PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 20 - numero 4169 di Lunedì 05 febbraio 2018

Continuano i problemi di applicativi di larga diffusione

I lettori certamente sono informati sui numerosi buchi che vengono gradualmente scoperti su applicativi e sistemi operativi di larga diffusione. Uno, che è stato poco pubblicizzato, ma potenzialmente assai pericoloso, riguarda i servizi GPS e GSM.

Oggi sono sempre più diffusi degli apparati che permettono di abbinare un ricevitore GPS ad un apparato GSM, il tutto accorpato in dispositivi di piccolissime dimensioni.

A parte i tracciatori che vengono utilizzati sia dalle forze dell'ordine, sia dalle compagnie di assicurazione, sia dagli investigatori, per tenere sotto controllo il movimento delle vetture, molti altri dispositivi del genere sono utilizzati per una moltitudine di applicazioni.

In un'applicazione di safety, ad esempio, questi dispositivi permettono di tenere sotto controllo il movimento di un tecnico di manutenzione, che si muove all'interno di qualche complesso industriale o del terziario, in modo da sapere con certezza dove il soggetto in questione si trova. Il dispositivo spesso è dotato di un pulsante aggiuntivo, che permette di lanciare una richiesta di soccorso, in caso di necessità.

Ho visto recentemente un tale dispositivo realizzato in versione, per così dire, francobollo, che può essere utilizzato come portachiavi e permette di sapere in ogni momento, grazie ad un'apposita applicazione scaricabile su un smartphone, dove si trova il mazzo di chiavi.

Orbene, è stato recentemente rilevato che una gran numero di questi servizi on-line, che utilizzano quindi sistemi di tracciamento basati su un ricevitore GPS ed un trasmettitore GSM, presenta una serie di vulnerabilità, che potrebbe consentire agli attaccanti di catturare tutti i dati che vengono trasmessi ed anche catturare lo storico dei movimenti del proprietario del dispositivo.

Due ricercatori del mondo della sicurezza hanno messo in evidenza, alla fine di dicembre, queste vulnerabilità, che hanno battezzato con il suggestivo nome di "Trackmageddon". I servizi esaminati sono più di 103 e complessivamente essi gestiscono milioni di apparati portatili. La gran parte di questi dispositivi è vulnerabile perché utilizza un sistema operativo di base, sviluppato da una azienda indiana.

Solo quattro aziende, alla data del 2 gennaio 2018, hanno confermato di avere già messo sotto controllo queste debolezze, mentre altre aziende stanno ancora esaminando la faccenda.

Per quanto riguarda il mondo della security, ricordo che questi dispositivi sono utilizzati in lucchetti intelligenti, che sono in grado di trasmettere a distanza la posizione GPS del lucchetto stesso, nonché informazioni relative all'eventuale apertura o

chiusura del lucchetto stesso.

Altri dispositivi di questo tipo sono installati su automezzi che trasportano valori o che sono messi a disposizione di persone a rischio, che possono utilizzarli per aumentare il livello della propria protezione contro possibili attacchi di rapinatori e rapitori.

Ancora più preoccupante è il fatto che, in alcune applicazioni, gli attaccanti possono persino scaricare le immagini e registrazioni audio che sono catturate da questi dispositivi, e trasmesse a distanza, insieme alle informazioni di posizione.

I ricercatori hanno quindi lanciato una allerta a tutti coloro che utilizzano questi dispositivi, raccomandando loro di prendere contatto con le aziende che gestiscono i segnali emessi da questi dispositivi, per sapere se hanno già provveduto a installare aggiornamenti del software, che possono mettere sotto controllo questa vulnerabilità. In attesa della ricezione di conferma dell'aggiornamento del software, i ricercatori raccomandano di spegnere il dispositivo ed attendere ulteriori istruzioni.

Particolarmente preoccupante è il fatto che gli attaccanti potrebbero ricostruire la sequenza dei movimenti fatti da un determinato soggetto, cercando di individuare gli elementi ripetitivi, che potrebbero favorire un attacco criminoso, diretto al soggetto in questione.

Questa segnalazione, che presento ai lettori, si inquadra però in un quadro ben più generale, che riguarda il livello di sicurezza degli innumerevoli dispositivi chiamati con l'acronimo IoT-Internet of Things. Nella grande maggioranza dei casi, chi ha sviluppato questi dispositivi si è preoccupato della funzionalità e assai poco della sicurezza della comunicazione.

Purtroppo ancora oggi le aziende, che sono sufficientemente sensibili da investire adeguate risorse non solo nella funzionalità, ma anche nella sicurezza dei dispositivi che vendono, rappresentano una quota minoritaria del mercato.

Adalberto Biasiotti

---

www.puntosicuro.it