Polizia di Stato

Bluetooth

Lo scopo principale della nascita della tecnologia bluetooth risiede nella capacità di far **dialogare e interagire fra loro dispositivi diversi** (telefoni, stampanti, notebook, computer palmari, etc) senza la necessità di collegamenti via cavo. In un sistema bluetooth la trasmissione avviene principalmente via radiofrequenza.

La tecnologia Bluetooth può essere fonte di virus. A conferma ci sono test condotti da importanti aziende del settore che hanno individuato oltre 1300 dispositivi Bluetooth potenzialmente attaccabili da malware.

La Polizia di Stato mette a disposizione un breve vademecum di suggerimenti per aiutare gli utenti a non cadere nelle trappole tese con detta tecnologia:

- attenzione a scaricare applicazioni da Internet o nuovi software con il vostro cellulare o computer palmare dotato di tecnologia Bluetooth: prima di procedere all'installazione di nuovi software o scaricare nuove applicazioni da Internet, verificare sempre l'affidabilità della fonte.
- Prestare attenzione a eventuali anomalie nel funzionamento del proprio dispositivo: premesso che senza un'applicazione di sicurezza installata è piuttosto difficile rintracciare un virus, ci sono però delle situazioni che possono mettere l'utente in allarme. In linea di massima, infatti, i virus tipicamente causano anomalie sul telefono, come ad esempio l'aumento di attività di comunicazione, un consumo insolito della batteria, la ricezione di messaggi non richiesti, la cancellazione di icone o la modifica delle stesse.
- Ricordarsi di disattivare Bluetooth dopo averlo utilizzato e se ciò non è possibile almeno impostare il dispositivo con connessione in modalità "nascosta". Questa precauzione garantisce almeno un livello minimo di sicurezza poiché allunga i tempi di un'eventuale aggressione.
- Modificare il nome identificativo del cellulare: molti utenti tendono a mantenere il nome identificativo del proprio cellulare impostato di default dal costruttore, normalmente associato al modello specifico dell'apparecchio. Questa semplice informazione può consentire a un aggressore di associare a un apparato delle vulnerabilità note, che possono quindi essere sfruttate.
- Aggiornare sempre eventuali software di sicurezza e antivirus: per poter contrastare con efficacia degli attacchi, tutti i software di sicurezza devono sempre essere aggiornati. Un software di sicurezza non aggiornato è inutile, in quanto la computer insecurity è in continua evoluzione e un software vecchio non è progettato per affrontare nuove problematiche. È importante sottolineare che "vecchio" può indicare anche solo un mese di vita, dal momento che gli aggiornamenti dei software antivirus si svolgono su base settimanale.
- Attenzione alla scelta dei codici PIN per associare i dispositivi: troppo spesso vengono mantenuti i codici forniti dal produttore o, peggio ancora, vengono usate informazioni a cui un aggressore può facilmente risalire (ad esempio la propria data di nascita)".

06/08/2013