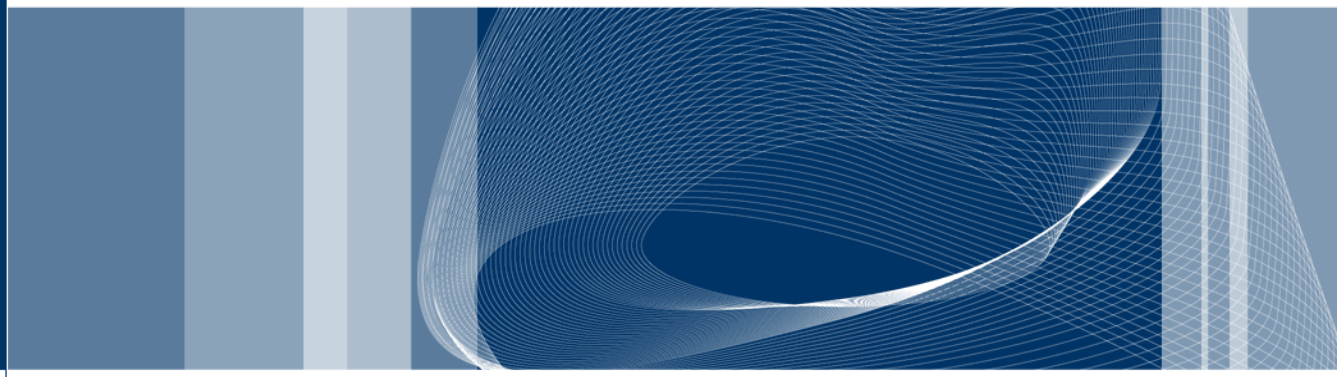
POLITECNICO DI MILANO



Anti-forensics: come ti sfuggo ai RIS

Ing. Stefano Zanero, PhD
Dip. Elettronica e Informazione – Politecnico di Milano

Ricapitolando...

- Obiettivo della forense: ricostruire “cosa è successo”
- Obiettivo più preciso: applicare metodi scientifici (=ripetibili) di analisi alle evidenze informatiche al fine di produrre delle prove
- Fasi
  - Raccolta dell'evidenza (acquisizione)
  - Identificazione delle prove
  - Valutazione ed analisi tecnico/legale
  - Presentazione dei risultati

Elementi critici

- Quali fasi dipendono significativamente dalla tecnologia ?
  - Raccolta dell'evidenza: uso di tool per l'acquisizione quanto più possibile ripetibile delle fonti di prova, e per la loro custodia e verifica
  - Identificazione delle prove: uso di tool per l'analisi e la ricostruzione, tipicamente, da file system
- Interferendo si può compromettere l'analisi
  - Transitoriamente: se si interferisce con la fase di identificazione in modo ovviabile
  - Definitivamente: se si interferisce con la fase di acquisizione, o comunque si modifica l'evidenza in modo non ovviabile

Anti-forensics: definizione

- Insieme di tecniche che mirano a confondere i tool, o usare i tool e i loro risultati per confondere l'analista forense
- Alcune, come vedremo, “fantascientifiche”, altre già incarnate in semplici tool
- Andiamo a colpire dove fa male
  - Scala dei tempi
  - Log
  - Ricupero di file cancellati
  - Identificazione di file ed eseguibili
  - Steganografia e metodi per nascondere dati

Timeline...

- I tool di analisi utilizzano gli indicatori MAC(E): Modified, Accessed, Changed, (Entry Changed: valore di controllo di NTFS)
- Andiamo a modificarli al fine di non far comparire “vicini” gli eventi di cui vogliamo nascondere la correlazione. Possiamo randomizzarli o cancellarli del tutto...
- Tool: “timestomp” (MACE) o “touch” (MAC)
- EnCase ci casca tranquillamente...
- Palliativo: confrontare gli attributi SIA (Standard Information Attributes) con quelli FN (FileName), cambiati solo al momento della creazione del file

Log analysis

- Analisi dei log: tipicamente con engine realizzati per analizzare “certi” formati (e.g. testo)
- Modifichiamo i log non solo editandoli, ma anche appendendo dati malformati (e.g. caratteri non stampabili)
- Se vengono usati vari tool con regular expression, si possono sfruttare bachi di questi tool per iniettare codice in vari modi

Recupero di file cancellati...

- Spesso forense = lettura delle ceneri
- Spargiamole queste ceneri !
  - Uso di tool di secure delete (heide, sysinternals sdelete, etc)
  - Wiping dello spazio non allocato
  - ... deframmentazione, anche...
    - Nota: alcune utility di secure delete non funzionano, sappiatelo...
- Nota: le fantascientifiche letture dei “residui di magnetizzazione”, a la Gutmann, paiono essere appunto fantascienza: se è sovrascritto è andato. Punto.

FISTing (cough...)

