Steganografia: evoluzione digitale dell’antica arte di occultare le informazioni, da strumento di riservatezza a strumento di offesa per dispositivi mobili

Date : 15 settembre 2017

A volte sembra così improbabile che tecniche inventate ed utilizzate migliaia di anni fà possano aver contribuito così significativamente allo sviluppo di internet. Pensiamo ad es. alla crittografia usata fin dai tempi degli egiziani e senza la quale tutto lo sviluppo delle odierne reti telematiche e del moderno mercato economico non sarebbe stato possibile.

Anche la steganografia ha origini antichissime ma a differenza della crittografia che ha come obiettivo quello di rendere inaccessibili i dati a chi non conosce la chiave, la steganografia ha lo scopo di mantenere nascosta l'esistenza dei dati a chi non conosce la procedura atta ad estrarli. Anche se meno nota, questa tecnica ha trovato in internet una rilevanza ed un utilizzo elevato.

Spesso ricordata come strumento di comunicazione dei terroristi di Al Qaida che sfruttavano i file mp3, al tempo in piena proliferazione su internet grazie a Napster, come contenitori per veicolare i loro messaggi, la tecnica steganografica in ambito informatico ha trovato miriadi di applicazioni e non è stata solo applicata a file audio ma anche ad immagini, video e a diverse altre tipologie di dati come ad es. interi filesystem.

Un elemento in più di cui la steganografia dispone per le sue applicazioni è, a mio parere, la creatività nel trovare i campi di applicazione che non richiedono necessariamente la capacità di progettare complessi algoritmi matematici come spesso accade con la crittografia. Un tipico esempio di questo è quando nell’ anno 2000 fu presentato il nuovo sistema operativo di Microsoft: Windows 2k Server, un evento obiettivamente rilevante, visto che il nuovo sistema operativo introduceva nuove funzionalità che avrebbero influenzato le modalità di gestione dei sistemi ICT, come ad es. Active Directory che permetteva la gestione e l'amministrazione di reti aziendali anche di grandi dimensioni in maniera centralizzata. Tra le altre funzionalità fu annunciata la compatibilità del nuovo filesystem Microsoft (NTFS) con i sistemi Macintosh basati sul filesystem HFS, grazie all’implementazione di una tecnologia denominata Alternate Data Stream (ADS). Anche se l’utilizzo pensato da Microsoft per questa tecnologia non fù un vero e proprio successo, al contrario negli ambienti underground della rete ebbe un intenso utilizzo in ambito steganografico. L’ADS estende la possibilità di associare nuovi attributi (meta-

informazioni) di dimensioni praticamente illimitate ai file presenti su NTFS. Questo crea una sorta di filesystem parallelo nascosto in cui è possibile salvare file che restano “invisibili” al sistema operativo.

Un Proof of Concept per dimostrare in maniera semplice ed efficace l’utilizzo della steganografia tramite l’ADS è il seguente:

1. Aprite una finestra di Prompt DOS, create una cartella di prova (ad es. test) digitando il comando: **mkdir test** ed entrate nella cartella test con il comando: **cd test** (Fig.1) .

