

# KEYLOGGER



Lucia Canali,  
5 Dec

# KEYLOGGER

- strumento hardware o software in grado di intercettare e catturare segretamente tutto ciò che viene digitato sulla tastiera.



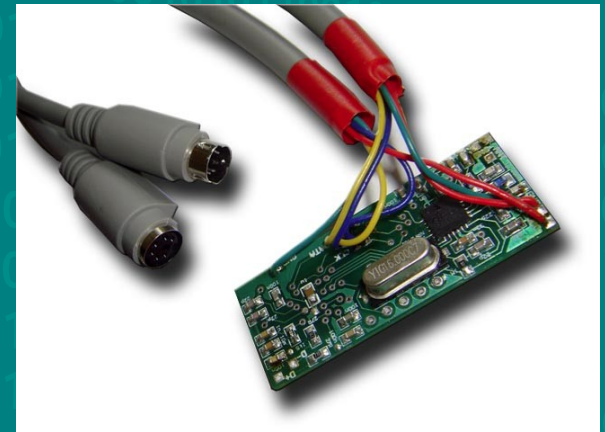
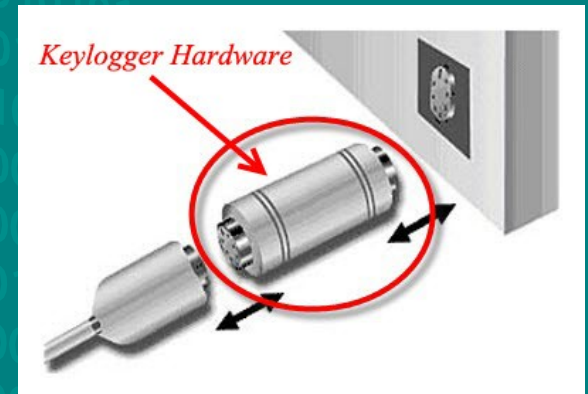
# KEYLOGGER HARDWARE

- dispositivo elettronico posizionato sul cavo di comunicazione tra la tastiera e il computer o all'interno della tastiera stessa.
- possono inviare i dati in rete
- possono essere monitorati e comandati in remoto
- devono essere recuperati fisicamente



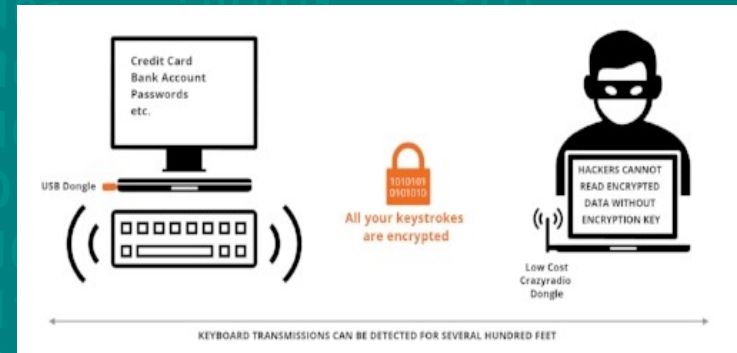
# KEYLOGGER HARDWARE

<b>vantaggi</b>	<b>svantaggi</b>
installazione molto semplice	è necessario ottenere l'accesso fisico alla tastiera o al computer
hanno sembianze di adattatori o di cavi prolunga	
invisibili ai software antivirus	
nascosti nella tastiera risultano del tutto invisibili	



# KEYLOGGER HARDWARE: TECNICHE

- Sniffing tastiera wireless:  
si usa uno sniffer per intercettare i pacchetti.



- Keylogger acustico:  
si basa sulla distinzione del suono dei tasti della tastiera.



# KEYLOGGER HARDWARE: TECNICHE

## Emissioni elettromagnetiche:

si usano ricevitori a banda larga per sintonizzarsi alla frequenza di emissione delle tastiere.



