Introduzione alla sicurezza delle reti e dei sistemi informativi

Antonio Lioy
< lioy @ polito.it >

Politecnico di Torino
Dip. Automatica e Informatica

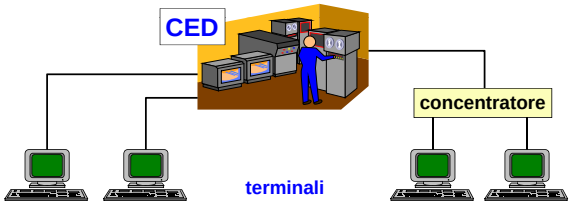
Indice

- **introduzione alla sicurezza dei sistemi ICT:**
  - l'evoluzione dei sistemi ICT ed il problema sicurezza
  - le problematiche ed il lessico della sicurezza ICT
  - gli attacchi tecnologici (sniffing, spoofing, …)
  - gli attacchi non tecnologici (social engineering)

Perché è esploso il problema "sicurezza" ?

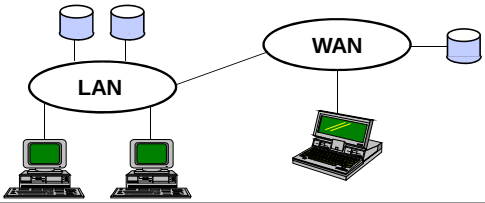
Vecchi paradigmi

- **informazioni ed elaborazione centralizzate**
- **accesso tramite postazioni "stupide"**
- **comunicazione "unicast" tramite linee dedicate**

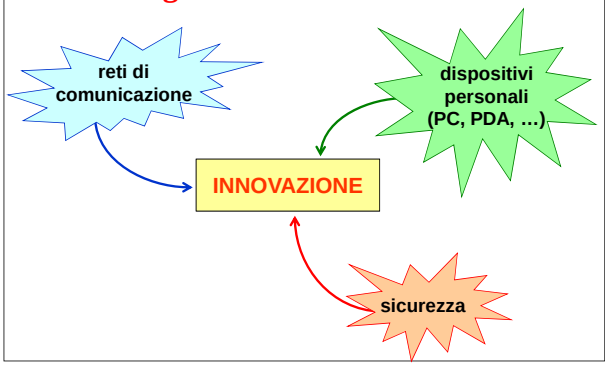


Nuovi paradigmi

- **informazioni ed elaborazione distribuite**
- **accesso tramite postazioni distribuite intelligenti**
- **comunicazioni "broadcast" e/o linee condivise**
- **nuovi paradigmi applicativi (web, P2P, SMS, …)**



La tecnologia come motore di innovazione



Una definizione di sicurezza informatica

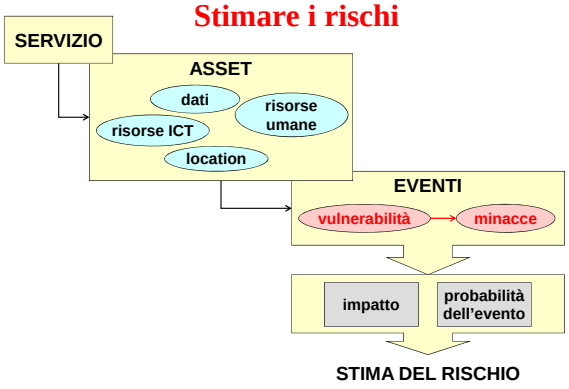
E' l'insieme dei prodotti, dei servizi, delle regole organizzative e dei comportamenti individuali che proteggono i sistemi informatici di un'azienda.

Ha il compito di proteggere le risorse da accessi indesiderati, garantire la riservatezza delle informazioni, assicurare il funzionamento e la disponibilità dei servizi a fronte di eventi imprevedibili (C.I.A. = Confidentiality, Integrity, Availability).

L'obiettivo è custodire le informazioni con la stessa professionalità ed attenzione con cui ci si prende cura di gioielli o certificati azionari depositati nel caveau.

Il sistema informatico è la cassaforte delle nostre informazioni più preziose; la sicurezza informatica è l'equivalente delle serrature, combinazioni e chiavi che servono a proteggerla.

