



Computer  
forensics

Mattia Monga

CERT-IT

Computer  
Forensics

DE  
CSI

Conclusioni

# Computer forensics in azienda: l'esperienza del CERT-IT<sup>1</sup>

Mattia Monga

CERT-IT Dip. di Informatica e Comunicazione  
Università degli Studi di Milano, Italia  
`mattia.monga@unimi.it`

Roma – 6 giugno 2007



## Il CERT-IT è il **Computer Emergency Response Team italiano** (CERT-IT)

- senza scopo di lucro, presso il Dip. di Informatica e Comunicazione dell'Università di Milano
- fondato nel 1994, iscritto al Forum of Incident Response and Security Teams (FIRST) dal 1995
- Punto di contatto fidato per coordinare la risposta agli attacchi informatici

# Il ruolo odierno del CERT-IT (1)



Computer  
forensics

Mattia Monga

CERT-IT

Computer  
Forensics

DE  
CSI

Conclusioni

- Dic 1995  $\rightsquigarrow$  16 MUtenti, Mag 2007  $\rightsquigarrow$  1'129 MUtenti (Europa: 315 Mutenti) [Internet World Stats]
- '90  $\rightsquigarrow$  pochi incidenti, molto interessanti
- oggi  $\rightsquigarrow$  moltissimi incidenti, pochissimi interessanti
  - Esistono attori istituzionali (p.es. Polizia Postale)
  - Lo smaltimento di tutti gli incidenti è insostenibile da un gruppo di volontari (ed esistono CERT in capo ai gestori delle reti)
  - La maggior parte degli attacchi è portato a termine (e rilevato) automaticamente (*malware*)

# Il ruolo odierno del CERT-IT (2)



Computer  
forensics

Mattia Monga

CERT-IT

Computer  
Forensics

DE  
CSI

Conclusioni

Perché restiamo in vita?

- Centro di competenza fidato e **indipendente**
- *Reality check* per l'attività di ricerca del Dipartimento
- Attività divulgative (Capture The Flag 2005)
- Sostentamento: consulenze, corsi



Con **Computer Forensics**<sup>2</sup> si intendono due cose leggermente diverse che è opportuno distinguere:

- ① **Digital Evidence Analysis (DEA)** L'analisi delle informazioni digitali in maniera tale che possano essere usate come prova in giudizio;
- ② **Crime Scene Investigation (CSI)** L'indagine sugli strumenti di calcolo coinvolti in un reato informatico.

---

<sup>2</sup>*forensics* sostantivo, *forensic* aggettivo



Due obiettivi e approcci diversi al problema della raccolta delle informazioni (eventualmente in conflitto)

**DEA** L'enfasi è sul garantire che l'informazione sia *autentica, integra, vera, completa e raccolta legalmente*, in modo da poterla utilizzare in giudizio.

**CSI** L'enfasi è sul reperimento di indizi che aiutino la comprensione della dinamica del delitto e l'identificazione dei responsabili.



Le tipiche domande del Giudice ai periti:

- La prova è stata raccolta senza alterarla (integrità)?
- Ho tutto ciò che mi serve per interpretare la prova in maniera corretta (completezza, veridicità)?
- Che valore posso dare alle catene causali di responsabilità che emergono dalla prova (autenticità, veridicità)?



- **Integrità:** memorie di massa acquisite da sistemi di calcolo in funzione. Anche supponendo la buona fede dell'operatore, si può *garantire* l'integrità dell'informazione digitale?



- **Integrità:** memorie di massa acquisite da sistemi di calcolo in funzione. Anche supponendo la buona fede dell'operatore, si può *garantire* l'integrità dell'informazione digitale?
- **Completezza:** uso di programmi complessi (p.es. EnCase) senza comprendere i dettagli tecnologici. È possibile essere ragionevolmente sicuri di aver raccolto tutta l'informazione?



- **Integrità:** memorie di massa acquisite da sistemi di calcolo in funzione. Anche supponendo la buona fede dell'operatore, si può *garantire* l'integrità dell'informazione digitale?
- **Completezza:** uso di programmi complessi (p.es. EnCase) senza comprendere i dettagli tecnologici. È possibile essere ragionevolmente sicuri di aver raccolto tutta l'informazione?
- **Autenticità:** i meccanismi di registrazione degli eventi (*log*) sono generalmente progettati per l'amministrazione, non la computer forensics. È possibile fidarsi di ciò che viene registrato?



