Live Forensics e Incident Response

Digital Investigations 2012/2013

Pavia, 3.4.2013

Davide Gabrini
Forensic Jedi

Università degli Studi di Pavia – Facoltà di Ingegneria
3 aprile 2013

Live Forensics e Incident Response

Davide Gabrini
Forensic Jedi

Chi sono

Davide 'Rebus' Gabrini

Per chi lavoro non è un mistero.

Oltre a ciò:

- Consulente tecnico e Perito forense
- Docente di sicurezza informatica e computer forensics per privati e P.A.
- Socio IISFA, DEFTA, Tech&Law fellow
- Certificazioni CIFI, ACE, AME

Come vedete **non** sono qui in divisa.

Live Forensics e Incident Response

Davide Gabrini

Forensic Jedi

Agenda

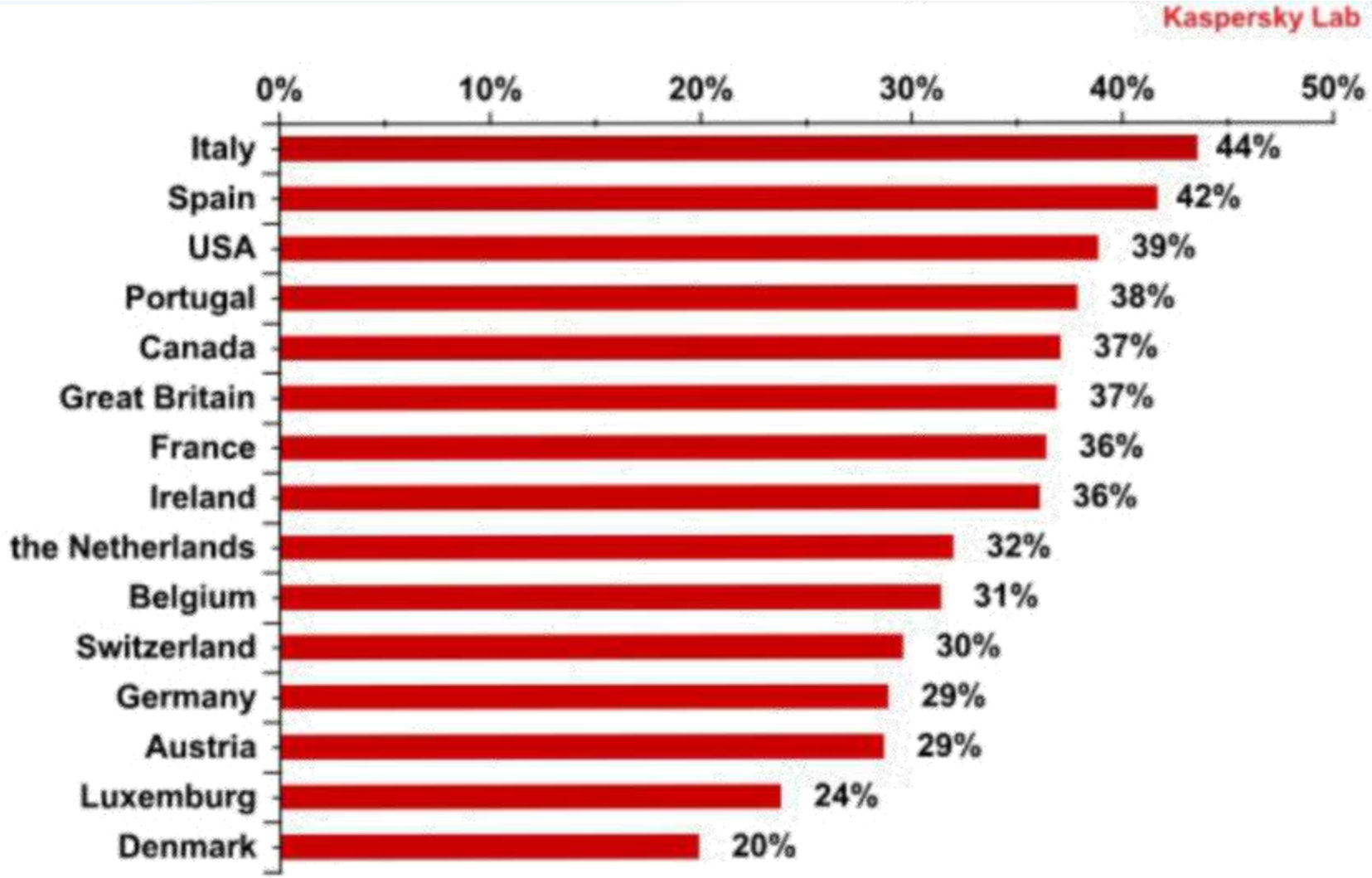
- Cybercrime e incidenti informatici
- Incident Response
- Normativa di riferimento
- Operazioni on-site
- Necessità e opportunità di accertamenti live
- Live Forensics e sue best practice
- Strumenti disponibili