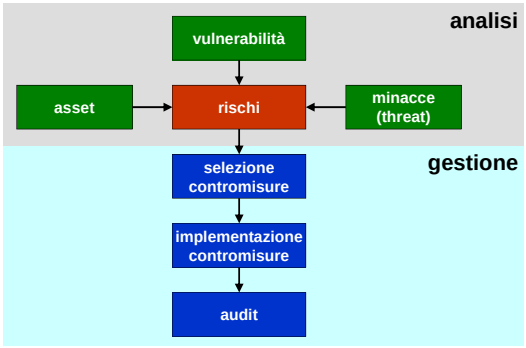
Stimare i rischi



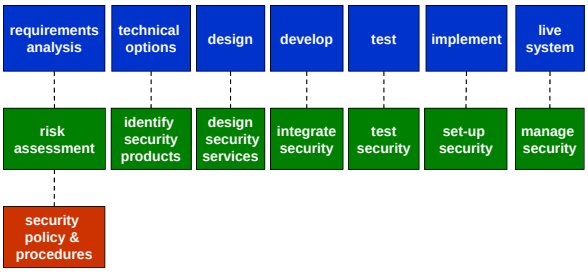
Terminologia

- **ASSET = l'insieme di beni, dati e persone necessarie all'erogazione di un servizio IT**
- **VULNERABILITA' = debolezza di un asset**
  - es. pwd = login; sensibile alle inondazioni
- **MINACCIA = evento intenzionale o accidentale che può causare la perdita di una proprietà di sicurezza**
- **ATTACCO = verificarsi di una minaccia di tipo "evento intenzionale"**
- **EVENTO (NEGATIVO) = verificarsi di una minaccia di tipo "evento accidentale"**

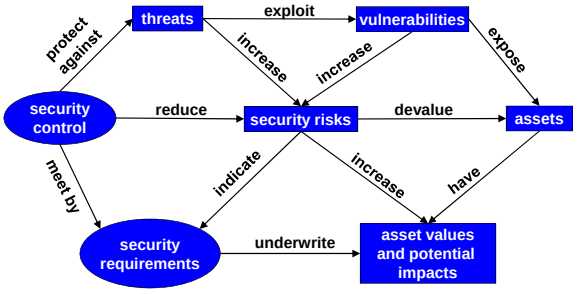
Analisi e gestione della sicurezza



La sicurezza nel ciclo di vita di un sistema



Relazioni nel campo della sicurezza

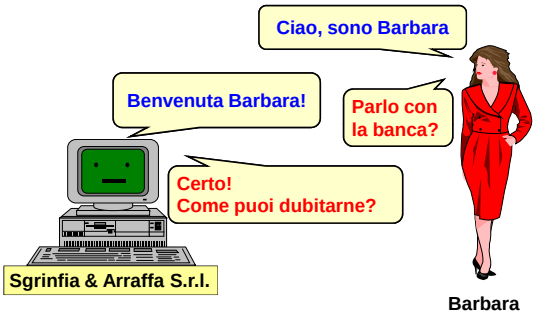


Proprietà (astratte) di sicurezza

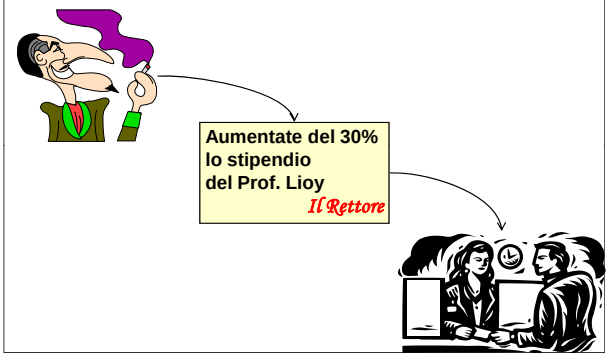
autenticazione (semplice / mutua)	***authentication (simple / mutual)***
autenticazione della controparte	***peer authentication***
autenticazione dei dati	***data / origin authentication***
autorizzazione, controllo accessi	***authorization, access control***
integrità	***integrity***
riservatezza, confidenzialità	***confidentiality, privacy, secrecy***
non ripudio	***non repudiation***
disponibilità	***availability***
tracciabilità	***accountability***

Autenticazione (della controparte)

Mutua autenticazione (delle controparti)



Autenticazione (dei dati)



