ISACA®
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

# *Computer Forensics applicata ai contesti di contro spionaggio industriale*

## *Accorgimenti ed implementazioni per la difesa aziendale*

Dott. Stefano Fratepietro

Roma 25/03/2014

# Presentazione relatore

## Dott. Stefano Fratepietro

**Chief Information Security Officer - Tesla Consulting srls**

OSCP - Offensive Security Certified Professional

OPST - OSSTMM Professional Security Tester Accredited Certification

**Consulente di Informatica Forense**

White hat Hacker

https://www.soldierx.com/hdb/Stefano-Fratepietro

**Presidente e Project Leader - Associazione DEFT**

www.deftlinux.net

# Agenda

- Presentazione relatore
- Panoramica e stato dell'arte dello spionaggio industriale
  - In Italia
  - Nel mondo
- Costi ed opportunità
- Soluzioni pre incidente
  - Policy degli asset aziendali
  - Soluzioni commerciali e non a supporto dell'azienda
- Soluzioni post incidente
  - Computer Forensics
  - Incident Response
- Bibliografia & sitografia
- Q&A

# Panoramica e stato dell’arte

# Panoramica e stato dell'arte

Sei in: Il Fatto Quotidiano > Tecno > Verizon, "...

## Verizon, "attacchi hacker e virus: cresce lo spionaggio industriale"

Nel rapporto pubblicato dal provider americano, furti di informazioni e violazioni dei sistemi informatici sono in netta crescita, con più di 47mila episodi registrati. E in molti casi le vittime se ne accorgono solo a di distanza di mesi

**di Marco Schiaffino | 24 aprile 2013** **Commenti (8)**

# Panoramica e stato dell'arte - Italia

## Hacker per spionaggio industriale: nei guai tre ex dipendenti di un'azienda di Parma

Inviato da Francesco Polimeni il Lun, 13/02/2012 - 18:12

Pubblicato in spionaggio industriale Iospio.org newsletter Hacker hacker

Avviso di fine indagine per tre ex dipendenti di una società parmense di progettazione e installazione di software per le imprese, accusati di aver fatto spionaggio industriale per carpire informazioni informatiche dalla azienda ed offrire così alla clientela, attraverso una nuova società, prodotti analoghi a prezzi più vantaggiosi.


20

Condividi

L'inchiesta era nata nel 2010 dopo che la ditta, la Cdm Tecnoconsulting, aveva rilevato una strana "migrazione" di clienti. Successivamente, controlli sulla rete informatica avevano messo in luce accessi abusivi, da cui la denuncia. L'indagine, affidata alla polizia postale, è stata coordinata dal pm della procura di Bologna Antonella Scandellari.

# Panoramica e stato dell'arte - Mondo

## NY Times says Chinese hacked paper's computers

Jan 31, 2013

Chinese hackers repeatedly penetrated The New York Times' computer systems over the past four months, stealing reporters' passwords and hunting for files on an investigation into the wealth amassed by the family of a top Chinese leader, the newspaper reported Thursday.

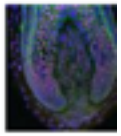
Security experts hired to investigate and plug the breach found that the attacks used tactics similar to ones used in previous hacking incidents traced to China, the report said. It said the hackers routed the attacks through computers at U.S. universities, installed a strain of malicious software, or malware, associated with Chinese hackers and initiated the attacks from Chinese university computers previously used by the Chinese military to attack U.S. military contractors.

The attacks, which began in mid-September, coincided with a Times investigation into how the relatives and family of Premier Wen Jiabao built a fortune worth over $2 billion. The report, which was posted online Oct. 25, embarrassed the Communist Party leadership, coming ahead of a fraught transition to new leaders and exposing deep-seated favoritism at a time when many Chinese are upset about a wealth gap.

Over the months of cyber-incursions, the hackers eventually lifted the computer passwords of all Times employees and used them to get into the personal computers of 53 employees.

The report said none of the Times' customer data was compromised and that information about the investigation into the Wen family remained protected, though it left unclear what data or communications the infiltrators accessed.

Featured


# Panoramica e stato dell'arte - Mondo

My favorite bit of the *New York Times* story is when they ding Symantec for not catching the attacks:

> Over the course of three months, attackers installed 45 pieces of custom malware. The Times -- which uses antivirus products made by Symantec -- found only one instance in which Symantec identified an attacker's software as malicious and quarantined it, according to Mandiant.

Symantec, of course, had to respond:

> Turning on only the signature-based anti-virus components of endpoint solutions alone are not enough in a world that is changing daily from attacks and threats. We encourage customers to be very aggressive in deploying solutions that offer a combined approach to security. Anti-virus software alone is not enough.