Live Forensics e Incident Response

Davide Gabrini

Forensic Jedi

Incidenza del cybercrime in Italia



Live Forensics e Incident Response

Davide Gabrini

Forensic Jedi

Incidenza del cybercrime in Italia

Live Forensics e Incident Response

Davide Gabrini

Forensic Jedi

Incidenza del cybercrime in Italia

Figure 20. The locations with the most computers reporting detections and removals by desktop antimalware products in 1H12

(Fonte: Microsoft Security Intelligence

	Country/Region	1Q12	2Q12	Chg. 1Q to 2Q
1	United States	9,407,423	12,474,127	32.6% ▲
2	Brazil	3,715,163	3,333,429	-10.3% ▼
3	Korea	2,137,136	2,820,641	32.0% ▲
4	Russia	2,580,673	2,510,591	-2.7% ▼
5	China	1,889,392	2,000,576	5.9% ▲
6	Turkey	1,924,387	1,911,837	-0.7% ▼
7	France	1,677,242	1,555,522	-7.3% ▼
8	United Kingdom	1,648,801	1,509,488	-8.4% ▼
9	Germany	1,544,774	1,486,309	-3.8% ▼
10	Italy	1,361,043	1,341,317	-1.4% ▼

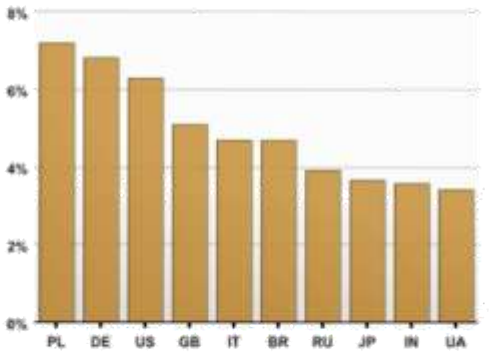
Live Forensics e Incident Response

Davide Gabrini

Forensic Jedi

Incidenza del cybercrime in Italia

Bot Activity, Top 10 Countries



This chart lists the top 10 countries seen contributing to botnet activity online in the last 24 hours, as a percentage relative to total malicious activity in the same period. IP geolocation isn't perfect, so this data isn't exact, but we believe it should be representative of the current global picture.

TEAM CYMRU

Live Forensics e Incident Response

Davide Gabrini

Forensic Jedi

Incidenza del cybercrime in Italia

- Statistiche aggiornate sul fenomeno nel rapporto Clusit – Security Summit 2012

ATTACCANTI PER TIPOLOGIA	2011	1Q 2012	Totale
Cybercrime	170	175	345
Unknown	148	122	270
Hacktivism	114	106	220
Espionage / Sabotage	23	3	26
Cyber warfare	14	17	31
TOTALE	469	423	892

VITTIME PER TIPOLOGIA	2011	1Q 2012	Tota
Institutions: Gov - Mil - LEAs - Intelligence	153	146	299
Others	97	95	192
Industry: Entertainment / News	76	56	132
Industry: Software / Hardware Vendor	27	18	45
Institutions: Research - Education	26	30	56
Industry: Gov. Contractors / Consulting	18	8	26
Industry: Banking / Finance	17	16	33
Industry: Security	17	7	24
Industry: Online Services / Cloud	15	28	43
Industry: Telco	11	6	17
Industry: Health	10	1	11
Religion	0	7	7
Industry: Chemical / Medical	2	5	7
TOTALE	469	423	892

TECNICHE DI ATTACCO PER TIPOLOGIA	2011	1Q 2012	Totale
SQL injection[22]	197	137	334
Known Vulnerabilities / Misconfigurations	107	69	176
Unknown	73	98	171
Malware	34	23	57
DDoS[23]	27	59	86
Account Cracking	10	13	23
Phishing / Social Engineering	10	11	21
Multiple Techniques	6	7	13
0-day[24]	5	3	8
Phone Hacking	0	3	3
TOTALE	469	423	892

Live Forensics e Incident Response

Davide Gabrini
Forensic Jedi

Sotto la punta dell'iceberg

Il grosso delle violazioni non viene denunciato. Possibili cause:

- La compromissione non viene rilevata
- Il problema viene "rattoppato" senza indagare ulteriormente
- L'indagine rimane interna all'azienda
  - Timore di danno d'immagine
  - Scarsa fiducia o interesse in un'azione legale

Live Forensics e Incident Response

Davide Gabrini

Forensic Jedi

E chi chiamerai?

