

L'indagine, in varie zone di Milano, è durata un giorno intero e ha rilevato oltre 1.400 tra cellulari e smartphone attaccabili

I rischi del telefonino bluetooth Come gli 007 contro virus e worm

di AGNESE ANANASSO

UN'INDAGINE con metodi da 007 per smascherare i possibili attacchi a telefoni cellulari e smartphone attraverso bluetooth, uno dei protocolli più diffusi di comunicazione senza fili. L'idea di questa "prova sul campo" - e la sua attuazione a Milano - è merito dei ricercatori di F-Secure e Secure Network, due aziende specializzate in soluzioni e servizi di sicurezza informatica.



Un'indagine diretta che ha prodotto dati tutt'altro che rassicuranti per gli utenti.

Il necessario per questo esperimento era racchiuso in un semplice trolley da viaggio di medie dimensioni, che è stato chiamato "BlueBag". Al suo interno è stato piazzato un sistema di rilevamento in grado di identificare dispositivi bluetooth presenti nel raggio di 150 metri. Insomma, un vero e proprio laboratorio di ricerca viaggiante che ha consentito di condurre il test senza dare nell'occhio, anche nelle zone più affollate. L'obiettivo non era stabilire la percentuale di utenti "distratti" rispetto al totale dei possessori di cellulari, ma semplicemente di valutare i danni potenziali che un aggressore - o anche un ignaro utente infettato - potrebbe provocare.

FieraMilanoCity (durante Infosecurity 2006), centro commerciale Orio Center, stazione metropolitana Cadorna, centro direzionale Assago MilanoFiori, stazione centrale di Milano, aeroporto di Malpensa, Politecnico di Milano (sede Leonardo): queste le zone prescelte, molto diverse tra loro proprio per verificare se e come variasse la presenza di dispositivi mobili potenzialmente vulnerabili, che, a loro volta, possono essere causa del diffondersi dell'epidemia.

L'esperimento è stato volutamente concentrato cellulari o smartphone (e nella rete è finito anche qualche computer) con bluetooth attivo e in modalità visibile, nella condizione quindi di essere più vulnerabili. L'indagine è durata circa 24 ore (per l'esattezza 22 ore 58 minuti), "spalmata" su 7 giorni scelti tra febbraio e marzo. Sono stati ben 1405 i dispositivi con bluetooth attivo e in modalità visibile, tra cellulari e smartphone (1312), PC/notebook (39), palmari (21), navigatori satellitari (15), stampanti (5) e altri dispositivi (13).

Da notare come sia proprio il cellulare lo strumento prediletto per la tecnologia bluetooth e di conseguenza anche meno sicuro: nel quadro che ha delineato questa indagine, un programmatore di virus avrebbe avuto potenzialmente a disposizione oltre 1300 tra cellulari e smartphone in meno di 24 ore. Tutti da infettare, tutti egualmente indifesi e a loro volta possibili propagatori di virus.

E' interessante notare che 313 telefonini identificati dalla "BlueBag" avevano attivo il servizio OBEX Push, normalmente presente su tutti i cellulari e smartphone e usato per il trasferimento di informazioni (ad esempio biglietti da visita) o di file e applicazioni. Un servizio che, proprio perché consente il trasferimento di file, rischia di essere un pericoloso canale di propagazione di virus e worm.



La "BlueBag" è stata utilizzata in modalità "honeypot", ovvero un sistema messo a punto per essere usato come "esca" per proteggersi da attacchi informatici. Per esca si intende la possibilità di ricevere informazioni sugli attacchi, la loro frequenza e tipologia. Una "honeypot" non contiene mai informazioni reali ma simula una situazione reale in modo da attirare i pirati informatici. Rimane infatti visibile nell'ambiente e in ascolto, pronta a ricevere qualsiasi richiesta di connessione effettuata da dispositivi infetti catalizzandoli su di sé. Lo scopo? Scoprire e "catturare" quei worm che girano nei valigie dispositivo e provare a smascherare i suoi autori.

(8 giugno 2006)

Siti sponsorizzati *Un servizio Yahoo! Search Marketing*

Nuova soluzione assicurativa Risparmia il 50% sui costi annuali dell'auto con Easy Driver.

Ric...www.easydriver.com

Assicurazione auto Zuritel Polizza auto Zuritel: il risparmio di un'assicurazione online

con...www.zuritel.it

Sponsorizza il tuo sito

Visita anche:

gastronomia, anima gemella, finanziamenti, biglietti aerei