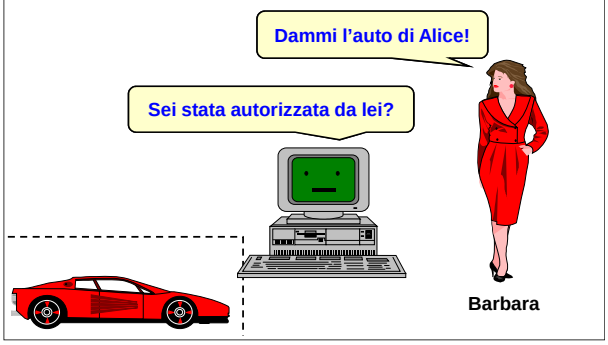
Non ripudio

- **prova formale - usabile in tribunale - che dimostra in modo innegabile l'autore dei dati**
- **molti aspetti da considerare:**
  - autenticazione (del mittente)
  - integrità
  - identificazione (del mittente)
  - . . .

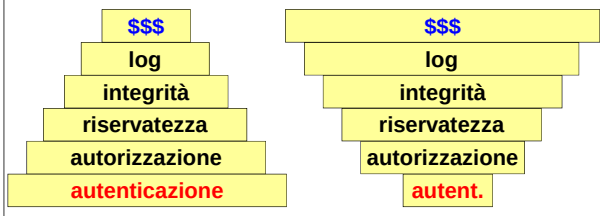
Non ripudio - esempio

- **consideriamo il non ripudio di una firma elettronica:**
  - sintassi (è la tua firma?)
  - semantica (hai capito ciò che stavi firmando?)
  - volontà (hai firmato volontariamente?)
  - identificazione (sei stato tu a firmare?)
  - tempo (quando hai firmato?)
  - luogo (dove hai firmato?)

Autorizzazione (controllo accessi)

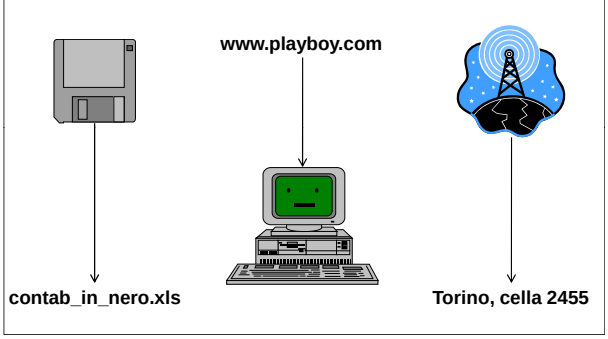


La piramide della sicurezza

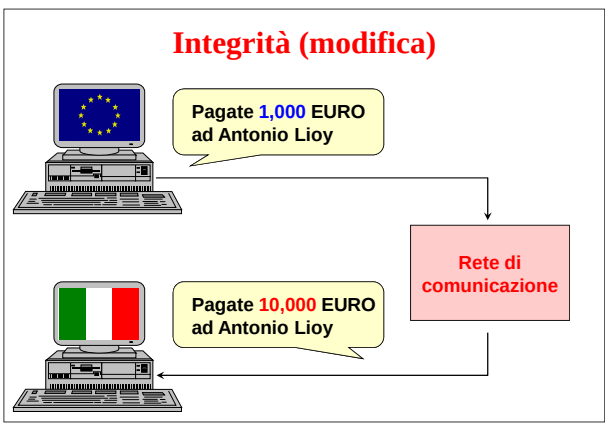


Riservatezza (delle comunicazioni)

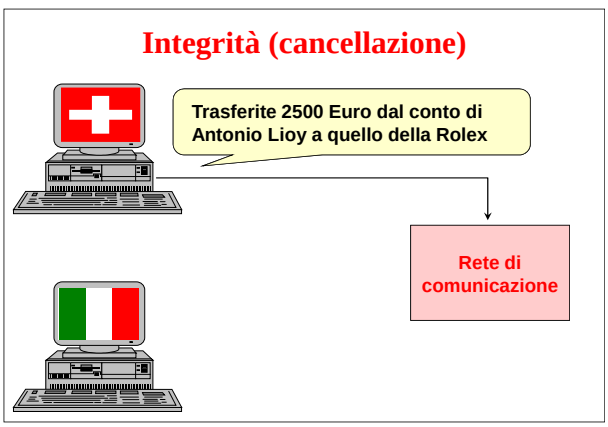
Riservatezza (dati, azioni, posizione)



