Falla negli antifurti “smart” per automobili. Rubarle è un gioco da ragazzi

Mar 11, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Le vulnerabilità permettono di trovare l’auto, disabilitare l’antifurto, aprirla e rubarla. Ma anche di spiare i proprietari a distanza…

La febbre delle funzionalità “smart” non accenna a diminuire e i danni che provoca nemmeno. A pagare dazio per il desiderio di avere uno strumento controllabile attraverso lo smartphone, a questo giro, sono i proprietari di automobili che hanno avuto la brillante idea di installare antifurti “intelligenti” sulle loro vetture.

I problemi riguardano i sistemi antifurto (in particolare quelli di **Pandora** e **Viper**) che utilizzano delle applicazioni per smartphone allo scopo di localizzare e controllare l’auto. Come spiegano ricercatori di **Pen Test Partners** in un report, le app in questione hanno una serie di falle di sicurezza che mettono a rischio le macchine stesse.

Le vulnerabilità, nel dettaglio, risiedono nelle **API** utilizzate dagli sviluppatori, che consentono di modificare l’indirizzo collegato all’email attraverso un collegamento senza autenticazione.

A questo punto, un pirata informatico può chiedere **un reset della password al nuovo indirizzo e, di conseguenza, “rubare” l’account del proprietario**.

Le conseguenze sono facili da comprendere: grazie all’antifurto “intelligente”, il pirata può fare qualsiasi cosa. **Localizzare l’auto, aprirla, accenderla**. Eventualmente, un criminale potrebbe anche forzare o spegnimento del motore mentre il legittimo proprietario la sta guidando.

La funzione, in teoria, è pensata per bloccare un veicolo che è stato rubato, ma **nelle mani di un criminale può diventare uno strumento per rapinare o addirittura rapire il proprietario del veicolo**.

Nel caso degli antifurti Pandora, è anche possibile spiare le vittime attraverso un microfono che normalmente viene utilizzato per inviare messaggi di aiuto, ma che attraverso l’app è possibile utilizzare come microfono spia.

Secondo i ricercatori, le app permetterebbero di comunicare anche con il **CAN (Controller Area Network)** e, di conseguenza, consentirebbero di eseguire veri e propri sabotaggi, modificando la velocità del veicolo o forzando l'attivazione dei freni. Nel report, spiegano però di non aver ancora approfondito questo aspetto.

I veicoli coinvolti sarebbero 3 milioni e **il problema sarebbe stato risolto a tempo di record dai produttori**, ai quali Pen Test Partners aveva dato sette giorni di tempo prima di rendere pubblica la notizia delle vulnerabilità.

Tutta la vicenda, però, evidenzia ancora una volta quanto sia rischioso affidare il controllo (o anche solo la sorveglianza) dei veicoli a sistemi software che troppo spesso soffrono di

bug e falle di sicurezza macroscopiche. Questa volta è andata bene… la prossima?

Please follow and like us:

Kaspersky Lab scende nel dettaglio della loro Global Transparency Initiative

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/03/11/falla-negli-antifurti-smart-per-automobili-rubarle-e-un-gioco-da-ragazzi/