



DIRITTI CIVILI
E
«CAPTATORE INFORMATICO»

Andrea Ghirardini, CTO BE.IT SA





Diapositiva 2


▶ Senza annoiare nessuno dico solo che:

- ▶ Mi occupo di digital forensics da oltre 15 anni
- ▶ Ho un passato da hacker
- ▶ Ho lavorato per svariati VAR, ISP e Telco
- ▶ Mi occupo di IT Security da molto tempo
- ▶ Mi sono specializzato nelle tecnologie utilizzate in ambito enterprise e datacenter
- ▶ Vedo gente, faccio cose

CHI SONO





Diapositiva 3

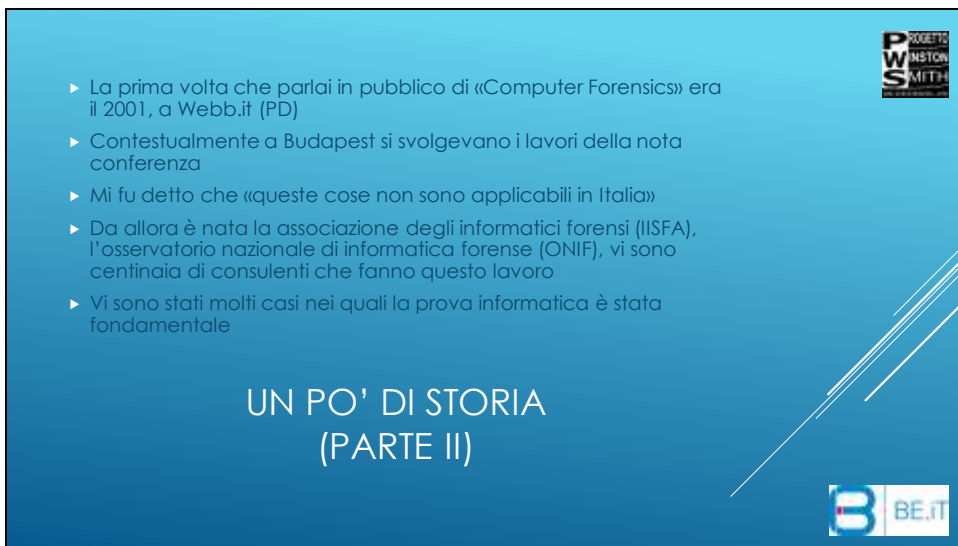


Avete mai letto questo libro?
Narra delle vicende relative una bruttissima indagine della procura di Pesaro, per la quale moltissimi nodi Fidonet furono chiusi e sequestrati senza alcun reale motivo. Un compendio di errori tecnici e giudiziari che ha scritto un brutto capitolo della nostra storia. Era il 1994 però... di acqua sotto i ponti ne è passata tanta.

UN PO' DI STORIA



Diapositiva 4



► La prima volta che parlai in pubblico di «Computer Forensics» era il 2001, a Webb.it (PD)



► Contestualmente a Budapest si svolgevano i lavori della nota conferenza

► Mi fu detto che «queste cose non sono applicabili in Italia»

► Da allora è nata la associazione degli informatici forensi (IISFA), l'osservatorio nazionale di informatica forense (ONIF), vi sono centinaia di consulenti che fanno questo lavoro

► Vi sono stati molti casi nei quali la prova informatica è stata fondamentale

UN PO' DI STORIA
(PARTE II)