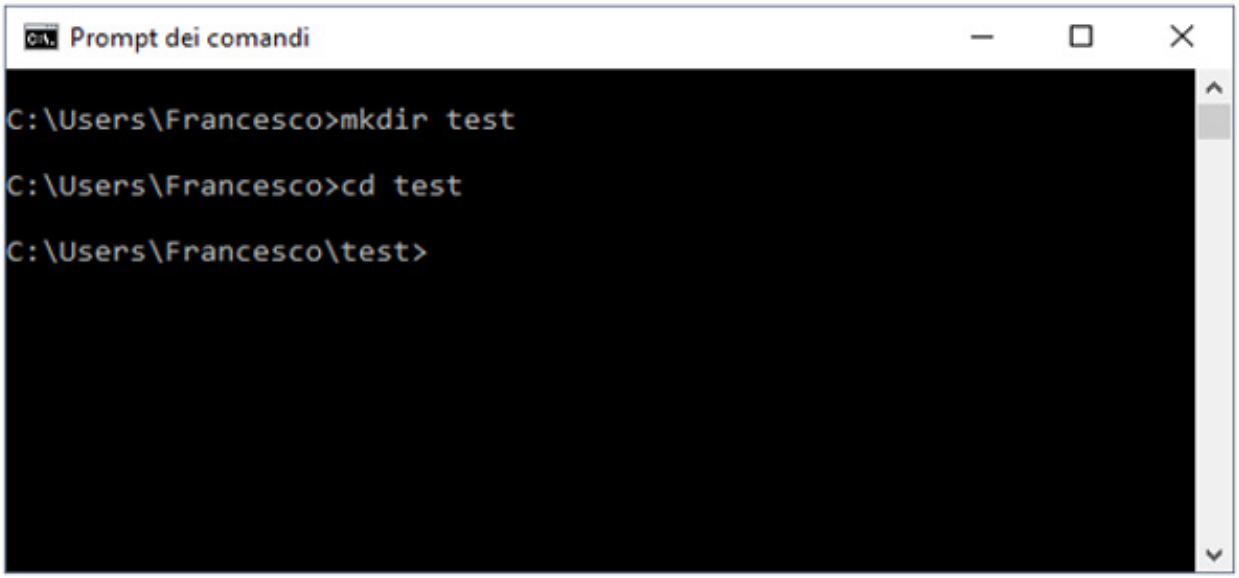

Fig.1

2. Digitare il comando: **notepad.exe visibile.txt** (Fig.2), quando appare una finestra di dialogo per la conferma di creazione del file visibile.txt premere il pulsante SI.