# Panoramica e stato dell'arte - Gli attori

Attivisti

Militari-Governi

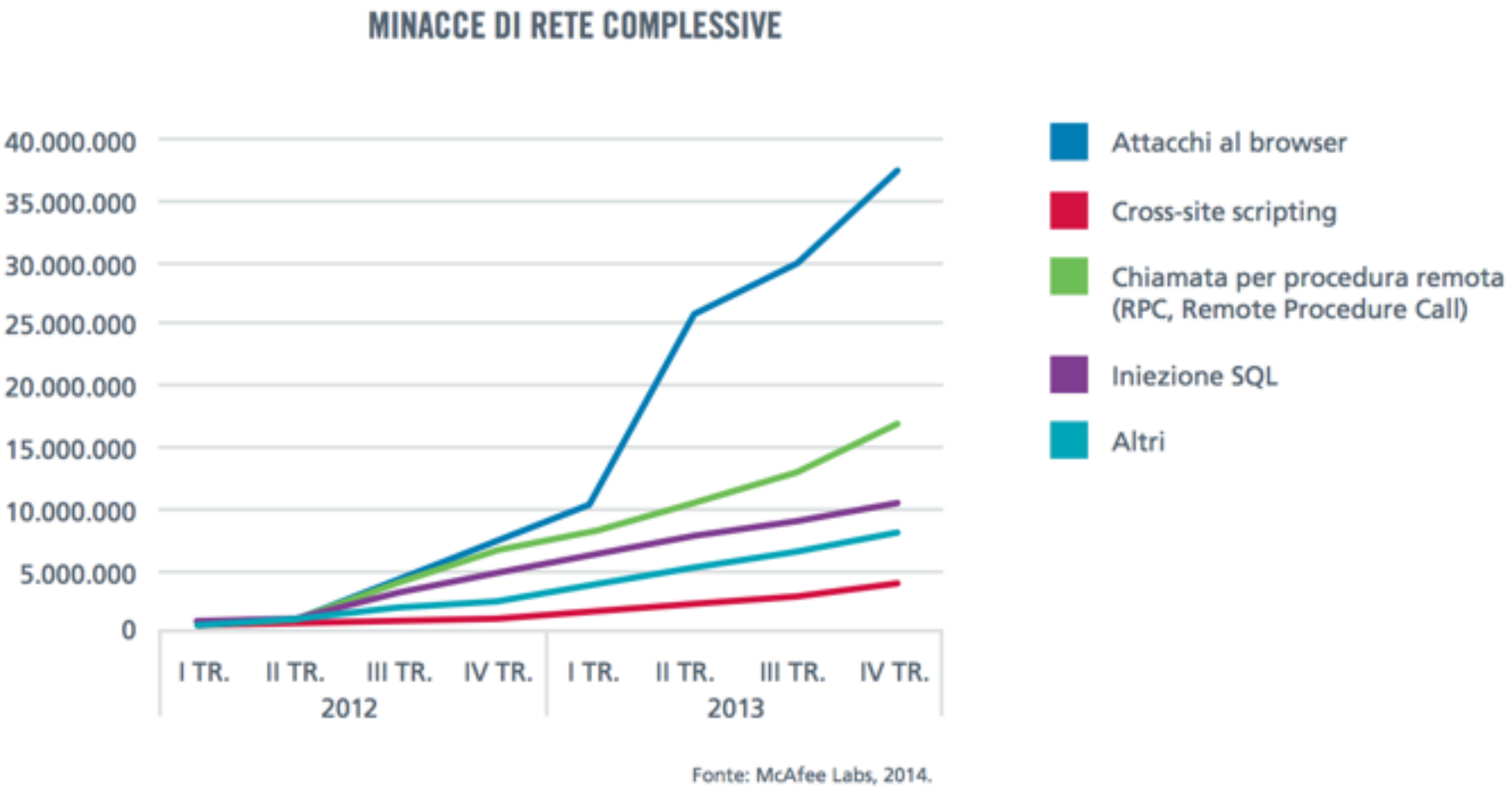
Crimine organizzato

Wannabe Hacker

# Panoramica e stato dell'arte - Chi interessato a cosa

| | ORGANIZED CRIME | STATE-AFFILIATED | ACTIVISTS |
|---|---|---|---|
| VICTIM INDUSTRY | Finance<br>Retail<br>Food | Manufacturing<br>Professional<br>Transportation | Information<br>Public<br>Other Services |
| REGION OF OPERATION | Eastern Europe<br>North America | East Asia (China) | Western Europe<br>North America |
| COMMON ACTIONS | Tampering (Physical)<br>Brute force (Hacking)<br>Spyware (Malware)<br>Capture stored data (Malware)<br>Adminware (Malware)<br>RAM Scraper (Malware) | Backdoor (Malware)<br>Phishing (Social)<br>Command/Control (C2) (Malware, Hacking)<br>Export data (Malware)<br>Password dumper (Malware)<br>Downloader (Malware)<br>Stolen creds (Hacking) | SQLi (Hacking)<br>Stolen creds (Hacking)<br>Brute force (Hacking)<br>RFI (Hacking)<br>Backdoor (Malware) |
| TARGETED ASSETS | ATM<br>POS controller<br>POS terminal<br>Database<br>Desktop | Laptop/desktop<br>File server<br>Mail server<br>Directory server | Web application<br>Database<br>Mail server |
| DESIRED DATA | Payment cards<br>Credentials<br>Bank account info | Credentials<br>Internal organization data<br>Trade secrets<br>System info | Personal info<br>Credentials<br>Internal organization data |