Diapositiva 5

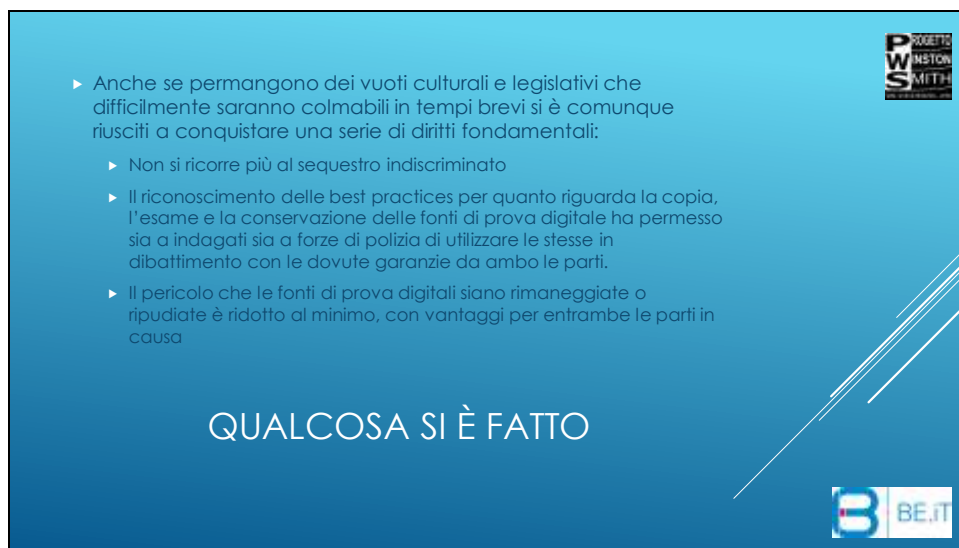
► Possiamo dire che **latita** (per essere reali e non «politically correct») possiamo affermare che non capisce la materia, legifera a caso o, nel migliore dei casi, se ne frega ampiamente)

- La Conferenza di Budapest è stata ratificata in legge con solo 7 anni di ritardo (legge 48/2008)
- La figura dell'esperto di Computer Forensics non è ancora riconosciuta dal Codice di Procedura Penale e quindi viene ancora pagato a «vacazioni» ovvero con la folle cifra di poco più di 4 € lordi a ora. **Questo ha un impatto devastante sulle indagini**
- Vi sono stati esempi di cattiva legislazione, come per esempio il decreto Pisanu, che ha dimostrato che chi è al governo non capisca nulla di tecnologia.

IL LEGISLATORE





Diapositiva 6



▶ Anche se permangono dei vuoti culturali e legislativi che difficilmente saranno colmabili in tempi brevi si è comunque riusciti a conquistare una serie di diritti fondamentali:

- ▶ Non si ricorre più al sequestro indiscriminato
- ▶ Il riconoscimento delle best practices per quanto riguarda la copia, l'esame e la conservazione delle fonti di prova digitale ha permesso sia a indagati sia a forze di polizia di utilizzare le stesse in dibattimento con le dovute garanzie da ambo le parti.
- ▶ Il pericolo che le fonti di prova digitali siano rimaneggiate o ripudiate è ridotto al minimo, con vantaggi per entrambe le parti in causa

QUALCOSA SI È FATTO



Diapositiva 7

- ▶ Nel corso degli scorsi anni la comunicazione in Italia (come anche negli altri paesi più civili di noi) è cambiata drasticamente
- ▶ La banda larga (da noi più pseudo banda larga) e gli smartphone sono stati una rivoluzione nelle nostre abitudini comunicative
- ▶ Nel corso degli scorsi anni si è visto il progressivo abbandono della telefonata per passare ad altri sistemi, come Instant Messaging, E-Mail, Chat, Social Network, VOIP ecc. ecc.
- ▶ Oltre a questo la crittografia si è fatta pervasiva e quindi moltissimi servizi utilizzati da milioni di persone sono passati sotto SSL/TLS (Google, FaceBook, Twitter, Bing, Outlook, Skype)