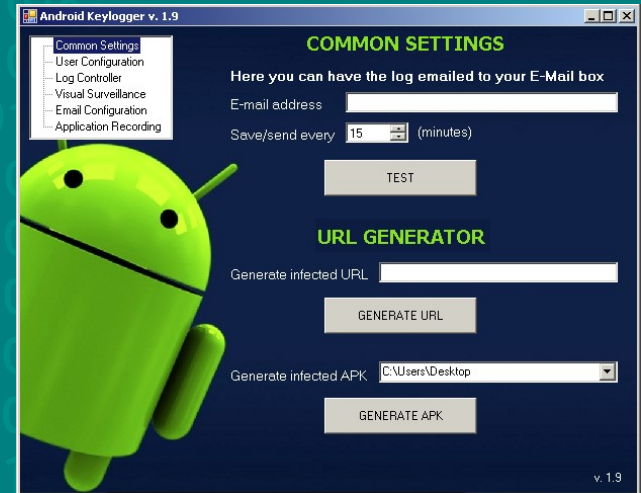
# KEYLOGGER SOFTWARE

- software creato per rilevare e memorizzare la sequenza dei pulsanti che vengono digitati. Normalmente l'esecuzione è nascosta.
- I dati possono essere trasmessi in remoto.



# KEYLOGGER SOFTWARE

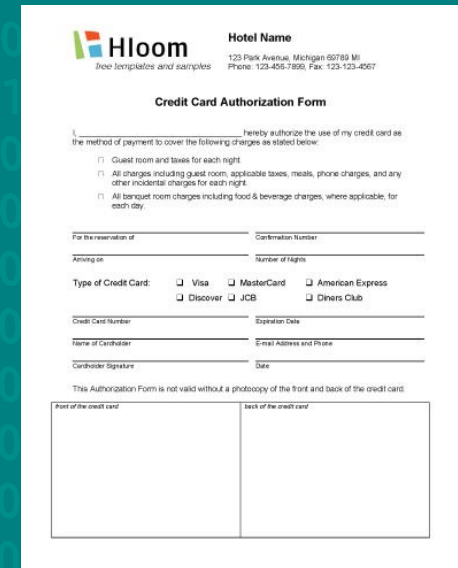
- Esistono keylogger anche per smartphone dotati di sistemi operativi come Android o iOS.
- I programmi possono essere inseriti fra il browser e il WWW e sono grado di intercettare informazioni provenienti da qualsiasi periferica di input ( tastiera, mouse, microfono)





# KEYLOGGER SOFTWARE: TECNICHE

- Form grabbing: malware memorizza informazioni inserite in un form di una pagina web. Le informazioni vengono memorizzate prima che siano inviate dal browser.



**Hloom** Hotel Name  
123 Park Avenue, Michigan 62789 MI  
Phone: 123-456-7890, Fax: 123-123-4567

**Credit Card Authorization Form**

I, \_\_\_\_\_, hereby authorize the use of my credit card as the method of payment to cover the following charges as stated below:

- Guest room and taxes for each night
- All charges including guest room, applicable taxes, meals, phone charges, and any other incidental charges for each night.
- All banquet room charges including food & beverage charges, where applicable, for each day.

For the reservation of \_\_\_\_\_ Confirmation Number: \_\_\_\_\_  
Arriving on \_\_\_\_\_ Number of nights: \_\_\_\_\_

Type of Credit Card:  Visa  MasterCard  American Express  
 Discover  JCB  Diners Club

Credit Card Number: \_\_\_\_\_ Expiration Date: \_\_\_\_\_  
Name of Cardholder: \_\_\_\_\_ Email Address and Phone: \_\_\_\_\_  
Cardholder Signature: \_\_\_\_\_ Date: \_\_\_\_\_

This Authorization Form is not valid without a photocopy of the front and back of the credit card.

front of the credit card	back of the credit card
--------------------------	-------------------------



# KEYLOGGER SOFTWARE: TECNICHE

- **Memory injection**: sfrutta le vulnerabilità di un browser. Le tabelle di memoria associate sono modificate in modo da bypassare i sistemi di controllo utente.
- **Sniffing di rete**: catturare i pacchetti in transito in una rete. L'uso di connessioni HTTPS esclude il problema.

# CONTROMISURE

- **Antikeylogger**: software di protezione creato per rilevare keylogger software. Spesso è in grado di bloccare l'esecuzione del programma spia, non fa distinzione tra keylogger legittimi e malware.



# CONTROMISURE

Tastiera USB : tastiera con interfaccia USB elimina il rischio di un keylogger hardware sul computer.



