per ragioni completamente diverse da quelle steganografiche e il fatto che possano essere usati anche per questo tipo di applicazione è solo un accidente logico; le applicazioni steganografiche con gli ADS sono note a molti e molti sono i tools in grado di individuarli nei filesystem, quindi non possono essere considerati un metodo innovativo e sicuro per fare steganografia ma solo uno dei tanti fantasiosi metodi. L' utilizzo della steganografia forse più che la Crittografia ha da sempre ossessionato le strutture governative deputate al controllo della sicurezza nazionale in quanto ragiona con tecniche e modelli completamente diversi, non catalogabili e quindi difficilmente identificabili per sistemi automatici di analisi delle comunicazioni come Echelon o Carnivore. In alcuni forum sulle problematiche di sicurezza sembra che addirittura ci sia una sorta di *complotto* dei vari servizi segreti nel fare disinformazione e nello scoraggiare le ricerche e l'uso della steganografia. Come per la crittografia questi algoritmi se utilizzati da criminali potrebbero rivelarsi estremamente pericolosi e potrebbero rendere più difficile per le forze dell'ordine combatterli. Ma il problema fondamentale è che l'onesto cittadino deve avere la possibilità di proteggere la propria privacy e questo compito non può essere delegato ad altri (altrimenti non sarebbe più privacy) ed in ogni caso i criminali di norma non obbediscono alle leggi, quindi vietare l'uso della crittografia o della steganografia non ha senso, togliendo tra l'altro, dei validi strumenti al cittadino onesto. Detto questo però va ricordato che esiste un etica professionale che impone sopratutto a chi opera nell'ambito della sicurezza, di agire nel rispetto degli altri e delle cose altrui, quindi non sempre è possibile divulgare informazioni dettagliate su argomenti che potrebbero, in maniera certa, creare gravi problemi di sicurezza, ad esempio se si scopre un exploit, una falla su un sistema operativo o un'applicazione che possono arrecare gravi danni agli utilizzatori è imperativo (tralasciando tutte le implicazioni legali a cui si può andar incontro) che tali informazioni siano immediatamente comunicate al produttore affinchè rilasci la relativa patch risolutiva e che fino a quel momento rimangano assolutamente riservate. ●