E PARLIAMO DI INTERCETTAZIONI



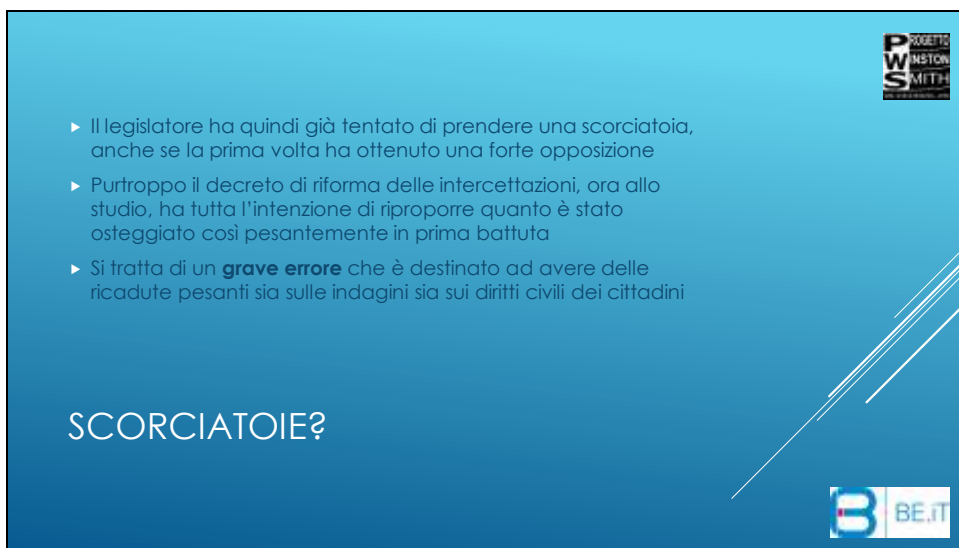
Diapositiva 8

- ▶ Inutile dire che questo ha progressivamente reso la vita più difficile agli inquirenti
- ▶ Si è cercato di utilizzare strumenti di investigazione e intercettazioni sempre più sofisticati e che possano controllare più media contemporaneamente includendo ben più della sola parte telefonica, compresi decine di servizi basati su IP
- ▶ Purtroppo nessuna attuale tecnologia può nulla contro la matematica e quindi molta parte del traffico IP (quella crittografata) rimane un mistero

INTERCETTAZIONI




Diapositiva 9



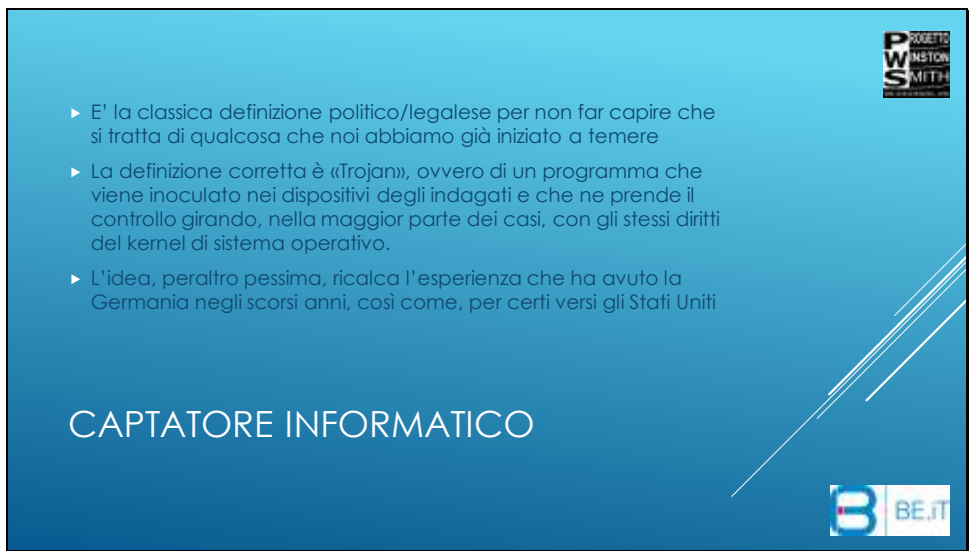
PWS
PROGETTO
WINSTON
SMITH

- ▶ Il legislatore ha quindi già tentato di prendere una scorciatoia, anche se la prima volta ha ottenuto una forte opposizione
- ▶ Purtroppo il decreto di riforma delle intercettazioni, ora allo studio, ha tutta l'intenzione di riproporre quanto è stato osteggiato così pesantemente in prima battuta
- ▶ Si tratta di un **grave errore** che è destinato ad avere delle ricadute pesanti sia sulle indagini sia sui diritti civili dei cittadini

SCORCIATOIE?