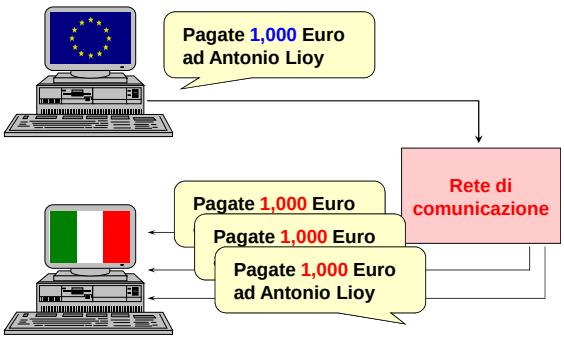
Integrità (modifica)



Integrità (cancellazione)

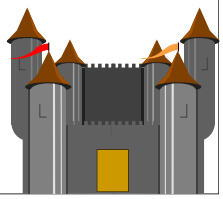


Attacchi di tipo “replay”



Sicurezza: dove è il nemico?

- **fuori dalla nostra organizzazione**
  - difesa del perimetro (firewall)
- **fuori dalla nostra organizzazione, con l’eccezione dei nostri partner**
  - protezione dell’Extranet (VPN)
- **dentro la nostra organizzazione**
  - protezione della Intranet (?!)
- **ovunque !**
  - protezione delle applicazioni
  - protezione dei dati

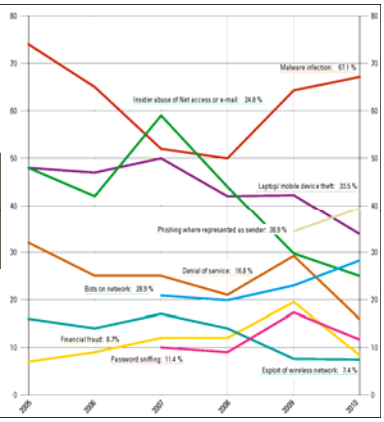


Origine dell’attacco? (2010)

- **percentuale di attacchi esterni / interni:**
  - interni 30-50%
  - esterni 70-50%
- **percentuale delle perdite totali causate da personale interno:**
  - 40% da personale “malvagio”
  - 60% da personale “stupido”

(dai report CSI/FBI e Verizon/USSS 2010)

Evoluzione temporale dei principali attacchi rilevati dalla survey annuale CSI/FBI



Furto di laptop / PDA

- **non solo un danno economico per rimpiazzare l'oggetto rubato …**
- **ma la perdita di dati non più disponibili (backup?)**
- **o la diffusione di informazioni riservate**

Scoop di giornalista del Global Post nella città tra Pakistan e Afghanistan

Nei mercatini di Peshàwar i PC dei marine

Computer con contenuti riservati in vendita a 650$ lungo la strada dove i convogli Nato sono attaccati dai talebani. … computer dell'esercito Usa. Ancora pieni di informazioni classificate, come nomi di militari, siti di dislocamento, debolezze e carenze strutturali dei mezzi di trasporto e di combattimento. (corriere.it, 9/2/09)

Insicurezza: le cause profonde (I)

- **“Attack technology is developing in a open-source environment and is evolving rapidly”**
- **“Defensive strategies are reactionary”**
- **“Thousands - perhaps millions - of system with weak security are connected to the Internet”**
- **“The explosion in use of the Internet is straining our scarse technical talent. The average level of system administrators … has decreased dramatically in the last 5 years”**

Insicurezza: le cause profonde (II)

- **"Increasingly complex sw is being written by programmers who have no training in writing secure code"**
- **"Attacks and attack tools trascend geography and national boundaries"**
- **"The difficulty of criminal investigation of cybercrime coupled with the complexity of international law means that … prosecution of computer crime is unlikely"**

da "Roadmap for defeating DDOS attacks" (feb. 2000, after Clinton meeting at White House) aggiornamenti su www.sans.org/dosstep/roadmap.php

Problemi base (tecnologici)

- **le reti sono insicure:**
  - le comunicazioni avvengono in chiaro
  - le reti locali funzionano in broadcast
  - le connessioni geografiche non avvengono tramite linee punto-punto ma:
    - attraverso linee condivise
    - tramite router di terzi
- **autenticazione debole degli utenti (normalmente basata su password)**
- **non c'è autenticazione dei server**
- **il software contiene molti bachi!**