Cosa fare, dal punto di vista legale, in caso di accertato accesso abusivo? E' possibile presentare una **querela**:

- **Chi**: la parte lesa. Nel caso di un'azienza, chi ne ha la rappresentanza legale.
  - La procedibilità d'ufficio è possibile solo in presenza di aggravanti
  - È comunque opportuno che il legale/amministivo sia accompagnato dal tecnico
  - Quando si tratta di reati con alto profilo tecnico, serve una querela con un profilo tecnico altrettanto alto
- **Quando**: entro 3 mesi dal giorno in cui si è appreso il fatto
- **Dove**: qualunque ufficio di Polizia Giudiziaria. Tuttavia la Polizia Postale è solitamente più avvezza alla materia
- **Cosa serve**: tutto! Ogni informazione, dato, rilievo utile a circostanziare i fatti. Meglio ancora se già filtrato, ma attenti alla conservazione degli originali! Per operare al meglio, sono utili nozioni di **computer forensics**

Live Forensics e Incident Response

Davide Gabrini
Forensic Jedi

Incidente informatico

- Un incidente informatico è qualcosa di più ampio, che non riguarda necessariamente il cybercrime, ma comprende imprevisti e malfunzionamenti anche accidentali, sia hardware che software
- Per quanto riguarda gli incidenti di sicurezza, la RFC 2350 distingue tra
  - Loss of confidentiality of information.
  - Compromise of integrity of information.
  - Denial of service.
  - Misuse of service, systems or information.
  - Damage to systems.

Live Forensics e Incident Response

Davide Gabrini
Forensic Jedi

Incident Response

Live Forensics e Incident Response

Davide Gabrini

Forensic Jedi

Computer Forensics e Incident Response

- Le procedure di CF ben si inseriscono nel processo di gestione degli incidenti
- Un processo di IR non è completo senza una fase di *indagine*
- Nonostante i possibili obiettivi comuni, CF e IR hanno spesso priorità e finalità diverse
- Ciò che va bene per l'IR, non è detto che vada altrettanto bene per la CF
  - sempre se si desidera arrivare in sede di giudizio

Live Forensics e Incident Response

Davide Gabrini
Forensic Jedi

NORMATIVA DI RIFERIMENTO

Live Forensics e Incident Response

Davide Gabrini
Forensic Jedi

Raccolta delle prove

Oltre che dalla Polizia Giudiziaria, le prove possono essere raccolte anche da altri soggetti:

- il Pubblico Ministero durante le indagini preliminari;
- la parte sottoposta a indagine, a fini difensivi;
- la parte offesa, per valutare l'opportunità di una denuncia o querela.

Live Forensics e Incident Response

Davide Gabrini
Forensic Jedi

Prove atipiche

Art.189 c.p.p. comma 1: Prove non disciplinate dalla legge

Quando è richiesta una prova non disciplinata dalla legge, il giudice può assumerla **se** essa risulta **idonea** ad assicurare l'accertamento dei fatti e **non pregiudica** la libertà morale della persona. Il giudice provvede all'ammissione, **sentite le parti** sulle modalità di assunzione della prova.

Live Forensics e Incident Response

Davide Gabrini
Forensic Jedi

Indagini difensive

- Principio di parità tra accusa e difesa
- L. 397/2000: Disposizioni in materia di indagini difensive
  - Art. da 391bis a 391decies cpp
- Il difensore, gli investigatori privati, i consulenti tecnici possono:
  - Ricevere dichiarazioni dalle persone in grado di riferire su circostanze utili
  - Richiedere documentazione alla Pubblica Amministrazione
  - Prendere visione dello stato di luoghi e cose ed effettuare rilievi
  - Accedere a luoghi privati o non aperti al pubblico, eventualmente su autorizzazione del giudice, al solo fine di ispezione.

Live Forensics e Incident Response

Davide Gabrini
Forensic Jedi

Art.391-nonies: Attività investigativa preventiva

- L'attività investigativa del difensore (Art.327-bis) può essere svolta anche preventivamente, su apposito mandato e per l'eventualità che si instauri un procedimento penale.
- Il difensore può incaricare dell'attività il sostituto, l'investigatore privato autorizzato o il consulente tecnico
- L'attività investigativa preventiva non può comprendere atti che richiedono l'autorizzazione dell'Autorità Giudiziaria

Si possono dunque svolgere autonomamente indagini private in attesa di valutare l'eventualità di procedere a un'azione penale e/o civile.

Live Forensics e Incident Response

Davide Gabrini
Forensic Jedi

Legge 48/2008

- Per la prima volta, vengono introdotte **procedure di acquisizione dell'evidenza informatica**, mediante l'imposizione dell'adozione di misure tecniche dirette ad assicurare la **conservazione** dei dati originali e ad **impedirne l'alterazione**;
- Adozione di procedure che assicurino la **conformità** dei dati acquisiti a quelli originali e la loro **immodificabilità**.
- Le novità riguardano, tra l'altro, gli articoli relativi a perquisizione, ispezione, sequestro, accertamenti urgenti, oltre al concetto stesso di corpo del reato.