Diapositiva 10





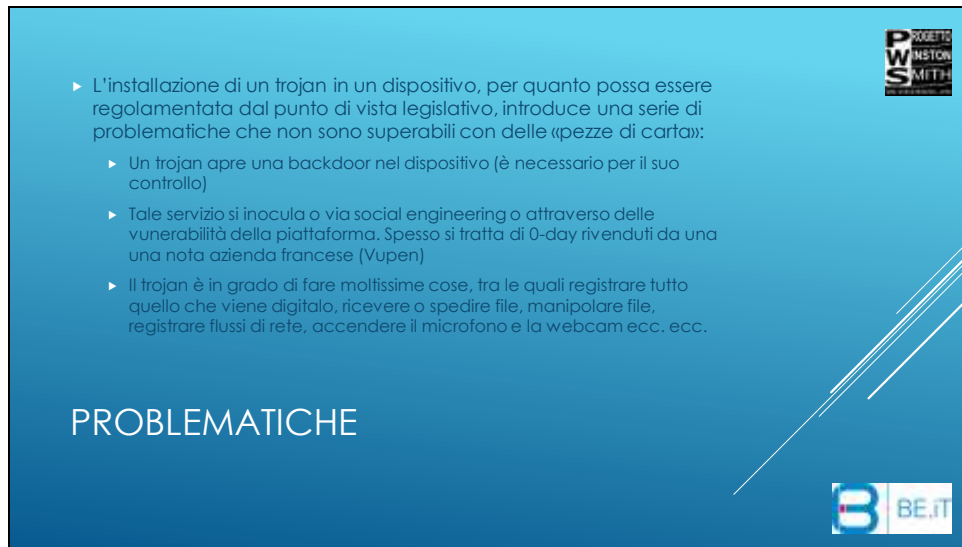
► E' la classica definizione politico/legalese per non far capire che si tratta di qualcosa che noi abbiamo già iniziato a temere

► La definizione corretta è «Trojan», ovvero di un programma che viene inoculato nei dispositivi degli indagati e che ne prende il controllo girando, nella maggior parte dei casi, con gli stessi diritti del kernel di sistema operativo.

► L'idea, peraltro pessima, ricalca l'esperienza che ha avuto la Germania negli scorsi anni, così come, per certi versi gli Stati Uniti