Alcune tipologie di attacco

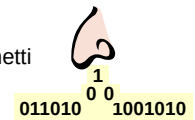
- **IP spoofing / shadow server**
  qualcuno si sostituisce ad un host
- **packet sniffing**
  si leggono password di accesso e/o dati riservati
- **connection hijacking / data spoofing**
  si inseriscono / modificano dati durante il loro transito in rete
- **denial-of-service (DoS) e distributed DoS (DDoS)**
  si impedisce il funzionamento di un servizio (es. la guerra dei ping)

IP spoofing

- **falsificazione dell'indirizzo di rete del mittente**
- **solitamente si falsifica l'indirizzo di livello 3 (IP) ma nulla vieta di falsificare anche quello di livello 2 (ETH, TR, ...)**
- **meglio chiamarlo *source address spoofing***
- **attacchi:**
  - falsificazione di dati
  - accesso (non autorizzato) a sistemi
- **contromisure:**
  - NON usare mai autenticazione basata sugli indirizzi di rete

Packet sniffing

- **lettura dei pacchetti destinati ad un altro nodo della rete**
- **facile da fare in reti broadcast (es. LAN) o nei nodi di smistamento (es. switch, router)**
- **attacchi:**
  - permette di intercettare qualunque cosa (password, dati, ...)
- **contromisure:**
  - reti non broadcast (!?)
  - crittografia del payload dei pacchetti



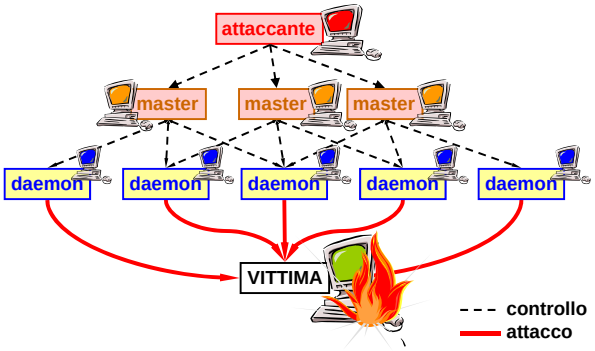
Denial-of-service (DoS)

- **si tiene impegnato un host in modo che non possa fornire i suoi servizi**
- **esempi:**
  - saturazione della posta / log
  - ping flooding ("guerra dei ping")
  - SYN attack
- **attacchi:**
  - impedisce l'uso di un sistema / servizio
- **contromisure:**
  - nessuna definitiva, solo palliativi quantitativi

Distributed denial-of-service (DDoS)

- **software per DOS installato su molti nodi (chiamati daemon, zombie o malbot) costituendo una Botnet**
- **daemon controllati remotamente da un master (spesso tramite canali cifrati) e con capacità di auto-aggiornamento**
- **effetto dell'attacco base moltiplicato per il numero di daemon**
- **esempi:**
  - TrinOO
  - TFN (Tribe Flood Network)
  - Stacheldraht (=filo spinato)

DDoS attack



Feb 8th 2000, 10.30am (PST) @ Yahoo Server Farm

- **"the initial flood of packets, which we later realized was in excess of 1G bits/sec, took down one of our routers …"**
- **"… after the router recovered we lost all routing to our upstream ISP …"**
- **"… it was somewhat difficult to tell what was going on, but at the very least we noticed lots of ICMP traffic …"**
- **"… at 1.30pm we got basic routing back up and then realized that we were under a DDoS attack"**

http://packetstorm.decepticons.org/distributed/yahoo.txt

The lawyer said ...

"There is a distinct probability that if your site has been hijacked for a denial of service attack, then you could be liable for damages.

I would definitely advise clients they have grounds to sue."

Nick Lockett, e-commerce lawyer at Sidley & Austin

"Be Secure or Be Sued"
Silicon.com, 16 Nov 2000

http://www.silicon.com/a40900

Shadow server

- **elaboratore che si pone come fornitore di un servizio senza averne il diritto**
- **richiede address spoofing e packet sniffing**
- **il server ombra deve essere più veloce di quello reale, oppure questo non deve essere in grado di rispondere (guasto o sotto attacco, es. DoS)**
- **attacchi:**
  - fornitura di un servizio sbagliato
  - cattura di dati forniti al servizio sbagliato
- **contromisure:**
  - autenticazione del server