Live Forensics e Incident Response

Digital Investigations 2012/2013

Pavia, 3.4.2013

Davide Gabrini

Forensic Jedi

INTERVENTI ON-SITE

Live Forensics e Incident Response

Davide Gabrini
Forensic Jedi

Questioni pratiche

- Dopo aver enunciato i principi della digital forensics, occorre confrontarsi col reale
  - Cosa ci si trova di fronte operando sul campo?
  - Quali scelte si hanno a disposizione nella trattazione dei reperti?
  - Tutti i metodi sono equivalenti o possono portare a risultati diversi?
  - Quali strumenti e metodi sono compatibili con la normativa?
  - Come comportarsi quando qualcosa non funziona?

Live Forensics e Incident Response

Davide Gabrini
Forensic Jedi

Operazioni preliminari

- Prendere il controllo dell'area:
  - Individuare le apparecchiature accese
    - attenzione agli screensaver
  - Tenere le persone lontane dagli apparati, dalle prese di corrente, dalle connessioni dati...
  - Non spegnere apparecchiature accese prima di esser certi di poterlo fare
  - **NON** accendere apparecchiature spente
    - se necessario, attendere l'intervento di personale specializzato
- Isolare la scena del crimine o dell'incidente sia **fisicamente** che **logicamente**

Live Forensics e Incident Response

Davide Gabrini
Forensic Jedi

Isolamento logico

- Rilevare se ci sono apparati collegati in rete e se c'è attività
  - Se c'è un modem non connesso, scollegarlo
  - Se c'è attività, scollegare i cavi solo dopo gli opportuni accertamenti, se ritenuti utili per l'indagine
  - Attenzione ai dispositivi wireless
- Staccare i cavi dal lato del PC, non delle prese (è più difficile sbagliarsi…)
- Rimuovere le batterie dei dispositivi mobili (sempre se opportuno)

Live Forensics e Incident Response

Davide Gabrini
Forensic Jedi

Analisi ambientale

- Rilevare elementi ambientali può fornire informazioni sugli usi e la disponibilità dei sistemi, soprattutto per individuare responsabilità personali
- Simili informazioni, se non annotate con precisione, andrebbero facilmente perse
- Spesso chi esegue il primo intervento e l'acquisizione è persona diversa da chi effettuerà l'analisi
- Il primo passo di un'indagine digitale è l'**identificazione**
  - se si fallisce in questa fase, difficilmente c'è rimedio
- Individuare cosa acquisire non è sempre facile
  - Sarebbe bello sapere anzitutto cosa si cerca…
  - I dati e i supporti potrebbero essere nascosti, fisicamente o logicamente, oppure essere altrove

Live Forensics e Incident Response

Davide Gabrini

Forensic Jedi

Analisi *Live* vs *Post-mortem*

- Quando si rinviene un sistema acceso, si è davanti ad una scelta:
  - Spegnerlo subito per procedere ad acquisizione e analisi post-mortem
  - Esaminarlo mentre è in esecuzione
- Entrambe le scelte hanno pro e contro, dipendenti anche da:
  - Competenza del personale impiegato
  - Strumentazione a disposizione
  - Perdita di dati e loro rilevanza
- Probabilmente occorrerà comunque valutare la modalità di spegnimento

Live Forensics e Incident Response

Davide Gabrini

Forensic Jedi

SPEGNIMENTO DEL SISTEMA

Live Forensics e Incident Response

Davide Gabrini
Forensic Jedi

Spegnimento

- Cosa si perde sicuramente allo spegnimento:
  - memorie volatili
  - stato di rete, sistema, applicazioni ecc.
    - chat in corso, cronologia di una shell…
    - eventi in corso che non prevedono log
  - **volumi cifrati** (BitLocker, FileVault, TrueCrypt, PGDisk, BestCrypt ecc. ecc.)
- Per acquisire queste informazioni serve però personale addestrato
- Diversamente, si rischia di far danni…

Live Forensics e Incident Response

Davide Gabrini
Forensic Jedi

Metodi di spegnimento

1) Procedura canonica (in genere deprecata)

- Start -> Spegni computer -> Spegni
- # shutdown –h now

- le normali procedure alterano numerose informazioni sul disco!
- ogni scrittura sovrascrive dati preesistenti (rilevanti?)
- è possibile siano state predisposte procedure di "pulizia", dal proprietario o dall'*intruso*

Live Forensics e Incident Response

Davide Gabrini
Forensic Jedi

Metodi di spegnimento

2) Interrompendo l'alimentazione

- Staccare il cavo dal lato del PC
  - Non fidarsi degli interruttori
- L'impatto è minore che con lo shutdown del sistema; il rischio di shock elettrico limitato
- Anche personale non esperto può procedere senza rischiare troppo danno
- Per contro, potrebbero perdersi dati non ancora registrati su disco
  - scritture in cache, transazioni DB…
  - e se il disco non ci fosse proprio?