# Panoramica e stato dell'arte



# Panoramica e stato dell'arte - Casistiche

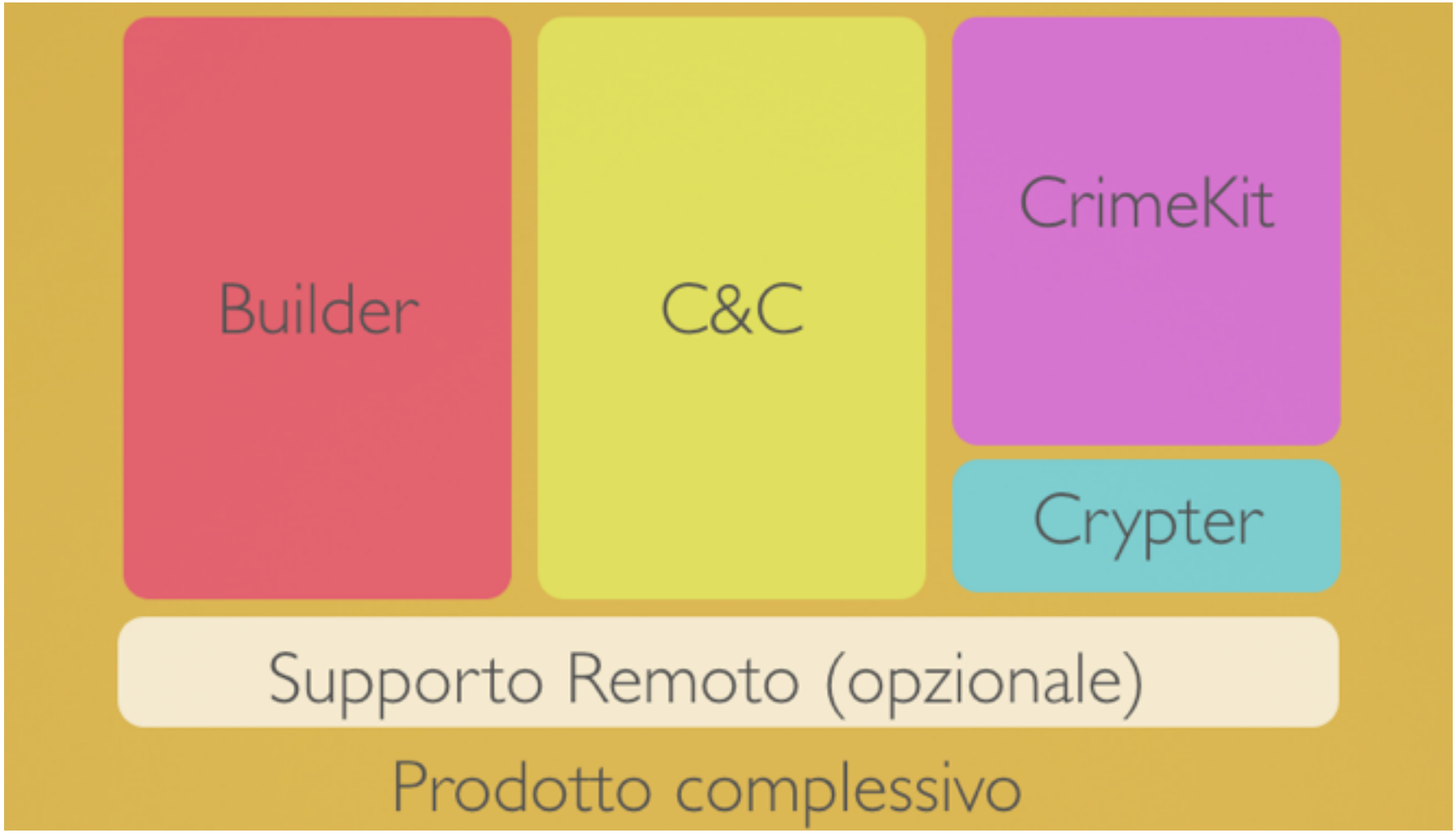
- PMI
  - nella maggior parte dei casi non si accorge di nulla
  - nessun budget di spesa per la tutela del patrimonio aziendale
  - nessuna cultura in materia
- Media impresa
  - mediamente si accorge del problema DOPO il furto delle informazioni
  - investimenti fuori budget solo quando "il fattaccio" è già accaduto
- Grande impresa
  - realtà più sensibile all'argomento, soprattutto se vi sono brevetti di mezzo
  - potrebbe accorgersene anche ad azioni in corso
  - budget annuale investito a tutela del patrimonio aziendale

# Agenda

- Presentazione relatore
- Panoramica e stato dell'arte dello spionaggio industriale
  - In Italia
  - Nel mondo
- Costi ed opportunità
- Soluzioni pre incidente
  - Policy degli asset aziendali
  - Soluzioni commerciali e non a supporto dell'azienda
- Soluzioni post incidente
  - Computer Forensics
  - Incident Response
- Bibliografia & sitografia
- Q&A