Connection hijacking

- **anche detto *data spoofing***
- **si prende il controllo di un canale di comunicazione e si inseriscono, cancellano o manipolano dei pacchetti**
- **MITM (Man In The Middle) logico o fisico**
- **attacchi:**
  - lettura, falsificazione e manipolazione di dati
- **contromisure:**
  - autenticazione, integrità e serializzazione di ogni singolo pacchetto di rete

Software bug

- **anche il miglior software contiene dei bug che possono essere sfruttati per vari fini**
- **sfruttamento più semplice: DoS**
- **esempio: WinNT server (3.51, 4.0)**
  - telnet alla porta 135
  - 10 caratteri a caso, poi CR
  - server non disponibile!
    (CPU al 100% senza che venga svolto alcun lavoro)
  - soluzione: installare SP3

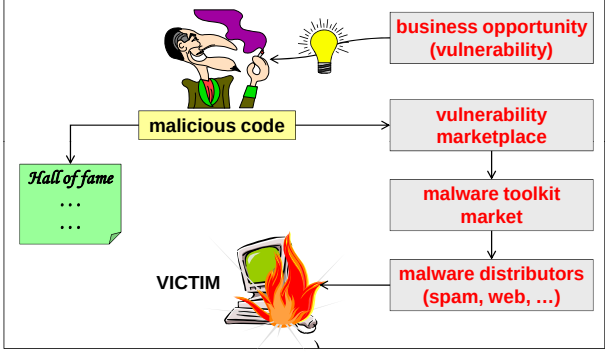
Alcuni tipici problemi applicativi

- **buffer overflow**
  - permette l'esecuzione di codice arbitrario iniettato tramite un input appropriatamente manipolato
- **memorizzare nei cookie informazioni sensibili**
  - leggibili da terzi (in transito o localmente sul client)
- **memorizzare le password in chiaro in un DB**
  - leggibili da terzi (es. l'operatore del backup)
- **"inventare" un sistema di protezione**
  - rischio di protezione inadeguata (se sbagliano i grandi figuriamoci cosa combinano i novizi ...)

Virus e worm (malware)

- **virus = provoca danni e si replica**
- **worm = provoca danni perché si replica**
- **richiede complicità (anche involontaria):**
  - dell'utente (gratis, free, urgente, importante, …)
  - del sistemista (malconfigurazione)
  - del produttore (esecuzione automatica, trusted, …)
- **contromisure:**
  - sensibilizzazione degli utenti
  - configurazioni corrette / sw sicuro
  - installazione (ed aggiornamento!) degli antivirus

Malware food chain



Problemi base (non tecnologici)

- **scarsa comprensione del problema (awareness)**
- **fallibilità degli esseri umani (soprattutto in condizioni di sovraccarico, frustrazione, …)**
- **gli esseri umani hanno una naturale tendenza alla fiducia**
- **interfacce / architetture complesse che facilitano gli errori**
- **calo di prestazioni dovuto all'applicazione delle misure di sicurezza**
- **…**

Social engineering

- **si chiede la partecipazione (inconsapevole) dell'utente all'azione di attacco**
- **si sfruttano utenti ingenui ("per favore cambia subito la password con la seguente, perché il tuo PC è sotto attacco") …**
- **… ma si attaccano anche utenti esperti (es. copiando un mail autentico ma cambiandogli un allegato o una URL)**
- **via mail, telefono o anche comunicazioni cartacee**

Esempi di social engineering

- **il Phishing (~ fishing = la pesca al gonzo)**
  - "gentile utente del servizio di Internet banking la preghiamo di compilare e spedirci il seguente modulo ai sensi della legge 675 …"
- **pressioni psicologiche:**
  - "se non mi aiuti sono nei pasticci …"
  - "se non fai quello che chiedo lo segnalerò al tuo responsabile …"
- **dimostrare di conoscere bene l'azienda, le persone, le procedure per far abbassare la guardia**

Un mail dalla CIA …

```
From: Post@cia.gov
Date: Tue, 22 Nov 2005 17:51:14 UTC
X-Original-Message-ID: <1e3c8.15d13bbb95@cia.gov>
Subject: You_visit_illegal_websites

Dear Sir/Madam,
we have logged your IP-address on more than 30 illegal Websites.
Important: Please answer our questions!
The list of questions are attached.

Yours faithfully,
Steven Allison

++++ Central Intelligence Agency -CIA-
++++ Office of Public Affairs
++++ Washington, D.C. 20505
++++ phone: (703) 482-0623
++++ 7:00 a.m. to 5:00 p.m., US Eastern time
```

l'allegato è il worm SOBER !