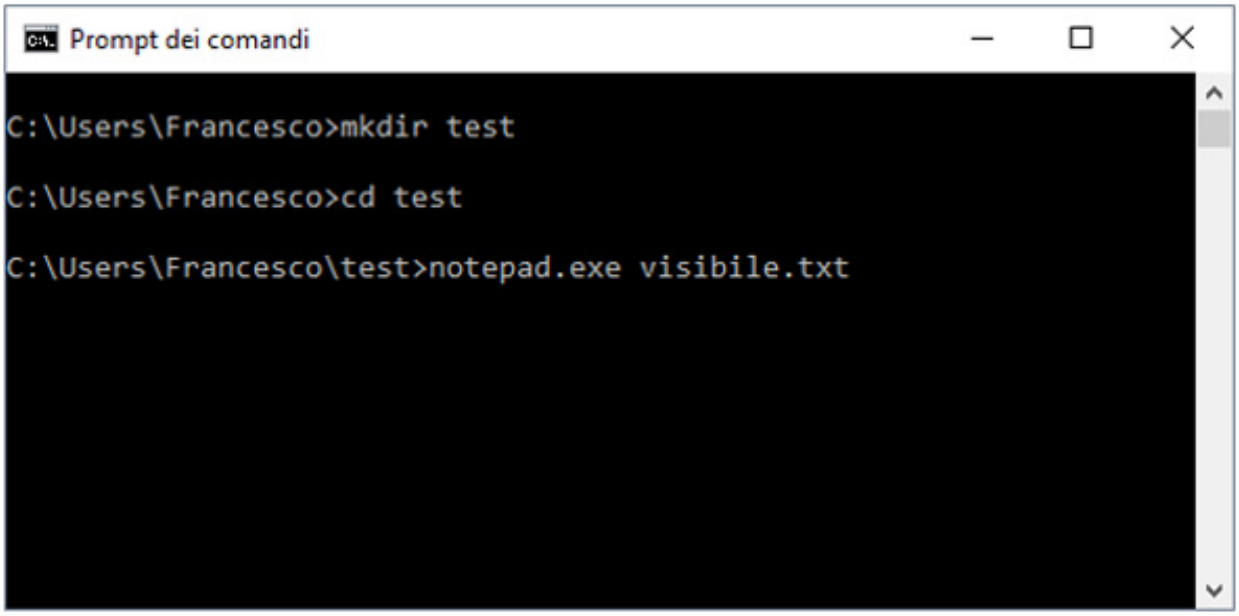

Fig.2

3. Scrivete nel file visibile.txt del testo, ad esempio “ABCDEFGHILMNO”, salvate il file e chiudete l’applicazione notepad. Adesso se si rilancia il comando **exe visibile.txt** il file verrà aperto e mostrerà il testo appena inserito.
4. Dal Prompt DOS digitate ora il comando **exe visibile.txt:segreto.txt** l’applicazione notepad si aprirà e vi chiederà nuovamente di creare il file, rispondete ancora SI. Vi troverete davanti un file vuoto in cui potete scrivere altro testo ad es. “12345678”, salvate il file e chiudete l’applicazione notepad. A questo punto avete appena generato un file sul “filesystem nascosto” di NTFS, utilizzando i normali tool di ricerca non troverete alcun file segreto.txt, visibile.txt:segreto.txt o il suo contenuto , il file apparentemente non esiste. Per riaprirlo digitate nuovamente il comando **notepad.exe visibile.txt:segreto.txt** (Fig.3).

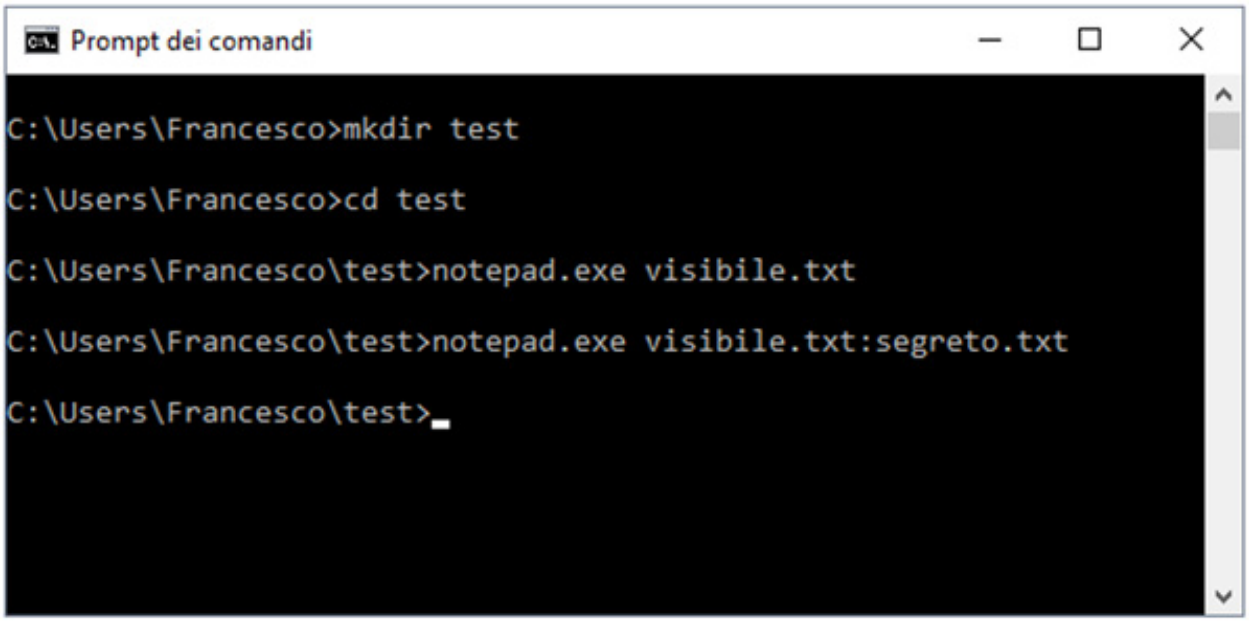

Fig.3

In questo caso i due punti (:) sono di fatto “la chiave” per accedere al file system nascosto di ADS ed il file iniziale (visibile.txt) rappresenta l’indice da utilizzare per aprire i file nascosti . Il file visibile.txt può generare l’accesso ad infiniti altri file (ad es. segreto1.txt, etc..). Sfruttando tecniche simili è possibile nascondere non solo file di testo ma di qualsiasi tipologia (immagini, video, eseguibili, etc..) , un nascondiglio spesso utilizzato anche da malware e virus nel tentativo di sfuggire ai sistemi antivirus.

