

Allarme virus Esperimento finlandese a Milano: in 24 ore, scovati 1.400 apparecchi mobili leggibili dai truffatori

Il bottino dei pirati?

La rubrica del cellulare

Con il Bluetooth, dati personali a rischio hacker. Come evitarlo

DI UMBERTO TORELLI

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, può essere equipaggiata all'interno con sofisticate apparecchiature elettroniche, in grado di scoprire la vulnerabilità dei cellulari verso virus e attacchi hacker. È proprio questo l'esperimento che è stato condotto a Milano, per la prima volta in Italia, da **F-Secure**, azienda finlandese specializzata in sicurezza informatica, fondata da Risto Siilasmaa.

L'obiettivo era testare sul campo la sicurezza dei collegamenti Bluetooth, quelli che ci consentono di scambiare informazioni con il Pc e altri dispositivi mobili, come il computer-navigatore di bordo delle automobili, il palmare e anche le stampanti. Collegamenti comodi: ma rischiosi. Una volta attivato il collegamento, infatti, l'utente rimane «visibile» anche ai pirati dell'hi-tech: che, nel raggio di 50-100 metri, possono catturare le informazioni in memoria. I cyberfurti più frequenti riguardano i dati dell'agenda personale, i nomi della rubrica telefonica. Ma vengono rubate anche fotografie scattate con smartphone, compilation musicali e contenuti multimediali.

Lo dimostra l'esperimento milanese, condotto tra febbraio e marzo ma reso noto soltanto 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 (l'hanno chiamato «BlueBag»). All'interno, c'era un sistema telematico capace

di identificare dispositivi Bluetooth, attivi nel raggio di 150 metri. Un laboratorio di ricerca viaggiante, insomma, che ha consentito di condurre i test senza dare nell'occhio, in momenti e luoghi diversi. I trolley-spia sono stati dislocati in aree milanesi ad alta densità telefonica: nella zona di FieraMilanoCity, durante «Infosecurity 2006»; alla stazione metropolitana di Cadorna; al centro direzionale di Assago; alla stazione Centrale; all'aeroporto di Malpensa; e al Politecnico di Milano, denso di popolazione studentesca. Gli itinerari sono stati 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»: è questa, infatti, la condizione considerata a rischio dagli esperti perché l'utente diventi preda di cybercriminali. I risultati? Nei sette giorni dell'esperimento, per un totale di 24 ore non consecutive, sono stati identificati 1.400 dispositivi mobili con Bluetooth in modalità «visibile»: cellulari e smartphone, notebook e computer palmari, ma anche navigatori satellitari e alcune stampanti.

«Il risultato si presta a una doppia chiave di lettura — dice Miska Repo, responsabile di **F-Secure** Italia —. Da un lato, sottolinea la diffusione capillare della tecnologia Bluetooth nella realtà quotidiana. Dall'altro invece porta a una considerazione preoccupante: potenzialmente, un malintenzionato aveva a disposizione un numero sufficiente di cellulari per veicolare un'infezione. Potevano essere attaccati in meno di 24 ore e l'infezione si sarebbe diffusa a catena, creando un'epidemia verso altri apparecchi visibili». In-

somma, un «effetto domino» dovuto al fatto che Bluetooth, per sua natura, è un valido sistema per passare informazioni con il metodo *peer to peer* (punto a punto, il collegamento diretto da un utente all'altro).

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 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.

«Fino a oggi, i virus 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 — dice il responsabile di F-Secure —. Il telefono

cellulare rappresenta infatti una preziosa fonte di dati personali inseriti in rubrica, agenda e nei messaggi». Tutte informazioni che possono essere cancellate, modificate e rubate, attraverso singoli attacchi *peer to peer*.

Come ci si difende? Quando non usate Bluetooth, ricordate sempre di disabilitarne l'accesso: rendendolo invisibile, specie nei luoghi pubblici. Per aumentare la sicurezza bastano piccoli accorgimenti: come impostare la connessione Bluetooth del proprio cellulare in modalità nascosta anziché visibile. Questo scoraggerà possibili attacchi.

L'epidemia

Evoluzione del virus nei telefoni cellulari



Il primo virus su cellulare, nome in codice Redbrowser, è comparso nel febbraio 2004.

Tentava di sottrarre denaro alla carta prepagata con finti collegamenti a servizi Wap



Dall'aprile 2004 all'aprile 2006 il numero di virus è cresciuto da tre a duecento

Fonte: elaborazione di CorriereEconomia su dati F-Secure



Spy Risto Siilasmaa, fondatore di **F-Secure**: «trolley-spia» piazzati a Milano per scoprire la vulnerabilità dei cellulari