Phishing

- **attrarre via mail o IM l'utente di un servizio di rete su un server fasullo (shadow server) per:**
  - catturare credenziali di autenticazione o altre informazioni personali
  - convincerlo ad installare un plugin o estensione che è in realtà un virus o un trojan
- **varianti specializzate:**
  - spear phishing (include molti dati personali per aumentare la credibilità del messaggio, es. indirizzi di posta, nome del Dipartimento/Ufficio, telefono)
  - whaling (mirato a persone importanti tipo CEO o CIO, es. circa 20,000 colpiti ad aprile'08 ed hanno installato un trojan collegato ai server di Piradius)

Pharming

- **termine di uso controverso**
- **insieme di varie tecniche per re-indirizzare un utente verso uno shadow server**
  - cambiamento del file "host" sul client
  - cambiamento dei puntatori ai nameserver sul client
  - cambiamento dei nameserver su un DHCP server (es. un router ADSL e/o wireless)
  - avvelenamento della cache di un nameserver
- **tramite:**
  - attacco diretto (vulnerabilità o malconfigurazione)
  - attacco indiretto (virus o worm)

Tecniche di social engineering

- **(74%) solicitation / bribery = corruzione**
- **(44%) pretexting = impersonificazione**
- **(16%) counterfeiting / forgery = contraffazione**
- **(11%) *ing = phishing, pharming, …**
- **(4%) hoax / scam = false comunicazioni**
- **(4%) influence tactics = principio di autorità**
- **(3%) extortion / blackmail = estorsione, ricattu**

Nota: % di uso in attacchi di social engineering secondo la survey Verizon/USSS 2011.

Canali di social engineering

- **(78%) in persona**
- **(14%) documenti**
- **(10%) e-mail**
- **(6%) web / Internet**
- **(5%) telefono**
- **(4%) SMS / messaggistica**

Nota: % di uso in attacchi di social engineering secondo la survey Verizon/USSS 2011.

Key findings (Verizon 2011)

- **large-scale breaches dropped dramatically while small attacks increase**
  - easier to catch (many) small fishes than big ones
- **outsiders responsible for most data breaches**
  - proportion is about 80-20
- **physical attacks on the rise**
  - especially skimmers at ATM, gas-pumps, and POS
- **hacking / malware the most popular attack**
  - malware sent to install backdoor and keylogger
- **stolen passwords / credentials out of control**
  - ineffective, weak, default, or stolen credentials

Key recommendations (Verizon 2011)

- **focus on essential controls across the whole IS**
  - better than exceptional protection for a few areas
- **eliminate unnecessary data**
  - don't keep data that are not strictly required
- **audit user accounts and monitor privileged users**
  - pre-employment screening, limited user privileges, separation of duties, audit attempted/successful violations
- **monitor and mine event logs**
  - favour speed of detection over analysis of minutia
- **monitor security of physical devices**
  - fast detection of tampered devices

Attacco a T.J.Maxx (2007)

- **rubati 45 milioni di numeri di carte di credito/debito**
- **in un periodo di 18 mesi (fino a gennaio 2007)**
- **intentata azione legale di classe per decine di M USD da parte di 300 banche (es. Massachusetts Bankers Association, Maine and Connecticut Associated Banks)**
- **attacco riuscito per uso di WEP invece di WPA**
- **attacco condotto da 10 persone (3 USA, 3 UKR, 2 CHN, 1 BEL, 1 EST + "Delpiero")**
- **un ex-cracker assunto dai servizi segreti USA**

blog.wired.com/27bstroke6/2008/08/11-charged-in-m.html
www.wired.com/politics/law/news/2007/06/secret_service#

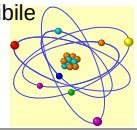
Phishing via Transformers3 (apr 2010)

- **Andersen Air Force Base (isola di Guam)**
- **ORE (Operational Readiness Exercise)**
  - phishing message
  - "the movie Transformers-3 will be filmed on Guam"
  - "looking for 20 airmen to be part of the movie"
  - application required disclosing sensitive information
  - event leaked on the web because one airman disclosed that on Transformer fans' blog
  - journalists called to confirm movie location

www.networkworld.com/news/2010/043010-us-air-force-phishing-test.html

Stuxnet (2010)