# Costi ed opportunità

# Costi ed opportunità - attacco remoto



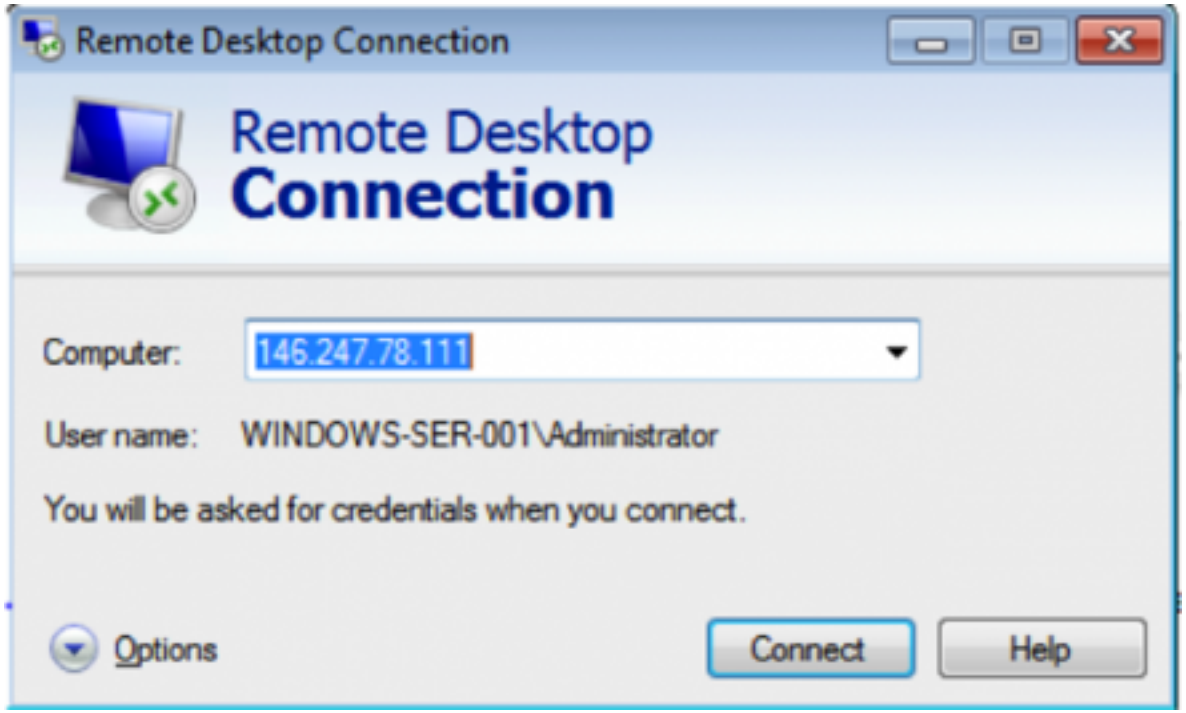
# Costi ed opportunità - attacco remoto

| | |
|---|---|
| ADOBE READER | $5,000–$30,000 |
| MAC OSX | $20,000–$50,000 |
| ANDROID | $30,000–$60,000 |
| FLASH OR JAVA BROWSER PLUG-INS | $40,000–$100,000 |
| MICROSOFT WORD | $50,000–$100,000 |
| WINDOWS | $60,000–$120,000 |
| FIREFOX OR SAFARI | $60,000–$150,000 |
| CHROME OR INTERNET EXPLORER | $80,000–$200,000 |
| IOS | $100,000–$250,000 |

# Costi ed opportunità - attacco interno, dipendente infedele

- Probabilmente la più costosa delle soluzioni
- Richiede nella maggior parte dei casi, l'obbligo da parte dell'azienda di assumere la risorsa infedele
- Nessuna specializzazioni in hacking richiesta

# Costi ed opportunità - attacco stupido ma efficace




Sistemi direttamente esposti su Internet, abbandonati e con credenziali uguali da dieci anni

# Agenda

- Presentazione relatore
- Panoramica e stato dell'arte dello spionaggio industriale
  - In Italia
  - Nel mondo
- Costi ed opportunità
- Soluzioni pre incidente
  - Policy degli asset aziendali
  - Soluzioni commerciali e non a supporto dell'azienda
- Soluzioni post incidente
  - Computer Forensics
  - Incident Response
- Bibliografia & sitografia
- Q&A

# Soluzioni pre incidente

Tutte le aziende, PMI o grandi, DEVONO difendersi

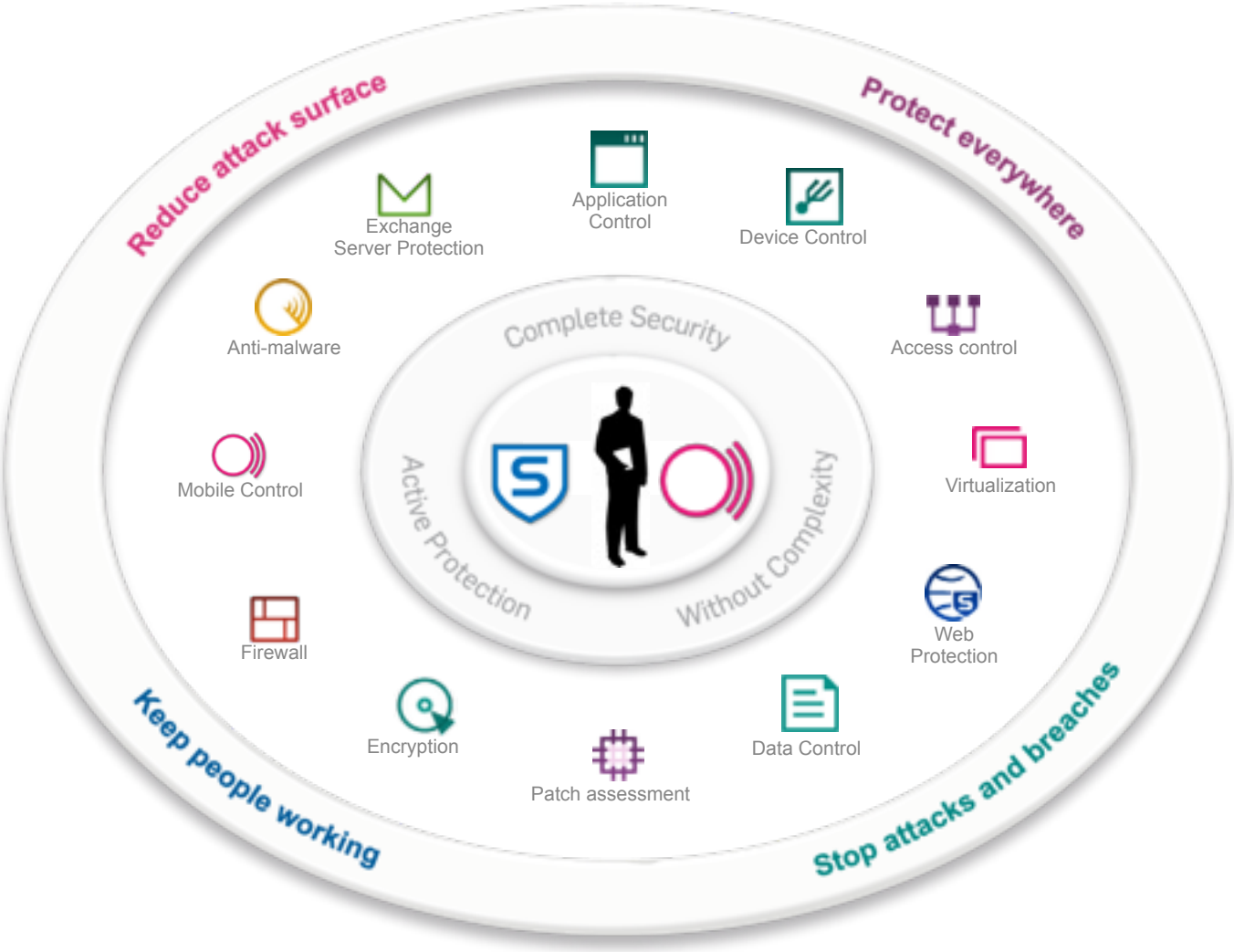
La sicurezza non è un prodotto ma un processo