CAPTATORE INFORMATICO





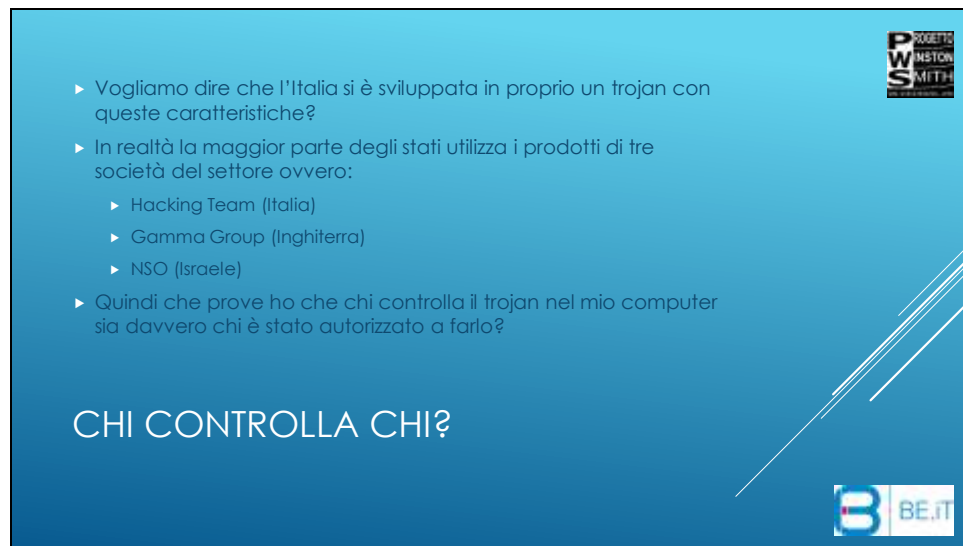
PROBLEMATICHE

- ▶ L'installazione di un trojan in un dispositivo, per quanto possa essere regolamentata dal punto di vista legislativo, introduce una serie di problematiche che non sono superabili con delle «pezze di carta»:
 - ▶ Un trojan apre una backdoor nel dispositivo (è necessario per il suo controllo)
 - ▶ Tale servizio si inocula o via social engineering o attraverso delle vulnerabilità della piattaforma. Spesso si tratta di 0-day rivenduti da una nota azienda francese (Vupen)
 - ▶ Il trojan è in grado di fare moltissime cose, tra le quali registrare tutto quello che viene digitato, ricevere o spedire file, manipolare file, registrare flussi di rete, accendere il microfono e la webcam ecc. ecc.

PWS

BE.IT

Diapositiva 12





▶ Vogliamo dire che l'Italia si è sviluppata in proprio un trojan con queste caratteristiche?

▶ In realtà la maggior parte degli stati utilizza i prodotti di tre società del settore ovvero:

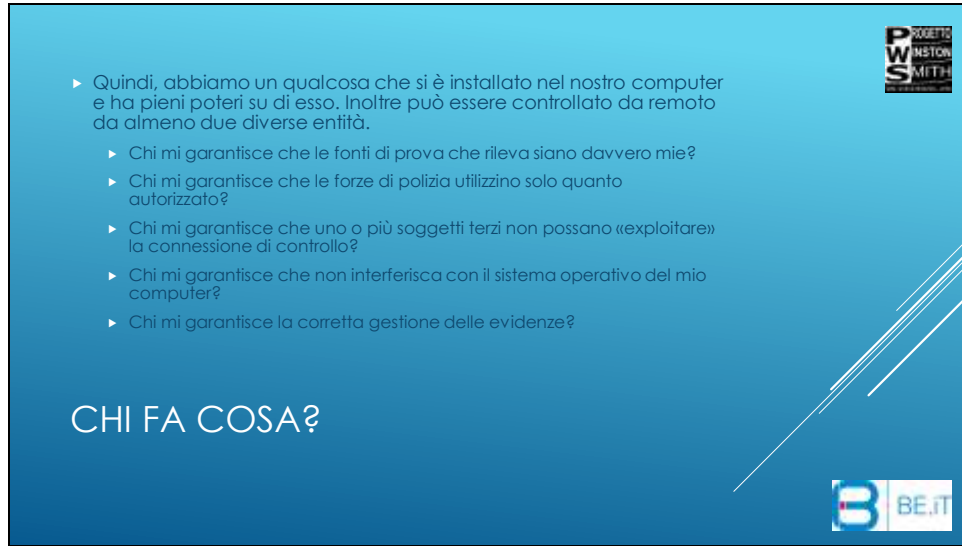
- ▶ Hacking Team (Italia)
- ▶ Gamma Group (Inghilterra)
- ▶ NSO (Israele)

▶ Quindi che prove ho che chi controlla il trojan nel mio computer sia davvero chi è stato autorizzato a farlo?

CHI CONTROLLA CHI?



