PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 28 - numero 5994 di Lunedì 12 gennaio 2026

Le serrature intelligenti sono molto attraenti, ma...

Negli ultimi tempi si stanno diffondendo sempre di più le serrature intelligenti, comandate ad esempio da telefoni cellulari. Come sempre, l'evoluzione tecnologica va confrontata con quella dei possibili rischi, di cui offriamo un elenco.

Il comitato tecnico CEN/TC 263/WG 3, che si occupa di serrature di sicurezza, ha recentemente elaborato un documento, che mette in evidenza quali siano i rischi legati all'utilizzo di serrature, ad esempio comandate da smartphone.

Poiché l'attrattiva della soluzione fa sì che aumentino sempre più gli utenti, che si orientano su questa soluzione, è bene che gli esperti di sicurezza informatica e di serrature siano messi a conoscenza dei rischi legati a queste particolari tecnologie.

Le tecnologie di attacco si possono suddividere in quattro famiglie:

- tecnologie di attacco legate alle comunicazioni,
- tecnologie legate ai sistemi operativi di smartphone,
- tecnologie legate ad acque specifiche, ed infine
- tecnologie legate alla cattura di informazioni riservate.

Analizziamo insieme queste quattro famiglie di tecnologie di attacco.

Evidentemente le tecniche di attacco legate alla comunicazione fra la serratura e lo smartphone possono comportare la manipolazione della comunicazione senza fili tra lo smartphone e la serratura, che permette di catturare dati fondamentali per poter duplicare i messaggi di apertura della serratura.

Per quanto riguarda la seconda categoria di metodi di attacco, è ben noto che il caricamento di Troian e il ricorso ad attacchi, che siano in grado di catturare l'archivio delle chiavi, presente sullo smartphone, non sono certamente una novità.

Gli attacchi legati invece ad applicazioni particolari si articolano in varie forme, che vanno dal phishing, alla violazione dell'applicativo criptografico, se non è sufficientemente sicuro, ad attacchi legati alla cattura dei messaggi scambiati fra lo smartphone della serratura, nell'arco di un certo periodo di tempo, per avere a disposizione elementi in grado di violare la

cifratura del messaggio e produrre un duplicato funzionante.

Infine, non dimentichiamo che lo scambio di informazioni tra lo smartphone e la serratura intelligente può portare alla individuazione della posizione della serratura, nonché all'identificazione del tipo di serratura e delle modalità di azionamento. Con questi elementi potrebbe, ad esempio, essere possibile per un malvivente sapere quando l'utente sta per azionare la serratura e procedere quindi ad una imboscata, in danno dell'utente.

Diciamo che la situazione non è molto diverso da quando per la prima volta vennero prodotte in serie le rivoltelle: erano utili per difendere i buoni, ma potevano essere pericolose in mano ai cattivi!

Adalberto Biasiotti

www.puntosicuro.it