Inutile spendere milioni di euro di budget nell'IT Security se la vulnerabilità si chiama "UTONTO"

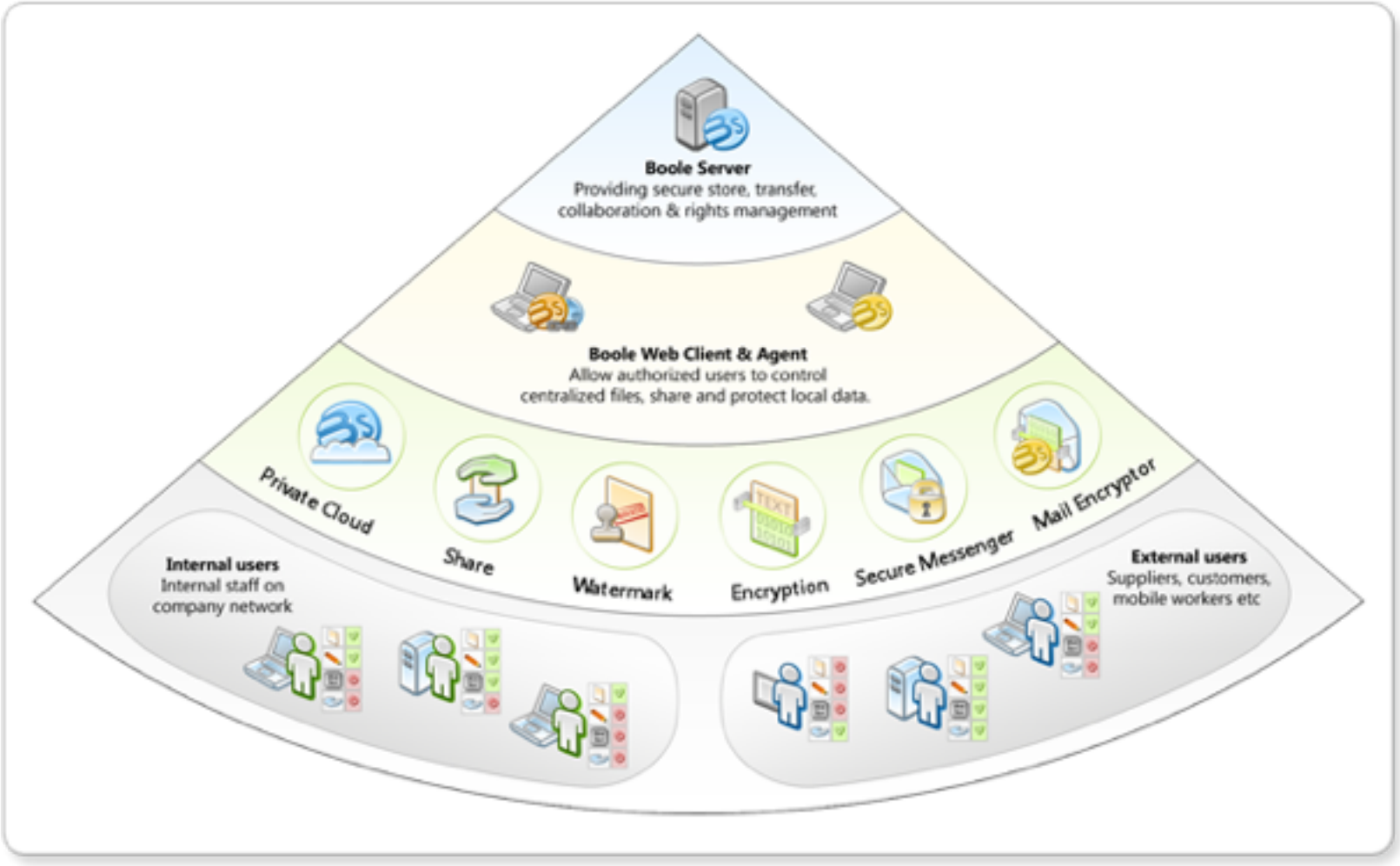
# Soluzioni pre incidente

- Blocco degli storage esterni con censimento delle memorie di massa aziendali
- Controllo dei vettori di uscita dei dati in tempo reale
- Full disk encryption dei device in mobilità
- Policy puntuali di accesso al dato con audit log verboso

# Soluzioni pre incidente - end point protection



# Soluzioni pre incidente - DLP



# Soluzioni pre incidente - firewall e sonde


# Soluzioni pre incidente - cifratura con indipendence key

- Non è una penna usb! È un microkernel base Linux per la cifratura dei dati
- Crittografia 100% hardware
- Generazioni di chiavi crittografiche univoche, irripetibili e non esportabili dal dispositivo
- Associazione crittografica tra più dispositivi creando il così detto “silent circle”
- Condivisione cifrata del dato indipendentemente dal canale usato (penne usb, dropbox, file server, amazon, etc)

# Agenda

- Presentazione relatore
- Panoramica e stato dell'arte dello spionaggio industriale
  - In Italia
  - Nel mondo
- Costi ed opportunità
- Soluzioni pre incidente
  - Policy degli asset aziendali
  - Soluzioni commerciali e non a supporto dell'azienda
- Soluzioni post incidente
  - Computer Forensics
  - Incident Response
- Bibliografia & sitografia
- Q&A

# Soluzioni post incidente - Digital Forensics

In questo contesto, diventa sempre più necessario ricercare all'interno dei sistemi informativi dell'azienda (corporate forensics) e del cittadino (digital forensics) la prova digitale utilizzabile nella successiva fase giudiziale (penale, civile e amministrativa)

La prova digitale è qualunque informazione generata, memorizzata o trasmessa attraverso uno strumento elettronico che possa essere ammessa in giudizio (Fonte: Digital Forensics Guide - Council of Europe - 2013).