## Example

Un'applicazione registra gli accessi

```
172.23.11.19  Mike  2002-09-03  13:02:43  file.txt
```

Accesso ad un file dal nome particolare...

```
file.txt\n127.0.0.1\tAlice\t2002-09-03\t13:03:44\tsecret.txt
```

```
172.23.11.19  Mike  2002-09-03  13:02:43  file.txt
```

```
127.0.0.1      Alice 2002-09-03  13:03:44  secret.txt
```



Qualora si vogliono raccogliere prove da presentare a sostegno di una denuncia occorre procedere in maniera sistematica, documentando

- Identificazione dell'informazione
- Acquisizione
- Analisi ed eventuali elaborazioni



Un messaggio di posta elettronica di un dipendente diffama l'amministratore delegato di un'azienda

- Messaggio spedito da un sistema di webmail, identità di fantasia. Esistono accessi riconducibili a macchine aziendali?



Un messaggio di posta elettronica di un dipendente diffama l'amministratore delegato di un'azienda

- Messaggio spedito da un sistema di webmail, identità di fantasia. Esistono accessi riconducibili a macchine aziendali?
- **Integrità:** L'operazione di acquisizione dei log è stata interamente filmata in modo da permetterne la critica da parte del *convenuto*.



Un messaggio di posta elettronica di un dipendente diffama l'amministratore delegato di un'azienda

- Messaggio spedito da un sistema di webmail, identità di fantasia. Esistono accessi riconducibili a macchine aziendali?
- **Integrità:** L'operazione di acquisizione dei log è stata interamente filmata in modo da permetterne la critica da parte del *convenuto*.
- **Legalità:** L'acquisizione dei dati è stato operato dagli amministratori del sistema, secondo le procedure aziendali già in essere (rispetto della privacy dei lavoratori)



In azienda spesso l'interesse è proprio per l'attività investigativa, che per ragioni di opportunità o riservatezza non si vogliono affidare ad enti istituzionali. (Fermo restando l'obbligo di informare le autorità competenti qualora il reato lo preveda)



Un obiettivo primario è in genere quello di **ridurre al minimo i fermi macchina**

- Acquisizione di memorie di massa in RAID su un server evitando la sospensione del servizio grazie a tecniche di hotswap



Un obiettivo primario è in genere quello di **ridurre al minimo i fermi macchina**

- Acquisizione di memorie di massa in RAID su un server evitando la sospensione del servizio grazie a tecniche di hotswap
- ma... non è stato possibile ricostruire i dati senza il server originale



Un obiettivo primario è in genere quello di **ridurre al minimo i fermi macchina**

- Acquisizione di memorie di massa in RAID su un server evitando la sospensione del servizio grazie a tecniche di hotswap
- ma... non è stato possibile ricostruire i dati senza il server originale
- la ricostruzione mediante macchina “gemella” appositamente allestita è fallita a causa della nuova versione del firmware del controller!



Hosting di *phishing* su di una macchina aziendale; ci sono buone ragioni per ricercare le responsabilità dirette al di fuori dell'azienda.

- Come fare a identificare eventuali persistenze della compromissione?



Hosting di *phishing* su di una macchina aziendale; ci sono buone ragioni per ricercare le responsabilità dirette al di fuori dell'azienda.

- Come fare a identificare eventuali persistenze della compromissione?
  - Spesso i backup sono misti per dati e sistemi.
  - Servono tool che permettano di operare in maniera sistematica e scalabile



Hosting di *phishing* su di una macchina aziendale; ci sono buone ragioni per ricercare le responsabilità dirette al di fuori dell'azienda.

- Come fare a identificare eventuali persistenze della compromissione?
  - Spesso i backup sono misti per dati e sistemi.
  - Servono tool che permettano di operare in maniera sistematica e scalabile
- Come fare a identificare quale falla nel processo organizzativo ha permesso la compromissione? Come aggiornare le policy aziendali?



Computer  
forensics

Mattia Monga

CERT-IT

Computer  
Forensics

DE  
CSI

Conclusioni

# Grazie!

<http://cert-it.dico.unimi.it>



- Communications of the ACM, February 2006/Vol. 49, No. 2, Special issue on Computer Forensics
- Forensic Discovery, by Dan Farmer, Wietse Venema, Addison Wesley Professional 2004 (disponibile anche sul web <http://www.porcupine.org/forensics/forensic-discovery/>)
- File System Forensic Analysis by Brian Carrier, Addison Wesley Professional 2005