- **prototipo di un nuovo tipo di attacco**
- **worm + virus per Windows**
  - cerca di propagarsi ad altri sistemi
  - cerca di danneggiare gli eventuali sistemi SCADA (di uno specifico fornitore) collegati
- **vettori di attacco e propagazione:**
  - 2 vulnerabilità "zero-day"
  - 1 vulnerabilità nota e con patch disponibile
  - 1 vulnerabilità nota ma senza patch



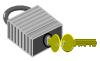
Stuxnet: tempistica e localizzazione

- **17/6/10 primo avvistamento**
- **24/6/10 notato uso di un certificato di firma**
  - **viene revocato il 17/7/10**
  - **… e quindi scoperto l'uso del secondo certificato**
- **14-15-16/7/10 vari avvisi di sicurezza da CERT e MS**
- **rilascio graduale di patch sino ad ottobre 2010**
- **auto-cesserà di propagarsi il 24/6/2012**
- **localizzazione geografica:**
  - **52% Iran**
  - **17% Indonesia**
  - **11% India**

Stuxnet: meccanismi

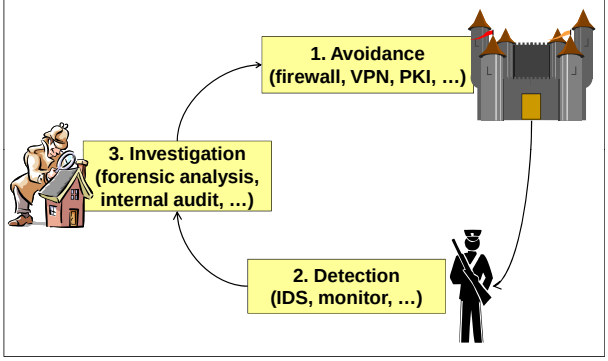
- **distribuzione e propagazione:**
  - chiavetta USB
  - dischi condivisi (network share)
  - bachi di MS-RPC e MS-spool
- **probabile primo veicolo di infezione una chiavetta USB dei tecnici di manutenzione**
- **si mimetizza come un driver**
  - con firma digitale validata da Microsoft!!!
  - usa due diversi certificati
- **accesso dal sistema infettato al DB di back-end tramite pwd di default identica su tutti i sistemi**

Stuxnet: lezioni da imparare

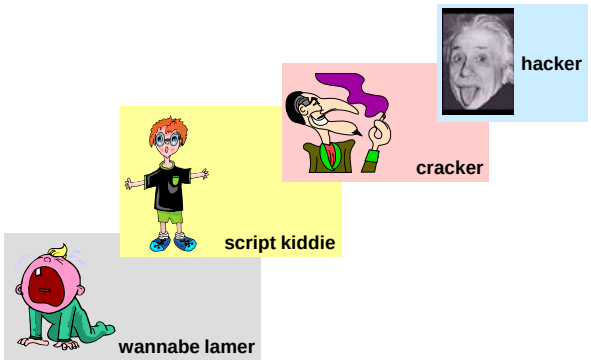


- **sistemi protetti da separazione fisica (air gap) ma privi di altre protezioni:**
  - no anti-virus
  - no patch
  - no firewall
- **servizi attivi non necessari:**
  - MS-RPC
  - condivisione coda di stampa in rete
  - condivisione dischi in rete
- **lista di validazione per il sw da installare**

I tre pilastri della sicurezza



Hacker & C.



Hacker (I)

hacker: /n./ [originally, someone who makes furniture with an axe]

1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary.

2. One who programs enthusiastically (even obsessively) or who enjoys programming rather than just theorizing about programming.

3. A person capable of appreciating {hack value}.

4. A person who is good at programming quickly.

Hacker (II)

5. An expert at a particular program, or one who frequently does work using it or on it; as in "a Unix hacker". (Definitions 1 through 5 are correlated, and people who fit them congregate.)

6. An expert or enthusiast of any kind. One might be an astronomy hacker, for example.

7. One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations.

8. [deprecated] A malicious meddler who tries to discover sensitive information by poking around. Hence "password hacker", "network hacker". The correct term for this sense is {cracker}.

Cracker

cracker: /n./ One who breaks security on a system. Coined ca. 1985 by hackers in defense against journalistic misuse of {hacker} (q.v., sense 8). An earlier attempt to establish "worm" in this sense around 1981-82 on Usenet was largely a failure.

Kevin Siers, NC, USA (cartoon from the Charlotte Observer)