**Autentica:** non deve subire alcuna alterazione

**Ammissibile**: essere utilizzabile in giudizio come fonte di prova

**Proporzionale:** ossia rispettare I diritti fondamentali

**"Credibile":**Facilmente comprensibile dall'autorità giudiziaria

# Soluzioni post incidente - Digital Forensics

Cosa NON fare:

- Mancata copia forense (bitstream) dei supporti
- Accensione e utilizzo del PC originale
- Mancata conservazione dei supporti originali
- Mancata apposizione di data certa
- Monitoraggio del dipendente in tempo reale
- Violazione Privacy
- Errata repertazione (hash, sigilli, catena di conservazione)
- Uso di strumenti di duplicazione inadeguati (es. Norton Ghost)
- Utilizzo di strumenti di analisi o metodologie non adeguate
- Per l'avvocato: non chiamare il CT all'ultimo momento

# Soluzioni post incidente - Digital Forensics

Cosa fare:

- Acquisire la prova informatica tenendo presente le 6 fasi della Computer Forensics
  - Individuazione
  - Preservazione
  - Acquisizione
  - Analisi
  - Documentazione
  - Catena di custodia
- Non limitarsi all'analisi dei dati provenienti dalle sole fonti aziendali ma analizzare ANCHE le fonti aperte (OSINT)

# Soluzioni post incidente - Digital Forensics

Fase 1, Individuazione

- Identificazione dei componenti informatici di interesse aventi memorie di massa utilizzabili da un utente






# Soluzioni post incidente - Digital Forensics

Fase 2, Preservazione

- Mettere in sicurezza i dispositivi mediante appositi sigilli
- Calcolo dell'hash delle memorie oggetto di sequestro
- Verbale delle operazioni

Fase 2, Preservazione

- Funzione che data una sequenza definita di bit restituisce un valore univoco.
- La funzione restituisce una stringa di numeri e lettere a partire da un qualsiasi flusso di bit di qualsiasi dimensione; il risultato viene chiamato digest.
- L'algoritmo non è invertibile, cioè dal digest non si può ricavare la sequenza di bit

# Soluzioni post incidente - Digital Forensics

Fase 2, Preservazione

- Md5 Message Digest Algorithm 5 - rfc1321, dato un input, restituisce una stringa di 128 bit composta da 32 caratteri esadecimali

- Sha1 Secure Hash Algorithm 1 - rfc3174, dato un input, restituisce una stringa di 160 bit composta da 40 caratteri esadecimali

- Sha256 e Sha512 - rfc4634, dato un input restituisce una stringa di 256 bit per lo sha256 e 512 bit per lo sha512, compoata rispettivamente da 61 e 122 caratteri esadecimali

# Soluzioni post incidente - Digital Forensics

In che contesto si sta lavorando?

- Accertamento tecnico privato
- Accertamento tecnico per causa civile o penale
- L'accertamento è di tipo irripetibile o ripetibile?
- 359 c.p.p. e 360 c.p.p.

Fase 3, Acquisizione

Accertamento tecnico ripetibile

- Clonazione della memoria di massa mediante una bit stream image
  - Raw
  - Ewf
  - Aff

La memoria da clonare deve essere collegata al sistema mediante opportuni dispositivi di blocco di scrittura (hardware o software)
L'acquisizione della memoria deve essere completa
La copia fedele deve avere lo stesso valore di hash dell'originale

Fase 3, Acquisizione

Accertamento tecnico irripetibile

- Procedura che potrebbe alterare, anche in minima parte, l'originalità della memoria di massa
- Memorie ove non è conosciuta la pratica per la clonazione
- Cellulari o Smartphone che necessitano procedure invasive preventive
- Dispositivi atipici

L'acquisizione della memoria può avvenire in modo completo (clonazione) o parziale (acquisendo i singoli dati di interesse).
La copia potrebbe non necessitare la comparazione di hash con la memoria originale

# Soluzioni post incidente - Digital Forensics

Fase 3, Acquisizione

Variabili e calcolo del rischio

Tener conto dello stato di usura dell'oggetto di perizia; nel caso in cui esso sia molto vecchio, è meglio eseguire un accertamento tecnico irripetibile

Lo stress che subirà la memoria durante la fase di acquisizione potrebbe alterare definitivamente il corretto funzionamento della memoria

# Soluzioni post incidente - Digital Forensics

Fase 3, Acquisizione

Eccezioni per l'acquisizione di cellulari

- Accendere il dispositivo solo all'interno di una gabbia di faraday
- Lasciare la sim dentro il dispositivo
- Eseguire una simulazione dell'attività su un dispositivo identico per prevenire spiacevoli imprevisti


# Soluzioni post incidente - Digital Forensics

Fase 3, Acquisizione

Vietato improvvisare!