Diapositiva 13





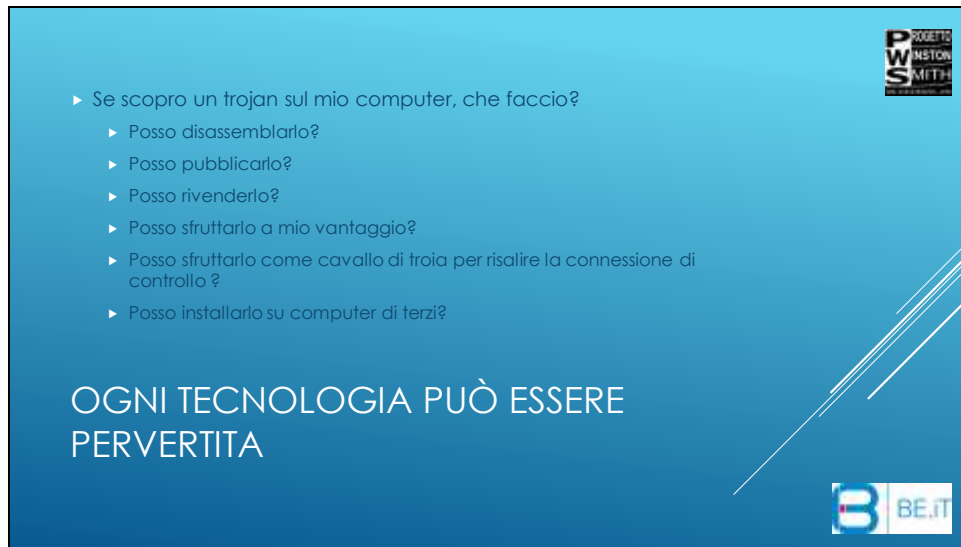
The slide features a blue gradient background. In the top right corner, there is a logo for 'PWS' with the names 'ROBERTO WILSON SMITH' stacked vertically. In the bottom right corner, there is a logo for 'BE.IT' with a stylized 'B' containing a flag. The main text is a bulleted list of questions, and the title 'CHI FA COSA?' is positioned in the lower-left area of the slide.

► Quindi, abbiamo un qualcosa che si è installato nel nostro computer e ha pieni poteri su di esso. Inoltre può essere controllato da remoto da almeno due diverse entità.

- Chi mi garantisce che le fonti di prova che rileva siano davvero mie?
- Chi mi garantisce che le forze di polizia utilizzino solo quanto autorizzato?
- Chi mi garantisce che uno o più soggetti terzi non possano «exploitare» la connessione di controllo?
- Chi mi garantisce che non interferisca con il sistema operativo del mio computer?
- Chi mi garantisce la corretta gestione delle evidenze?

CHI FA COSA?







▶ Se scopro un trojan sul mio computer, che faccio?


- ▶ Posso disassemblarlo?
- ▶ Posso pubblicarlo?
- ▶ Posso rivenderlo?
- ▶ Posso sfruttarlo a mio vantaggio?
- ▶ Posso sfruttarlo come cavallo di troia per risalire la connessione di controllo ?
- ▶ Posso installarlo su computer di terzi?

OGNI TECNOLOGIA PUÒ ESSERE
PERVERTITA




▶ I «trojan di stato» sono una pessima idea, da qualunque punto di vista li si guardi. In futuro saranno comuni scenari di questo genere:

- ▶ Abusi delle funzioni da parte delle forze di polizia o soggetti terzi
- ▶ Le fonti di prova portate a dibattimento saranno quasi certamente dichiarate inutilizzabili in quanto la loro autenticità e paternità non potranno in alcun modo essere garantite
- ▶ Si creeranno delle falle di sicurezza in centinaia di elaboratori diversi
- ▶ Si creerà un mercato (legale o meno) per le contromisure relative
- ▶ Chi davvero sa come usare la tecnologia non ne sarà affatto colpito



SCENARI FUTURI





DOMANDE? DUBBI?

Andrea Ghirardini
Email: ghirardini@beitsa.ch
darkpila@outlook.com
Tel: +39 377 110 110 1 +41 78 946 68 36