Live Forensics e Incident Response

Davide Gabrini
Forensic Jedi

Power off → sequestro fisico

- Prima dello spegnimento, annotare l'ora di sistema e gli eventuali sfasamenti con l'ora reale
- Annotare i seriali ed etichettare tutti reperti
  - eventualmente anche cavi e connettori
- Eseguire, se possibile e utile, rilievi fotografici
- Ricercare eventuali annotazioni utili, come utenze, password, indirizzi e-mail, URL…
  - Chiedere è lecito, rispondere cortesia :-)
- Non dimenticare CD, floppy o schede di memoria inserite nel lettore!
- Durante la repertazione, contare i supporti, non le custodie
- Ricercare e acquisire anche gli alimentatori e gli altri accessori necessari
- Trattare i reperti opportunamente, implementare una robusta **catena di custodia** ecc. ecc.

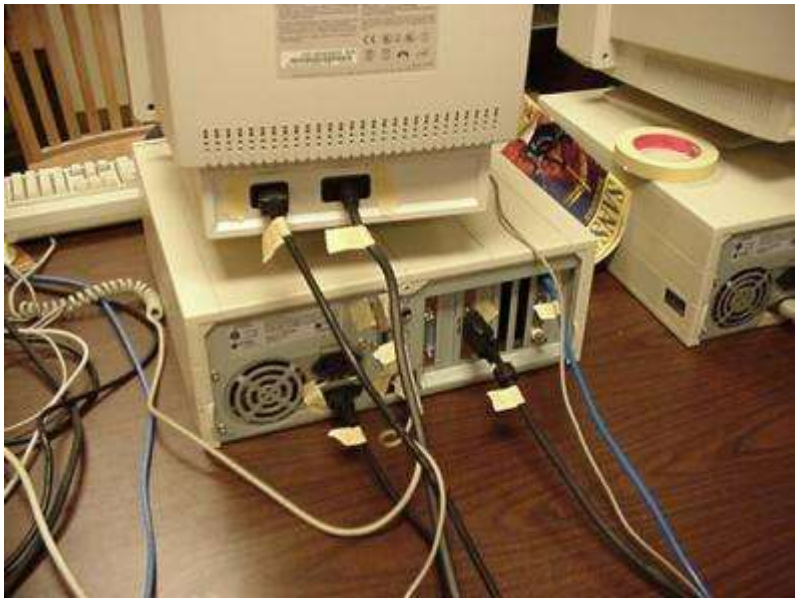
Live Forensics e Incident Response

Digital Investigations 2012/2013

Pavia, 3.4.2013

Davide Gabrini

Forensic Jedi



Live Forensics e Incident Response

Davide Gabrini

Forensic Jedi

ANALISI ON-SITE

(IN CSI FUNZIONA)

Live Forensics e Incident Response

Davide Gabrini
Forensic Jedi

Motivi per richiedere un'*analisi sul posto*

- Desiderio di avere risposte immediate
- Indirizzare meglio le stesse operazioni di ricerca o perquisizione
- Possibilità di eseguire *triage* su quanto disponibile
  - evitare "saccheggi" indiscriminati
  - individuare subito responsabilità personali in ambienti condivisi
  - evidenziare subito le informazioni più rilevanti rispetto a quelle secondarie
- Per la P.G., possibilità di procedere ad **arresto in flagranza** per i reati che lo prevedono

Live Forensics e Incident Response

Davide Gabrini

Forensic Jedi

Controindicazioni

- Sicuri che un'analisi sul posto sia la procedura migliore?
- Dalla RFC3227 in poi, le *best practices* internazionali consigliano prudenza…
- Quando si può scegliere tra acquisire e analizzare, **prima** si acquisisce, **poi** si analizza, non il contrario!
- Quando un sistema è spento, è solitamente consigliato **non** accenderlo
- Comunque di regola le analisi **NON** si fanno **MAI** sui reperti originali, ma **SOLO** sulle copie
  - Fare diversamente è rischioso
  - Correre rischi inutili è da irresponsabili

Live Forensics e Incident Response

Davide Gabrini
Forensic Jedi

Potenziale invasività

- Il sistema è spento, quindi in condizione statica (non facilmente alterabile)
- Accenderlo significa perturbarlo e perdere la sicurezza iniziale
- Senza opportune cautele, si rischia di inquinare irrimediabilmente il reperto
  - le modifiche apportate sono note?
  - sono documentabili?
  - intaccano significativamente il risultato dell'analisi?
  - ogni modifica distrugge qualcosa!
- Occorre quindi operare con cognizione di causa e grande cautela
- In ogni caso, **MAI** permettere l'avvio del sistema operativo residente!

