PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 21 - numero 4438 di Lunedì 01 aprile 2019

Un cavo USB diventa un temibile strumento di intercettazione

Un informatico americano ha dato notizia di un cavo USB, opportunamente modificato, che si trasforma in un temibile strumento non solo di intercettazione, ma perfino di sostituzione dell'operatore al computer.

I lettori hanno già avuto notizia di dispositivi che possono essere inseriti fra una tastiera ed un computer, in grado di trasmettere ad un utente remoto, tramite un collegamento Wi-Fi, tutti i dati che vengono digitati sulla tastiera. Uno studioso americano ha recentemente mostrato un nuovo strumento di attacco, ancora più letale.

In questo caso il cavetto USB è modificato, con l'inserimento di un piccolo computer ed un collegamento Wi-Fi.

Quando il cavetto viene collegato al personal computer, esso viene interpretato dal sistema operativo come una interfaccia di operatore. Ciò significa che, grazie al collegamento Wi-Fi, un attaccante può impersonare, a tutti gli effetti, l'operatore legittimo, digitando istruzioni, che vengono recepite dal computer, in quanto provenienti da un utente supposto legittimo.

È così possibile all'attaccante, posto a distanza, impartire istruzioni al computer e manipolare il mouse. In un'intervista con il tecnico, che ha sviluppato questo dispositivo, un video mostra con chiarezza come è sufficiente inserire questo apparato nel collegamento USB di un computer, per assumere l'intero controllo del computer. In altre parole, il cavo viene interpretato dal computer con una tastiera e come un mouse, con tutte le conseguenze che si possono immaginare.

Ad esempio, è possibile impedire che il computer vada in pausa, dopo un certo periodo di inattività, rendendo quindi possibile a soggetti terzi di avvicinarsi al computer, magari lasciato temporaneamente inattivo, ed operare direttamente sulla tastiera.

Anche se esistono dispositivi che permettono di bloccare questo impersonamento, chiamato normalmente con l'acronimo HIB - human interface device, utilizzando dei dispositivi che impediscono la trasmissione di dati fra il computer e la tastiera, il dispositivo può egualmente essere usato per attacchi che tendono a modificare i parametri di autentica.

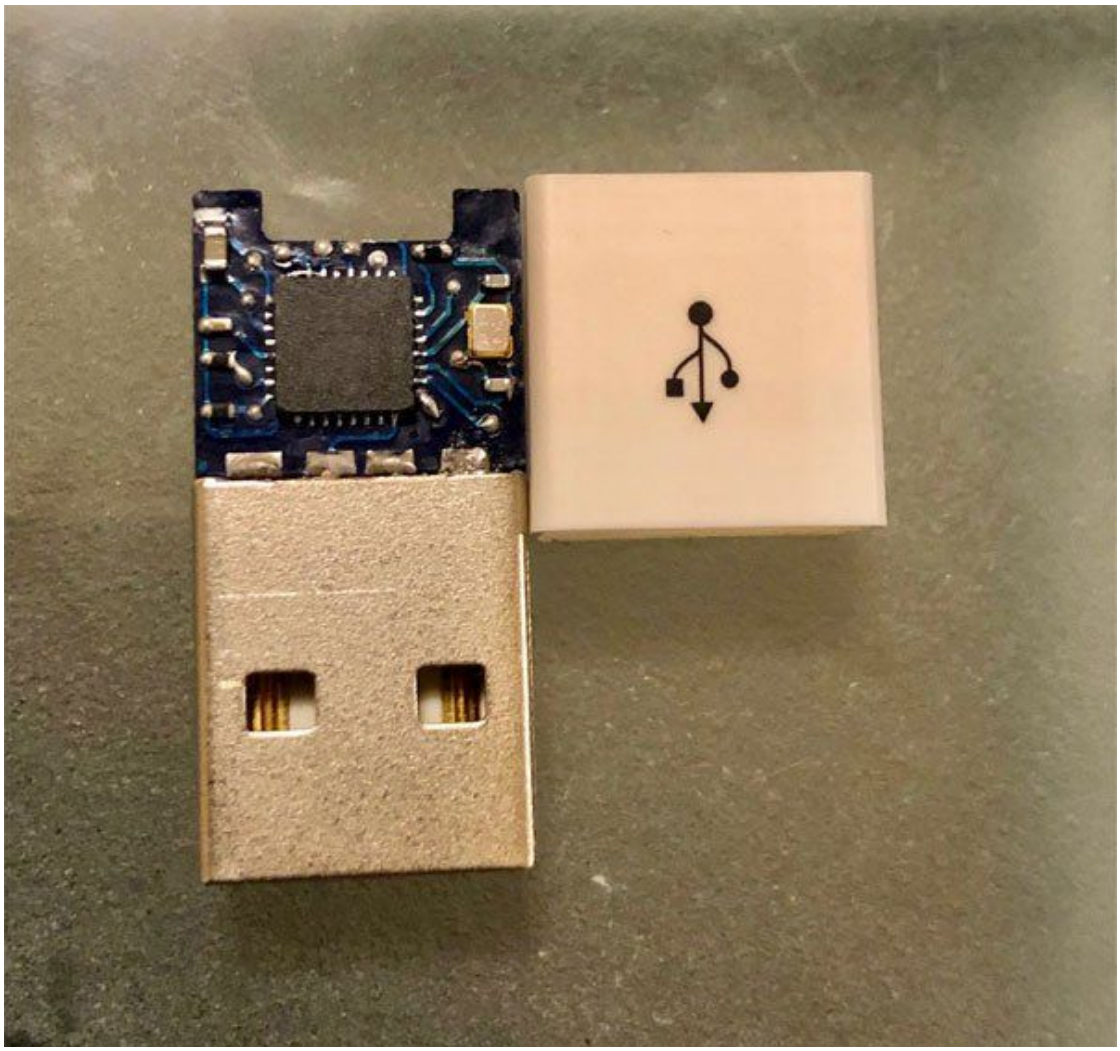
Utilizzando questo cavo, è evidentemente possibile portare l'attacco anche all'interno di un'area ad accesso strettamente controllato. Solo se l'area è dotata di protezioni elettromagnetiche, a livello tempest, il livello di schermatura potrebbe essere sufficiente a bloccare la trasmissione Wi-Fi all'esterno.

L'inventore ha dichiarato di aver speso circa 4000 ? e alcune diecine di giorni di ricerca per sviluppare questo circuito un installarlo sul connettore.

Al momento, il dispositivo non è in vendita, ma alcuni acquirenti si sono già fatti avanti.

I lettori sono avvertiti!

Segue fotografia del cavo USB con il circuito elettronico messo a punto dal ricercatore.



Adalberto Biasiotti

www.puntosicuro.it