Attacchi Bluetooth. Esperimento milanese per smascherare i cellulari rimasti abilitati, quindi possibili veicoli di virus.
In 24 ore, 1400 apparecchi sono risultati positivi al test
(Corriere Economia, luglio 2006)

Di solito una valigia viene usata per trasportare vestiti ed effetti personali. Se però è un trolley con rotelle, può servire per altri scopi. Ad esempio essere equipaggiata al suo interno con sofisticate apparecchiature elettroniche. In grado di scoprire la vulnerabilità dei cellulari verso virus e attacchi hacker. Ed è proprio questo l'esperimento condotto a Milano, per la prima volta in Italia, da F-Secure. Un'azienda finlandese specializzata in sicurezza informatica. Obiettivo? Testare sul campo la sicurezza dei collegamenti Bluetooth. Quelli che ci consentono di scambiare informazioni con computer e altri dispositivi mobili. Con una sola avvertenza. Non tutti sanno che una volta attivato il collegamento, l'utente rimane "visibile" anche a eventuali malintenzionati. Che, nel raggio di 50-100 metri, possono catturare le informazioni in memoria. I cyberfurti più frequenti riguardano i dati dell'agenda personale, i nominativi della rubrica telefonica. Ma anche fotografie scattate con smartphone, compilation musicali e contenuti multimediali.

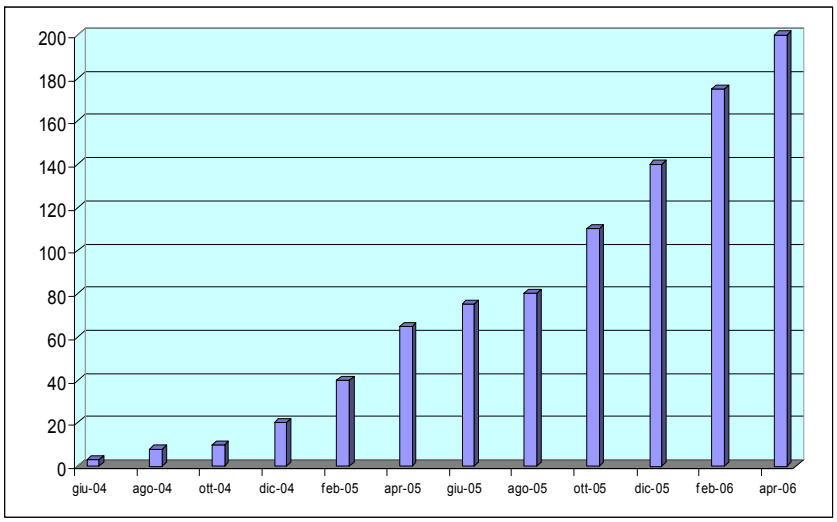
Lo dimostra quanto accaduto a Milano tra febbraio e marzo di quest'anno, ma reso noto solo in questi giorni. Un team di ricercatori di Secure Network, per effettuare i rilevamenti senza destare sospetti, ha nascosto la strumentazione elettronica in un innocuo trolley. "BlueBag", così l'hanno chiamato. All'interno, un sistema telematico capace di identificare dispositivi Bluetooth, attivi nel raggio di 150 metri. Un laboratorio di ricerca viaggiante, che ha consentito di condurre i test senza dare nell'occhio. In momenti e luoghi diversi. Dislocati in aree milanesi ad alta densità telefonica. Nella zona di FieraMilanoCity durante Infosecurity 2006, alla stazione metropolitana Cadorna, al centro direzionale di Assago, alla stazione Centrale e aeroporto di Malpensa. Senza tralasciare il Politecnico di Milano, denso di popolazione studentesca. Itinerari scelti per verificare la presenza di dispositivi vulnerabili.

Nel corso dell'esperimento si è deciso di concentrarsi sull'identificazione di apparecchi con Bluetooth "al lavoro". Considerata dagli esperti la condizione a rischio per diventare prede inconsapevoli di cybercriminali. I risultati? Nei 7 giorni dell'esperimento, per un totale di 24 ore non consecutive, sono stati identificati 1400 dispositivi mobili con Bluetooth in modalità "visibile". Cellulari e smartphone, notebook e computer palmari. Ma anche navigatori satellitari e alcune stampanti. «Il risultato rivela una duplice chiave di lettura - spiega Miska Repo, responsabile di F-Secure Italia -da un lato sottolinea la diffusione capillare della tecnologia Bluetooth nella realtà quotidiana, dall'altro porta a una considerazione preoccupante. Potenzialmente un malintenzionato aveva a disposizione

un numero sufficiente di cellulari per veicolare un'infezione. Che si poteva diffondere a catena, creando un'epidemia verso altri apparecchi visibili».

Insomma un effetto domino dovuto al fatto che Bluetooth, per sua natura, è un valido sistema per passare informazioni con il metodo peer to peer (ndr. punto a punto).

Ma fino a che punto bisogna preoccuparsi per possibili infezioni da virus sui cellulari? Teniamo conto che il primo, apparso nel febbraio 2004 con nome in codice Redbrowser, sottraeva denaro alla carta prepagata con finti collegamenti a servizi Wap. Pochi mesi dopo, nell'estate 2004, venne dimostrata la possibilità di intercettare il segnale Bluetooth dall'undicesimo piano di un albergo di Las Vegas, catturando le rubriche personali di 300 ignari passanti. Unico strumento usato un'antenna direzionale collegata a un semplice computer portatile. Ebbene in meno di 2 anni sono stati rilevati dai laboratori di F-Secure 200 virus per telefonini.



«Tuttavia fino a oggi quelli in circolazione non hanno causato danni rilevanti o epidemie diffuse - spiega ancora Miska Repo – in futuro però prevediamo un aumento di attacchi mirati a mettere fuori gioco i singoli apparecchi. Una delle tecniche più usate è quella di creare connessioni verso numeri a pagamento. Per generare guadagni illeciti per gli autori, e azzerare le schede prepagate». Dunque le intrusioni che fino a oggi interessavano i computer, minacciano adesso il mondo wireless. Con analoghe azioni di spamming e phishing, messe in atto via Bluetooth o Sms. «Però la minaccia più preoccupante rimane quella legata alla privacy dell'utente – conclude il responsabile di F-Secure - il telefono cellulare rappresenta infatti una preziosa fonte di dati personali inseriti in rubrica, agenda e nei messaggi». Informazioni che possono essere cancellate, modificate e rubate, attraverso singoli attacchi peer to peer.

E per difendersi? Quando non usate Bluetooth, ricordate sempre di disabilitarne l'accesso. Rendendolo invisibile. Specie nei luoghi pubblici. Senza creare inutili allarmismi, è importante capire come piccoli accorgimenti come quello di impostare la connessione Bluetooth del proprio cellulare in modalità nascosta anziché visibile possano contribuire ad aumentare il livello di sicurezza del proprio dispositivo, scoraggiando possibili attacchi da parte di aggressori più o meno pericolosi.

# # #