Live Forensics e Incident Response

Davide Gabrini

Forensic Jedi

Controindicazioni "ambientali"

- Nel proprio ufficio si "gioca in casa", ma in perquisizione l'ambiente è spesso ostile...
- Le condizioni operative non sono paragonabili a quelle di un laboratorio
- L'attrezzatura a disposizione non può che essere limitata
- Situazioni imprevedibili sono sempre in agguato

Live Forensics e Incident Response

Davide Gabrini
Forensic Jedi

Fattore tempo

- Anche il tempo a disposizione è forzatamente limitato
- La fretta è il primo elemento da tenere fuori dalla scena del crimine
- Spesso non si procede ad acquisizione sul posto perché i tempi sono proibitivi
  - Figuriamoci un'analisi!
- L'asportazione fisica rimane il più delle volte la soluzione più rapida e sicura,
- ma non sempre!

Live Forensics e Incident Response

Davide Gabrini

Forensic Jedi

Responso incerto

Un'analisi eseguita in queste condizioni può dare riscontri **solo in positivo**:

- nella migliore delle ipotesi, si può da subito confermare l'esistenza di un'evidence individuata,
- ma non individuarla **non ne conferma l'assenza** con altrettanta certezza!

Live Forensics e Incident Response

Davide Gabrini

Forensic Jedi

Alternative all'analisi sul posto

- Ovviamente una: acquisizione!
- L'acquisizione va fatta rispettando l'**ordine di volatilità**
- Per i sistemi accesi:
  - Registri, cache
  - Memorie RAM
  - Stato della rete (connessioni stabilite, socket in ascolto, applicazioni coinvolte, cache ARP, routing table, DNS cache ecc…)
  - Processi attivi
  - File system temporanei
  - Dischi

Live Forensics e Incident Response

Davide Gabrini
Forensic Jedi

Ordine di volatilità (segue)

- Dopo lo spegnimento si prosegue con:
  - Dischi (post-mortem)
  - Log remoti
  - Configurazione fisica e topologia di rete
  - Floppy, nastri e altri dispositivi di backup
  - Supporti ottici, stampe ecc.

Live Forensics e Incident Response

Davide Gabrini

Forensic Jedi

Casi inevitabili

E' davvero necessario accendere sul posto un sistema spento quando:

- il sistema non è fisicamente rimovibile
  - o sono rimovibili solo i dischi ma ciò potrebbe non bastare
- non è possibile sequestrare tutti i sistemi, ma occorre individuare solo quelli rilevanti
- occorre soltanto acquisire dati, senza operare il sequestro dell'hardware
- l'urgenza di ottenere informazioni è tale da non consentire ritardi

Live Forensics e Incident Response

Davide Gabrini

Forensic Jedi

La accendiamo?

- Se ancora non vi ho convinto e volete la vostra *preview* sul posto, considerate almeno un'alternativa alla macchina sospetta…
- Una macchina sospetta non è *trusted* come quella del laboratorio, da cui il nome "sospetta" ;-)
- Meglio estrarre le memorie di massa ed esaminarle con una macchina fidata
  - sempre che ciò sia possibile…
    - Write blocker, adattatori, lentezza dei bus…
  - sempre con i limiti dettati dalla contingenza
  - lavorare direttamente sugli originali è comunque un grosso rischio

Live Forensics e Incident Response

Davide Gabrini

Forensic Jedi

Metodi di accensione

- Se proprio occorre accendere un PC spento, adottare qualche precauzione:
  - rimuovere i dischi
  - accendere il PC e accedere al BIOS
  - verificare l'ora di sistema
  - verificare/cambiare la sequenza di boot
  - inserire il proprio CD (o device) di avvio con sistema operativo *forensically sound*
  - spegnere il PC
  - ricollegare i dischi
  - accendere il PC, accedere nuovamente al BIOS e verificare la sequenza di boot
  - riavviare il PC

Live Forensics e Incident Response

Digital Investigations 2012/2013

Pavia, 3.4.2013

Davide Gabrini
Forensic Jedi

LIVE FORENSICS

Live Forensics e Incident Response

Davide Gabrini

Forensic Jedi

Quando è necessario un intervento *live*

- Se il sistema è in esecuzione, **qualsiasi** azione lo modificherà
  - tanto vale intraprendere azioni utili…
- Se il sistema non è fisicamente rimovibile
- Se il sistema non può essere spento
- Se il sistema non può essere acquisito nella sua interezza
- Se le informazioni volatili possono essere rilevanti ai fini dell'indagine
- In particolar modo, se occorre acquisire il traffico di rete riguardante la macchina

