ARTICOLO DI PUNTOSICURO

Anno 20 - numero 4297 di Mercoledì 29 agosto 2018

Che patacca di lucchetto!

Certamente difficile presentarsi sul mercato con un prodotto veramente innovativo, e le difficoltà crescono se il prodotto, che sembra davvero innovativo, si rivela un'autentica patacca.

Poco tempo fa sui principali mezzi di comunicazione di massa, che pubblicizzano mezzi di difesa avanzati, è apparsa una campagna pubblicitaria massiccia, che metteva in evidenza i pregi di un nuovo tipo di lucchetto. Questo lucchetto, battezzato come lucchetto intelligente, funziona riconoscendo l'impronta digitale del proprietario.

La azienda che ha lanciato sul mercato questo prodotto a raccolto contributi per più di 300.000 $ per poter avviare la produzione di serie di questo lucchetto inviolabile. Il problema è nato quando tutti coloro che avevano investito in questa azienda cominciarono a preoccuparsi, perché la campagna pubblicitaria si era arrestata e la azienda non dava risposta a messaggi di richieste di chiarimenti, che giungevano da tutti sostenitori.

Dopo qualche mese di silenzio, questa azienda Startup rassicurò tutti gli investitori sul fatto che il ritardo era dovuto ad alcuni problemi produttivi dello stabilimento cinese.

Finalmente, nella seconda metà di quest'anno, il prodotto è apparso sul mercato ad un prezzo di 100 $, assai attraente, almeno in relazione alle caratteristiche funzionali di questo lucchetto.

Il principio di funzionamento è molto semplice: il proprietario del lucchetto invia, tramite una app, un messaggio codificato ad un lettore, situato nel corpo del lucchetto. Da quel momento in avanti, il lucchetto si aprirà solo dopo che il lettore avrà ricevuto il codice appropriato inviato dallo smartphone del padrone.

Appena gli specialisti hanno avuto in mano qualche esemplare di questo lucchetto, hanno cominciato a vivisezionarlo.

Tanto per cominciare, i materiali in cui è realizzato il lucchetto sono a base di una lega di zinco e alluminio. Questa lega è ormai famosissima sotto il nome di zamak. Il problema nasce dal fatto che questa lega è sì abbastanza robusta, ma è estremamente fragile e quindi un colpo secco sul corpo del lucchetto fa sì che si sbricioli in 1000 pezzi.

Il secondo problema che è stato messo in evidenza riguarda il sistema Bluetooth, che permette di bloccare e sbloccare il lucchetto. Un esperto informatico ha messo meno di un'ora per aprire il lucchetto.

Come è stato possibile questo attacco?

Bene: apparentemente il lucchetto trasmette il suo codice MAC attraverso un collegamento bluetooth e usa lo stesso indirizzo MAC per calcolare la chiave usata per bloccare e sbloccare l'apparato.

La struttura poco sicura dell'indirizzo MAC ha fatto sì che l'esperto fosse in grado di violare l'algoritmo in poco tempo, aprendo senza nessuna difficoltà qualunque lucchetto. Da buon professionista, questo specialista ha informato subito il fabbricante, dandogli sette giorni per rettificare l'errore, prima che egli rendesse pubblica questa debolezza strutturale.

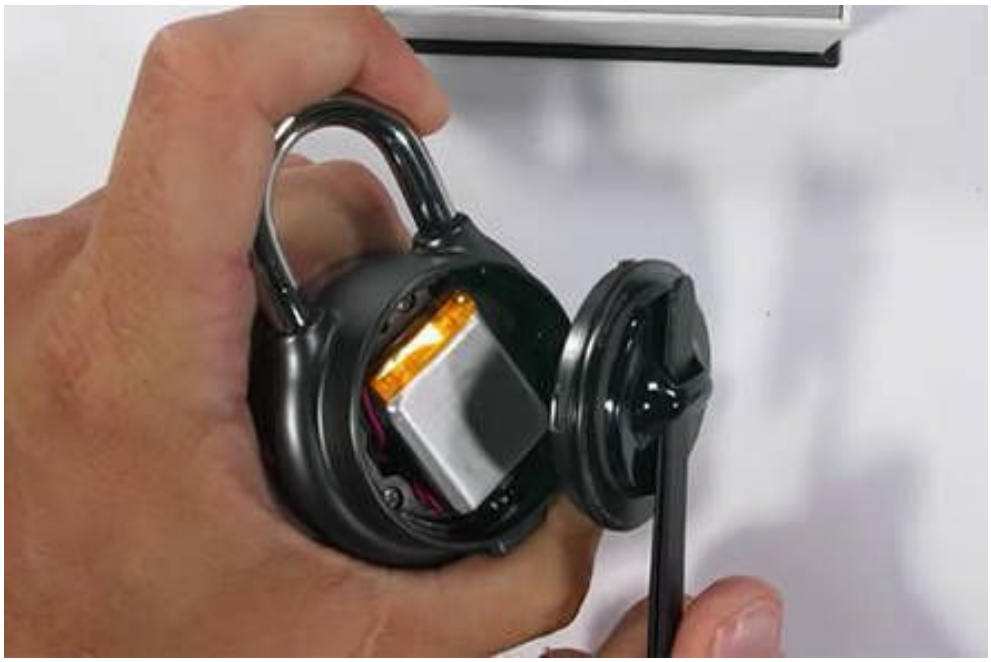
Il fabbricante ha reagito tempestivamente, ma ha messo in crisi tutti coloro che l'avevano acquistato, perché essi dovevano recarsi presso un punto di assistenza autorizzato per l'aggiornamento del firmware.

Infine, è entrato in azione un serraturiere, che capiva poco o nulla di informatica.

Egli ha preso un cacciavite ed è riuscito in un attimo ad aprire il fondello posteriore del lucchetto, sbloccando il gancio dall'interno.

Davanti a una tale clamorosa vulnerabilità del lucchetto, egli si è sentito in dovere di informare immediatamente il fabbricante. La candida risposta del fabbricante fu che l'operazione che egli aveva effettuato non avrebbe dovuto essere possibile, in quanto una spinetta del diametro di mezzo millimetro avrebbe dovuto bloccare il fondello al corpo del lucchetto!

Ancora una volta, purtroppo non è tutto oro quel che luccica, ma è una lega di zama con numerosi difetti meccanici ed informatici collegati.



Adalberto Biasiotti