# Soluzioni post incidente - Digital Forensics

Fase 3, Acquisizione

Variabili e calcolo del rischio

Tener conto dello stato di usura dell'oggetto di perizia; nel caso in cui esso sia molto vecchio, è meglio eseguire un accertamento tecnico irripetibile

Lo stress che subirà la memoria durante la fase di acquisizione potrebbe alterare definitivamente il corretto funzionamento della memoria

# Soluzioni post incidente - Digital Forensics

Fase 3, Acquisizione

Cosa dice la ISO 27037?

- Scollegare la memoria di massa quando possibile
- Collegarla ad un sistema adibito all'acquisizione delle memorie
- Utilizzare software che possano eseguire una acquisizione completa della memoria con relativa verifica

# Soluzioni post incidente - Digital Forensics

Fase 4, Analisi

- Raccolta dei file di interesse e classificazione dei dati individuati
- Navigazione Internet
- Posta elettronica
- File testuali e di pacchetti office
- Immagini e video
- File criptati
- File di configurazione di sistema
- File di log
- Recupero dei file cancellati nel caso di clonazione della memoria mediante tecniche di carving

# Soluzioni post incidente - Digital Forensics

Fase 4, Analisi

- Ad ogni evidenza raccolta va calcolato l'hash e riportato all'interno della documentazione in una apposita tabella dei file di interesse

- Va riportato anche il path esatto dove è stato trovata l'evidenza o l'offset della memoria con annessi riferimenti temporali

# Soluzioni post incidente - Digital Forensics

## Fase 5, Presentazione

- Elenco dei software e degli strumenti utilizzati per l'acquisizione e l'analisi
- Elenco di tutte le attività eseguite passo passo
- Il lettore della perizia, seguendo la documentazione prodotta, deve ottenere gli stessi ed identici risultati ottenuti da chi ha eseguito l'attività
- Catalogare i file di interesse con il loro relativo hash
- Le risultanze devono dare risposta a tutti i quesiti posti dal committente
- In caso di consulenza tecnica privata per azienda, creare doppio report, un "executive summary" e un "technical summary"
- In caso di ctu o di ct da consegnare ad un magistrato, la relazione deve essere completa dei riferimenti tecnici ma di semplice comprensione anche per un giurista
- Limitarsi alla parte tecnico informatica

# Soluzioni post incidente - Digital Forensics

Fase 6, Catena di custodia

Documentazione da allegare ad ogni singola memoria, posta sotto sequestro o oggetto di analisi, dove annotare:

- Descrizione, marca, modello e numero di serie
- Chi custodisce la memoria e in quale periodo
- Hash della memoria
- Note di interesse

# Soluzioni post incidente - Digital Forensics, un caso pratico

- Una nota PMI emiliana con 50 dipendenti e fatturato pari a 20.000.000 €
- Una serie di eventi interni che bloccano la produzione dall'aziendale, spingono la presidenza nel richiedere una serie di indagini interne volte a riscontrare l'autore o gli autori che hanno generato questi blocchi
- L'attività di investigazione coinvolge sia esperti in Digital Forensics che agenzia investigativa

I controlli investigativi (pedinamenti in primis), producono un ottimo risultato: un commerciale e uno degli amministratori di sistema sono stati “beccati” a cena con altri due soggetti che sono risultati dipendenti dell’azienda competitrice

**Partono i controlli sugli asset aziendali!**

- Computer portatili
- Smartphone
- Tablet

**Cosa la legge ci permette di fare?**
**Privacy? Statuto dei lavoratori?**

Art. 113 D.lgs. 196/03 e art. 4 Statuto Lavoratori
*È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori a meno che non siano richieste da:*

- *Esigenze organizzative*
- *Esigenze produttive*
- *Esigenze di sicurezza*
- ***CONTROLLI LEGITTIMI O PRAETERINTENZIONALI***

*Art. 114 D.lgs. 196/03 e art. 8 Statuto Lavoratori*
*È fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi su:*

*1. Opinioni politiche, religiose o sindacali del lavoratore*
*2. Su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore.*

# Soluzioni post incidente - Digital Forensics, un caso pratico

La giurisprudenza ha introdotto con **i controlli difensivi** una ulteriore ipotesi di non applicazione del divieto dell'art. 4 dello Statuto dei Lavoratori:

*"Devono ritenersi certamente fuori dall'ambito di applicazione dell'art. 4 Statuto dei Lavoratori i controlli diretti ad accertare condotte illecite del lavoratore (c.d. controlli difensivi), quali, ad esempio, i sistemi di controllo dell'accesso ad aree riservate, o appunto gli apparecchi di rilevazione di telefonate ingiustificate".*

**In abito penale…**
L'attività principale riconosciuta dall'art. 327-bis c.p.p., è senza dubbio l'assunzione di informazioni da soggetti che possono rendere informazioni utili all'indagine.

Tuttavia, è prevista dall'art. 391-sexies anche la possibilità di effettuare un sopralluogo e di redigere un verbale che documenti l'attività svolta. In questa attività investigativa, potrebbe rientrare l'accesso a un sistema informatico aziendale da parte di un consulente tecnico nominato dall'avvocato, finalizzato a controllare la commissione di eventuali illeciti da parte del lavoratore.

Modus operandi:

- Si chiese la collaborazione del secondo amministratore di sistema spiegandogli lo scenario
- Sfruttando le ferie del primo amministratore ed una scusa di aggiornamento software, vengono trattenuti per una sera, tutti i portatili dell'azienda

- I portatili vengono acquisiti durante la notte
  - Una copia clone disco -> disco in sostituzione dell'hard disk originale all'interno dell'asset
  - Una copia disco -> imagefile per l'anali

I dischi originali vengono sigillati e conservati in cassaforte

# Soluzioni post incidente - Digital Forensics, un caso pratico

- Il computer del commerciale è risultato pulito
- Il computer dell'amministratore di sistema aveva alcune anomalie, evidenziate grazie ad una Timeline, quali:
  - Ereser installato da poco ed avviato la sera prima dell'intervento
  - Navigazione Internet e cache cancellata tramite Ccleaner
  - Db della chat di Skype vuoto con data di ultima scrittura la sera prima dell'intervento

Errori compiuti:

- Computer trovato in "freeze" con annesso hyberlif.sys
- Pagefile non cancellato
- Windows search attivo

Bulk extractor + indicazione della memoria hanno prodotto risultati interessanti!