Live Forensics e Incident Response

Davide Gabrini

Forensic Jedi

Invasività

- Il sistema viene sicuramente alterato
  - le modifiche sono note?
  - sono documentabili?
  - intaccano significativamente il risultato dell'analisi?
  - ogni modifica distrugge qualcosa
- Gli accertamenti svolti su sistemi accesi non saranno ripetibili

Live Forensics e Incident Response

Davide Gabrini
Forensic Jedi

Live forensics best practices

- L'intervento dell'utente deve essere ridotto al minimo
- Ogni azione deve essere indispensabile e meno invasiva possibile
- Le modifiche ai dati memorizzati staticamente devono essere ridotte all'inevitabile
- Le aquisizioni hanno priorità secondo l'ordine di volatilità
- Ogni azione intrapresa deve essere scrupolosamente verbalizzata, con gli opportuni riferimenti temporali
- Gli strumenti utilizzati devono essere fidati, il più possibile indipendenti dal sistema e impiegare il minimo delle risorse; non devono produrre alterazioni né ai dati né ai metadati
- I dati estratti vanno sottoposti ad hash e duplicati prima di procedere all'analisi
- I dati che non sono volatili devono preferibilmente essere acquisiti secondo metodologia tradizionale

Live Forensics e Incident Response

Davide Gabrini
Forensic Jedi

Live forensics best practices

Più in generale:

- E' necessario comprendere le azioni che si stanno per compiere e le loro conseguenze
  - In caso contrario, è indispensabile ricorrere a personale specializzato
- E' consigliabile attenersi agli obiettivi dell'indagine, evitando divagazioni
- La *live forensics* non dovrebbe sostituirsi all'analisi *post-mortem*, ma esserne complementare

Live Forensics e Incident Response

Davide Gabrini
Forensic Jedi

Nemici delle live forensics

- Rootkit
  - user space (ring 3)
  - kernel space (ring 0)
  - VM based
- Non sempre è facile rilevarli
- Possono rilevare l'azione dei tool forensi
- Possono quindi alterarne i risultati, p.e. impedendo l'acquisizione di un'evidence
- Rendono **necessaria** l'analisi post-mortem

Live Forensics e Incident Response

Davide Gabrini

Forensic Jedi

STRUMENTI

Live Forensics e Incident Response

Davide Gabrini
Forensic Jedi

Distribuzioni forensi

- Analisi *live* e boot
  - **DEFT** (www.deftlinux.net)
  - CAINE (www.caine-live.net)
- Solo boot (linux-based)
  - Raptor
  - Paladin
- Solo boot (Windows-based)
  - **WinFE** (kit DIY di Microsoft)
  - SAFE BootDisk di ForensicSoft

Live Forensics e Incident Response

Davide Gabrini
Forensic Jedi

Cattura della RAM: tecniche

- Con privilegi amministrativi, la copia della RAM non é diversa da quella di altri device
  - tramite **/dev/mem** o **\\.\PhysicalMemory**
- Esistono però limitazioni, ben analizzate in "*Memory forensics: introduzione alle procedure di acquisizione delle memorie volatili*" – F.Schifilliti, IISFA Memberbook 2009
- Se il PC é bloccato?
  - Accesso diretto alla RAM (DMA) tramite porta Firewire IEEE1395
  - Cold boot attack
  - Duplicazione hardware?
    - Tribble, Co-Pilot

Live Forensics e Incident Response

Davide Gabrini

Forensic Jedi

Cattura della RAM

- **Win32dd** di Matthieu Suiche
- **FTK Imager** di AccessData
- **MDD** di ManTech
- **Nigilant32** di Agile Risk Management
- **Scaner** e **PZenDump**
- **Mandiant Memoryze**
- **winen** per i clienti Guidance Software
- **FastDump** di HBGary Inc.
- **PMDump** e **memimager** di Arne Vidstrom
- **Belkasoft Live RAM Capturer**
- **dd, dcfldd, dc3dd...**
- **fmem** per Linux
- **Mac Memory Reader** di CyberMarshal
- **pythonraw1394**
- Inoltre **msramdmp** e **memimage**, destinati ai solutori più che abili

Live Forensics e Incident Response

Davide Gabrini
Forensic Jedi

DART

- Dalla versione 7 di DEFT è stato introdotto il nuovo strumento **DART**
- Launcher per oltre 1GB di applicazioni portabili per live forensics, incident response e malware analysis
- Verifica l'integrità dei tool prima di lanciarli e registra un log delle operazioni
- E' in lavorazione **DART 2.0**, che esordirà a breve in DEFT 8, con nuovi strumenti e nuove funzioni
- In futuro sarà pienamente cross-platform e girerà quindi anche su Linux e Mac OSX

