Hacking, crimine informatico e investigazioni digitali

Prof. Avv. Giovanni Ziccardi

Università degli Studi di Milano

VENEZIA, 9 novembre 2012

Digital Investigation 7 (10/2010)

The Digital Crime Tsunami

di Greg Gogolin

Si tratta di un Articolo che cerca di "fotografare" lo "stato" corrente delle **investigazioni digitali** e della criminalità informatica in **Michigan** al fine di fare, poi, una sorta di "proiezione" complessiva a livello federale.

Michigan: circa 10.000.000 di abitanti e **Detroit** ("I'm from Detroit...").

Le conclusioni

- Prospetta un futuro **critico**.
- Prospetta un **peggioramento** sensibile nei prossimi anni circa la "capacità di investigare".
- Prospetta un cambiamento radicale nelle tecniche investigative.
- Prospetta alcuni problemi imprevedibili, o "comportamenti" informatici, capaci di diffondersi in tempi molto **rapidi**.
- Rischio di non riuscire ad adattare le tecniche investigative e il sistema legale ai cambiamenti e alle nuove minacce.

La c.d. *digital component*

- Nel 2009 negli USA c'è stato il "**sorpasso**". Oltre il 50% dei casi criminali ha una componente digitale.
- C'è un problema di **arretrato**: anche i casi digitali si accumulano.
- Ci sono i **tre fattori critici** da tenere sempre in considerazione:
  - 1. Il numero di **crimini** con componente digitale;
  - 2. Il numero di casi che un investigatore **può trattare** in un anno;
  - 3. Il numero di investigatori **disponibili.**

Time

- In una investigazione digitale occorrono dalle **4 alle 8 ore** solo per fare una **immagine** (copia forense) di un computer tipico, che è l'imprescindibile passo iniziale. Ma dopo? Ci deve essere almeno una analisi di base. Media: **40** ore.
- Non teniamo in considerazione: device non comuni o non conosciuti dall'investigatore, storage esterno, crittografia, incompatibilità con il software di forensics utilizzato dall'investigatore o altre cose che possono allungare i tempi della investigazione.
- Michigan: 35 casi digitali l'anno che può curare bene l'investigatore, in media (full time digital investigator).

Prima nozione tecnica: immagine

La nozione di immagine, o copia clone, è cardine delle modalità pratiche di investigazione digitale.

Si può effettuare con **software** o con **hardware**, richiede preventivamente il blocco in scrittura del dispositivo (write blocking) e consiste in una "fotografia" su altri supporti (dischi identici a quello trovato sulla scena del crimine) che riproduce ogni singola parte del disco (non solo cartelle o *file* ma anche spazi non utilizzati, nascosti, partizioni, aree non visibili).

Time with cell phone

- Un telefono cellulare o altro apparato complesso aumenta il tempo necessario rispetto a un computer.
- I telefoni cellulari stanno aumentando sensibilmente, e ciò porterà a un aumento del tempo necessario.
- A ciò si aggiungono altre tecniche da elaborare come la triangolazione delle celle, l'analisi del traffico, che aggiungono ancora tempo.
- Olgettina docet...

Secondo problema tecnico

- Il trattamento di un telefono cellulare (soprattutto moderno, che è un vero e proprio computer)
- Tre fonti di prova: il telefono, il telefono del "ricevente", il provider di servizi telefonici (tabulati/ dati di traffico)
- Vi sembrerà strano, ma il problema principale per l'investigatore è di collegamento (cavetti) perché ogni cellulare è tendenzialmente "chiuso" (non parliamo degli iPhone) ma i dati sono spesso in chiaro, quindi il principale problema è **dialogare con il dispositivo**.

Automazione?

- Ovvio che la complessità porta alla necessità di automazione…
- Elogio dei tools per l'automazione (Casey, DI April 2011, "The increasing need for automation and validation in digital forensics").
- Rapporto tra automazione delle indagini e garanzie processuali / trasparenza / possibili errori.
- Troiano/hacker/virus di stato anche in Italia.
- Microsoft ha annunciato **una impronta digitale evoluta** delle immagini pedoporno.

Formazione specifica e costi

- Michigan: 34% degli investigatori ha seguito un percorso formativo di 1 anno o 2 anni sulle investigazioni digitali.
- Costi di laboratorio: attrezzature, software, formazione specifica, hardware: aumenta il crimine digitale ma aumentano anche i fondi per combatterlo?
- Esperienza milanese: grande interesse "trasversale" di tutti i soggetti coinvolti nelle investigazioni digitali ma non facile coordinamento tra approcci, strategie e "filosofie".

+50% digital component USA

- Computer / Telefoni cellulari / GPS / Console per videogiochi / Fotocamere e telecamere digitali / iPod / Telecamere per sorveglianza
- 276 milioni di telefoni cellulari in USA nel 2009.
- Il 76% della popolazione ha un personal computer.
- Problema recente: una **lingua straniera** che entra nelle investigazioni anche digitali.

Il problema (e concludo)

- La crescita nel nostro settore non è in un certo senso prevedibile o puramente "aritmetica" ma è **esponenziale** con picchi sovente imprevedibili.
- Non basta sapere quanti messaggi sono stati scambiati l'anno precedente o quanti cellulari sono stati esaminati, il futuro è spesso oscuro.
- Si pensi a fenomeni nati "all'improvviso": gambling online, droghe e farmaci online, frodi e phishing.

Il futuro

- (1) Oscurità o trasparenza? Anche nell'uso dei tools e delle procedure. Replicabilità di ciò che viene fatto in laboratorio. O nelle indagini sotto copertura.
- (2) Automazione o "cara, vecchia **manualità**" nell'investigazione? Attenzione alle capacità di ingannare la macchina (anti-forensics).
- (3) Dominio della componente digitale anche in casi criminali **tradizionali**, con conseguente rischio di **sovra-stimare** la fonte di prova digitale?
- (4) Unione definitiva tra dati di traffico e **contenuto**, già attuata con posta elettronica e con la migrazione verso il digitale, e sempre maggiore confusione (o unità) tra i tipi di intercettazione?