# Soluzioni post incidente - Digital Forensics, un caso pratico

- Recuperati stralci di chat di Skype dove il commerciale e l'amministratore di sistema si accordavano per le azioni di sabotaggio

- Navigazione Internet recuperata grazie a bulk extractor che ha evidenziato una serie di bug applicativi, noti solo all'amministratore, che mandavano in blocco l'applicativo

- Riscontrate tracce di utilizzo della rete TOR

**Ci sono tutti gli elementi per un licenziamento per giusta causa e una denuncia penale con richiesta di compiere ulteriori accertamenti**

# Soluzioni post incidente - Digital Forensics & OSINT

# Soluzioni post incidente - Digital Forensics & OSINT

L'INTERVISTA di RICCARDO STAGLIANO'

Tweet Consiglia 2,3mila

## "Così combattiamo le ingiustizie sotto il segno di Anonymous"

Un gruppo di attivisti con la maschera di Guy Fakwes, protagonista del film 'V- Come Vendetta' e simbolo di Anonymous

**Incontro con uno dei leader dell'organizzazione mondiale di hacker che, in rete, attacca i siti di "nemici" potenti: da Trenitalia, per difendere la causa dei No Tav, al Vaticano. Un insospettabile professionista racconta cosa c'è dietro al gruppo più segreto e ricercato del mondo. Un movimento senza gerarchie, impenetrabile e implacabile nell'agire senza lasciare alcuna traccia di sè**

DA UNA LOCALITÀ SEGRETA.
Appuntamento al buio. Ci vediamo in una città del Sud che ho promesso di non rivelare. Non conosco il suo nome né il suo numero di telefono. Ho semplicemente scritto un'email. Per due settimane non ha risposto nessuno ("Ti stavo facendo le radiografie con Google"), poi il messaggio possibilista. Le condizioni sono chiare: dovrà essere assolutamente impossibile anche per sua madre e per la sua compagna, per non dire della polizia postale, riconoscerlo in quanto scriverò. Un'intervista criptata. Pixelata in ogni dettaglio che, incrociato con altri, possa far risalire alla sua vera identità. Perché i reati che ha commesso

# Soluzioni post incidente - Digital Forensics & OSINT

- Ribadisce le regole del gioco: “Non puoi neanche scrivere il mio nickname, quindi scrivi che hai parlato con uno tra Mendax, Attila, Savant, Phate Lucas, N4pst3r, Kirya, Case, B, Tor4k1k1, Netsec“

- “Non si aspettava qualcuno del genere, eh?” dice, allungando la mano. Inutile negare. Dov’è la felpa col cappuccio, magari un piercing o un tatuaggio?

- Promette nuove iniziative. Mi invita a seguirlo su twitter per essere il primo a sapere. “Ci saranno un paio di botti, nelle prossime settimane. Alcuni obiettivi grossi sui quali abbiamo, a grande maggioranza, convenuto”

# Soluzioni post incidente - Digital Forensics & OSINT

Cerco su Twitter Staglianò e mi metto a spulciare gli ultimi suoi "Following". Con un po di fortuna... Un anonimo con il cappuccio!!!

# Soluzioni post incidente - Digital Forensics & OSINT

Il caso Paola Landini (non è un case study di Spionaggio Industriale)

- Analizzando la memoria del pc, si evincono stralci di post dove la sig.ra Landini confidava il proprio stato d'animo
  - All'interno della memoria informatica non era possibile capire quando e dove quel post è stato scritto perché il computer era stato resettato
- Mediante l'utilizzo delle Google Dork e di frammenti di testo recuperati dalla memoria cancellata, è stato possibile ritrovare il post sul blog dove dichiarava di volersi togliere la vita

# Soluzioni post incidente - Digital Forensics & OSINT


site:url - ricerca solo nel sito indicato
site:url (image search) - mostra immagini solo del sito indicato
allintitle: - le parole ricercate sono tutte presenti nel page title
intitle: - le parole ricercate sono presenti nel page title
allintext: - le parole ricercate sono tutte presenti nel page text
intext: - le parole ricercate sono presenti nel page text

# Soluzioni post incidente - Digital Forensics & OSINT


allinurl: - le parole ricercate sono presenti nel URL
allinanchor: - le parole ricercate sono tutte presenti nel anchor text dei link
inanchor: - le parole ricercate sono tutte presenti nel anchor text dei link
cache: - mostra la versione contenuta nella google cache della pagina
info: - fornisce informazioni sulla pagina specificata
link: - fornisce le pagine che hanno un collegamento a quel URL
filetype: tipo - ricerca tutti i file aventi l'estensione che vogliamo cercare

# Bibliografia


- ISO 27037, Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence
- NIST SP800-86, Guide to Integrating Forensic Techniques into Incident Response
- Verizon, 2013 Data Breach Report
- McAffe quarterly threat q4 2013
- Avv. Giuseppe Vaciago, slide convegno Grow inSecurity - Bologna 2013
- Slide del corso di Computer Forensics con DEFT

# Contatti

**Dott. Stefano Fratepietro**

s.fratepietro@teslaconsulting.it
http://www.linkedin.com/in/stefanofratepietro
https://twitter.com/stevedeft

*Grazie… Domande?*