- Filesystem Insertion and Subversion Technologies
- Mettiamo i dati dove non c'è ragionevole motivo per guardare
  - Infiliamoli DENTRO i metadati del filesystem
  - FSCK è il nostro nemico: potrebbe aggiornare/riparare i metadati
  - 32 KB di dati smanettando dentro la tavola delle partizioni (non molto)
  - Nel file system EXT(2/3)
    - RuneFS: scrive nell'inode dei bad block (spazio illimitato)
    - WaffenFS: aggiungiamo un finto journal di EXT3 ad EXT2 (fino a 32 MB di storage)
    - KY FS: usa gli inode delle directory infilandoci dei dati, illimitato
    - Data Mule FS: infila i dati nel padding e nelle strutture dei metadati del FS (ignorati dai tool di forense), fino a 1MB sul file system tipico

Giocare con le partizioni

- Come la vostra colf nasconde la polvere sotto il tappeto, nascondiamo l'evidenza sotto il filesystem
- Smanettamento della tavola delle partizioni
  - Disallineamento delle partizioni
    - Usiamo un tool per il ripristino di partizioni per leggerle
  - Molteplicità di partizioni estese
    - Windows e Linux le tollerano, EnCase no...
  - Generiamo molte partizioni nell'estesa
    - Per n sufficientemente grande i tool muoiono

E se cercano tutti i file di un CERTO tipo?

- Encase usa due metodi base per identificare il tipo di file
  - L'estensione (oh, yeah !)
  - Una firma fissa (meglio ancora)
- ... Scommettiamo che con due righe di file bash non troverai mai una singola immagine pedopornografica sul mio disco ?
- Soluzione: usare firme più flessibili ed avanzate per identificare i file

“Cosa farà mai questo bel malware?”

- Alzi la mano chi ha voglia di decompilare un eseguibile ignoto per capire cosa fa
  - “gdb may be your friend... surely not mine!”
- Di solito si usano metodi molto barbari (strings, etc.)
- Come ingannare questi metodi base
  - Usare un packer (non funziona più strings)
  - Usare un loader custom

Liste di proscrizione e relativi ammenicoli

- Utilizzo di hash per identificare i file “known bad”
  - Dobbiamo proprio spiegarvi che basta modificare o appendere dei dati inutilizzati per falsare l'hash ?
- Utilizzo di hash per identificare i file “known good”
  - Ehm, quale hash ? MD4, MD5, SHA-1 consentono tutti di trovare collisioni...
  - Esistono dei tool per farlo (pubblici, per MD5; privati, per SHA-1) http://www.stachliu.com/research_collisions.html
- Morale della favola: non fidatevi degli hash, o usate algoritmi multipli (e/o confronti bit per bit) per sicurezza

Ghost in the shell

- Certe informazioni sul disco semplicemente non ci sono
- Esempio: il meterpreter di Metasploit (simili: Mosdef, IMPACT)
  - Si inietta nello spazio di memoria di un processo
  - Non scrive nulla su disco
  - Consente di aggiungere thread, eseguire codice...
- Quindi ?
  - Quindi se spegni la macchina l'evidenza è persa
  - ... e qual è la prima cosa che fai se pensi che una macchina sia compromessa ?
  - Per la memory forensics: Windows Memory Forensics Tool (M. Burdach) e memdump

Conclusioni

- L'analisi forense ha il fine di produrre prove chiare e robuste
- L'antiforense mira a ridurre il numero di prove (ridurre l'evidenza) e a renderle incerte o contestabili
- Su cosa va a colpire l'antiforense
  - Mancanza di **tempo** da parte del team di analisi: se l'evidenza è nascosta viene ignorata
  - Mancanza di **conoscenze** da parte del team di analisi che si basa solo sulle interfacce grafiche del tool-da-10000-EUR preferito
  - Colpa in **algoritmi**, **interfacce**, **procedure** ed **omissioni** da parte dei tool (mea culpa, mea culpa, mea maxima...)

Conclusioni (vere)

- Più si diffonderà l'uso dell'analisi forense a fini di contrasto e repressione della criminalità informatica, più si diffonderanno e automatizzeranno le tecniche di antiforense
- Contrastare l'antiforense
  - Dare **tempo** al team di analisi, evitare indagini con migliaia di supporti su cui fare la pesca dei tonni
  - Dare/richiedere **conoscenze** al team di analisi: chi si fida del tool-da-10000-EUR perché non saprebbe farne a meno, è bollito
  - Migliorare i tool di analisi e magari scegliere tool **di cui si possa capire il funzionamento** (open source, anyone ?)
- Nessun tool, a nessun prezzo, può trasformare una persona in un analista forense

Riferimenti

- MAFIA: MetaSploits Anti Forensics Investigation Arsenal
  http://metasploit.com/projects/antiforensics/
- Mariusz Burdach Forensics Tools
  http://forensic.seccure.net/
- Brian Carrier, “File System Forensic Analysis”, Pearson
  http://www.digital-evidence.org/