Live Forensics e Incident Response

Davide Gabrini
Forensic Jedi

Strumenti automatizzati

- **DEFT** mette a disposizione in DART tre strumenti:
  - **WFT**: Windows Forensic Toolchest
  - **linux-ir.sh**: script per sistemi Linux
  - **mac-ir.sh**: script per sistemi OSX
- Sono tutti *batch script* il cui scopo è raccogliere informazioni sul sistema su cui vengono avviati
- Possono salvare un report su un device locale (p.e. un pendrive) o una cartella di rete condivisa
- Consentono di velocizzare e standardizzare rilievi che, fatti da un operatore umano, richiederebbero tempo e competenze specifiche

Live Forensics e Incident Response

Davide Gabrini

Forensic Jedi

Strumenti automatizzati

- Altri strumenti simili sono:
  - **COFEE** di Microsoft: Computer Online Forensi Evidence Extractor (solo law enforcement)
  - **MIR-ROR**: Motile Incident Response – Respond Objectively, Remediate (basato su Sysinternals), divenuto ora **Confessor**
  - **RAPIER**: Rapid Assessment & Potential Incident Examination Report (Intel)
  - **Live Response** (e-fense)
  - **Drive Prophet** (Mark McKinnon, RedWolf)
  - **ADF Triage Kit** di ADF Solutions

Opportunamente configurati ed impiegati, possono coprire le esigenze di e-discovery, incident response, triage e forensics

Live Forensics e Incident Response

Davide Gabrini
Forensic Jedi

WFT: Windows Forensic Toolchest

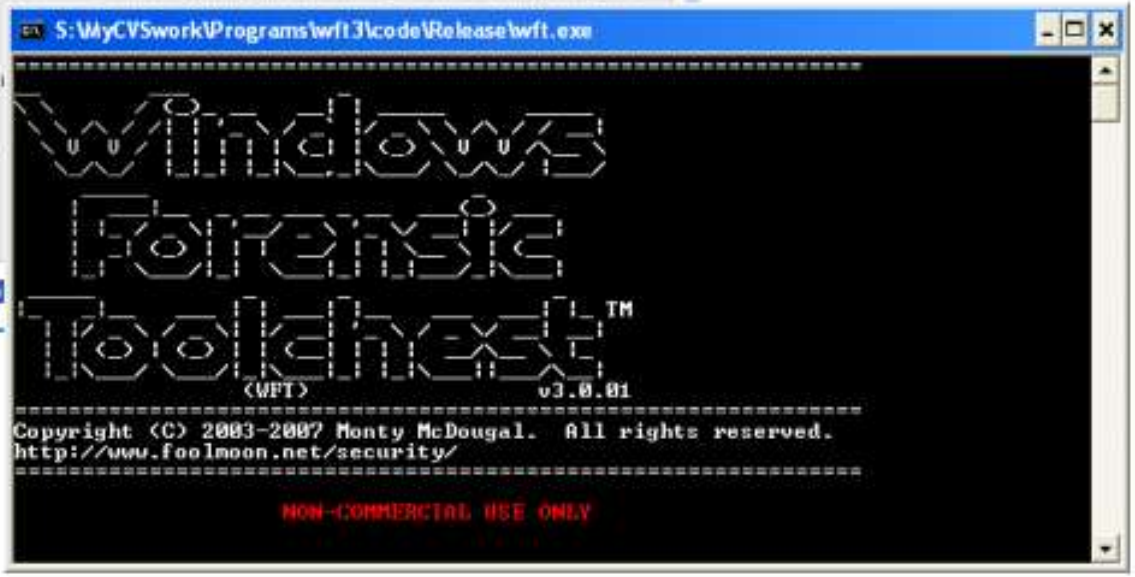
- Tool automatico per *live forensics* e *incident response*
- Avvia una serie di tool fidati e verificati al momento per catturare informazioni su sistemi Windows in esecuzione
- Minimizza l'invasività
- Logga ogni operazione e calcola l'hash di ogni risultato prodotto
- Genera un report completo sia in testo semplice che in HTML navigabile

Live Forensics e Incident Response

Davide Gabrini

Forensic Jedi

WFT: Windows Forensic Toolchest



Live Forensics e Incident Response

Davide Gabrini
Forensic Jedi

Teniamoci in contatto...

Davide Rebus Gabrini

e-mail:
rebus@mensa.it
rebus@tipiloschi.net

GPG Public Key: (available on keyserver.linux.it)
www.tipiloschi.net/rebus.asc
KeyID: 0x176560F7

Instant Messaging:

MSN	therebus@hotmail.com
ICQ	115159498
Yahoo!	therebus
Skype	therebus
Gtalk	therebus

Mi trovate su **LinkedIn**, Facebook, Twitter, FriendFeed...

Queste e altre cazzate su **http://www.tipiloschi.net**