Fino ad oggi le tecniche di steganografia sono sempre state utilizzate per nascondere informazioni, ma recentemente un esperimento effettuato da un gruppo di ricercatori dell’università di Berkeley in California ha dimostrato come la steganografia possa diventare una componente attiva per realizzare un attacco, nell’esperimento in questione, in particolare, un attacco alle interfacce vocali presenti sui dispositivi mobili.

L’esperimento dimostra come i dispositivi mobili possono essere attaccati con comandi vocali nascosti, inintelligibili agli ascoltatori umani ma interpretati come comandi da parte dei dispositivi, comandi che potrebbero ad es. far scaricare un file (malware) ed eseguirlo. L’attacco sfrutta una prima tecnica di offuscamento del comando vocale e successivamente una seconda tecnica di inserimento del suono offuscato come rumore di fondo in altre tracce audio, ad es. un video su Youtube, la vittima guardando il video potrebbe far inviare dei comandi vocali al suo dispositivo mobile. L’esperimento risulta molto interessante in quanto la tecnica steganografica utilizzata per offuscare l’audio da una parte nasconde all’essere umano la comprensione delle parole dall’altra comunica direttamente “in chiaro” con il dispositivo mobile. Per realizzare un audio offuscato i ricercatori hanno utilizzato CMU Sphinx una piattaforma open source di riconoscimento vocale per applicazioni mobile, tramite una sua libreria specifica hanno applicato un processo di modifica del suono (Mel-Frequency Cepstrum)

in grado di ridurre l’input audio in un spazio dimensionale più piccolo, successivamente hanno applicato un modello di gaussiano (GMM) per calcolare le probabilità che un dato pezzo di audio corrisponda a un determinato fonema.

Il risultato è che il cervello umano se non sa quale frase cercare nel suono che sente nella maggior parte dei casi non capisce il contenuto di quello che viene concepito come un rumore, mentre i dispositivi mobili che lavorano con algoritmi probabilistici per riconoscere le parole traduco il rumore in parole e quindi comandi. Per chi volesse maggiori dettagli tecnici sullo studio svolto potrà trovare i riferimenti nel paragrafo dei suggerimenti bibliografici, per chi invece non ha tempo ma vuole capire il meccanismo con cui la mente umana può essere ingannata possiamo semplificarlo con il seguente esempio :

1. Guardate questa immagine:

2. Adesso guardate questa immagine:

3. Infine guardate le due immagini vicine, adesso il cervello percepirà nell’immagine di sinistra delle caratteristiche dell’immagine di destra. In modo similare questo accade con i file audio offuscati.

Il video dimostrativo dell’esperimento è senza dubbio interessante:

Questo proof of concept apre le porte a diverse riflessioni, la prima è che ad oggi non esiste

una difesa per ipotetici attacchi di questo tipo, la seconda è che in un mondo in cui i sistemi informatici ed i dispositivi connessi ad internet cominciano ad interagire con gli esseri umani e tra loro in modalità diverse da quelle tradizionali, ad es. con linguaggi naturali come la voce, il paradigma della sicurezza ICT tradizionale fallisce e necessita di nuove strategie e strumenti per poter affrontare le minacce emergenti. Ultima considerazione rimane quella che nel caos di un mondo digitale fatto sempre più di Big Data e di oggetti connessi in rete, la steganografia dispone di un terreno applicativo sempre più fertile e che a differenza della cugina crittografia, palesemente manifesta, la steganografia può sempre più obnubilarsi nella rete e nei dati, custodendo gelosamente i segreti che gli saranno affidati.

Suggerimenti Bibliografici

url

- http://www.hiddenvoicecommands.com/
- https://www.youtube.com/watch?v=HvZAZFztlO0

Riferimenti

- Nicholas Carlini, Pratyush Mishra, Tavish Vaidya, Yuankai Zhang, Micah Sherr, Clay Shields, David Wagner, and Wenchao Zhou. Hidden Voice Commands. In USENIX Security Symposium (Security), August 2016.
- Tavish Vaidya, Yuankai Zhang, Micah Sherr, and Clay Shields. Cocaine Noodles: Exploiting the Gap between Human and Machine Speech Recognition. In USENIX Workshop on Offensive Technologies (WOOT), August 2015

A cura di: **Francesco Arruzzoli**