PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 24 - numero 5101 di Lunedì 14 febbraio 2022

La manipolazione delle serrature elettroniche

Non solo i lettori, ma anche i criminali sono al corrente di numerose tecniche di manipolazione delle serrature meccaniche. Ma quali tecniche sono applicabili alla manipolazione di serrature elettroniche?

Il comitato tecnico europeo, che sta lavorando all'aggiornamento delle norme sulle serrature di alta sicurezza (HSL), ha recentemente messo a punto una bozza aggiornata, nella quale vengono classificate le varie tecniche di manipolazione, applicabili alle serrature elettroniche. Ecco una panoramica.

La cattura del codice attraverso il cavo di connessione

Come i lettori sanno, il codice di apertura di una serratura elettronica viene digitato su una unità di comando e controllo ed inviato, attraverso un cavo di connessione, all'elaboratore centrale della serratura elettronica. Se il malvivente riesce a raggiungere questo cavo, ha la possibilità di catturare i codici in transito.

La cattura del codice attraverso un keylogger

Con questo nome si fa riferimento ad un dispositivo elettronico, che può catturare i dati, che vengono digitati sulla tastiera di comando e controllo della serratura elettronica.

L'immissione del codice attraverso il cavo di connessione

L'attacco avviene in due tempi, inizialmente catturando il codice appropriato e successivamente inserendolo sul cavo di connessione tra la tastiera e l'unità di comando e controllo.

L'attacco esaustivo

Con questo nome si fa riferimento un tipo di attacco, che prevede la digitazione successiva di tutti i numeri possibili, fino a individuare il codice appropriato.

Attacco attraverso un canale laterale

Si tratta di una tecnica in continua evoluzione, che prevede che l'attaccante possa avere accesso a qualsiasi cavo esistente, che si connetta alle batterie, alla tastiera, all'unità di comando e controllo ed al dispositivo meccanico azionato dai circuiti elettronici.

L'alimentazione parallela

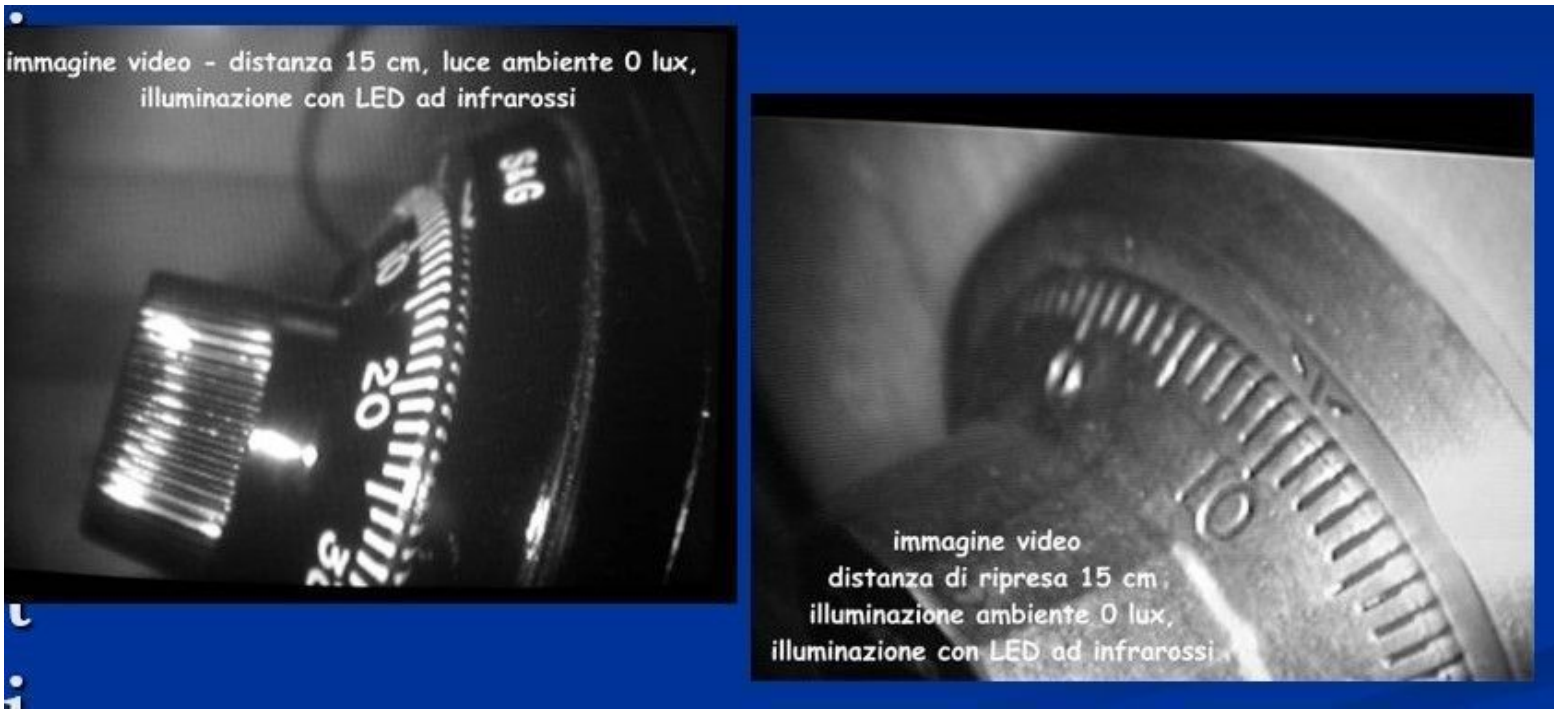
Con questa tecnica di attacco il malvivente utilizza un alimentatore, separato da quello incorporato nella serratura, alimentando direttamente il dispositivo meccanico attivato dai circuiti elettronici.

Il bypass meccanico

Se la serratura non è correttamente progettata ed installata, il malvivente può avere la possibilità di azionare meccanicamente il dispositivo di blocco. In una serratura meccanica a scrocco questo attacco, ad esempio, si perpetra utilizzando una carta di credito, fatta scivolare fra l'anta e il telaio, in corrispondenza del catenaccio.

La cattura ottica dei codici

L'istallazione di minuscole telecamere, installate in posizione defilata ed appropriata, può permettere ai malviventi di catturare la sequenza dei codici, che vengono digitati sulla tastiera. È questa una tecnica più volte utilizzata anche per la cattura dei codici delle serrature meccaniche.



Nella maggior parte dei casi, l'utilizzo di appropriati algoritmi criptografici rende molto difficile la perpetrazione degli attacchi sopra illustrati, ma l'esperienza di parecchi secoli ci insegna che alla lunga, i malviventi sanno essere più abili dei migliori progettisti!

Adalberto Biasiotti

www.puntosicuro.it