# A SPASSO CON BLUETOOTH
# IN TUTTA SICUREZZA

**F-Secure, in collaborazione con Secure Network,**
**ha realizzato il primo test *on the road* condotto in Italia**
**per verificare il livello di vulnerabilità della tecnologia Bluetooth**
**ormai disponibile su numerosi dispositivi,**
**compresi i cellulari "smart" di ultima generazione**

**Maggio 2006**

# Perché questo esperimento

Bluetooth è una parola ormai entrata nell'uso comune, il cui significato letterale pare risalire al nome del re vichingo Harald Bluetooth (Blåtand in scandinavo), che visse agli inizi del 900 e unì i regni di Danimarca, Norvegia e Svezia. **Il protocollo Bluetooth nasce infatti con l'obiettivo di unificare le varie tecnologie di trasmissione senza fili dei dati tra dispositivi elettronici sia mobili sia fissi** come PC, cellulari, notebook, palmari, DVD, lettori MP3, TV, Hi-Fi, registratori di cassa, terminali POS e persino elettrodomestici come frigoriferi e lavatrici. È in pratica **la nuova alternativa agli infrarossi** e si basa su una tecnologia radio a onde corte in grado di trasmettere dati oltrepassando anche ostacoli fisici come muri o altri oggetti.

Bluetooth è destinato a divenire una tecnologia pervasiva per supportare comunicazioni senza fili in vari contesti d'uso nella vita di tutti i giorni. Allo stato attuale, il maggior livello di diffusione si ha nei cellulari di ultima generazione e nei cosiddetti smartphone, apparecchi che, oltre a offrire tutte le funzionalità di telefonia più all'avanguardia, racchiudono funzioni e applicazioni caratteristiche di un computer palmare, gestite da un sistema operativo, come Symbian o Microsoft Windows Mobile. Gli smartphone permettono di inviare e ricevere SMS, MMS ed e-mail, ascoltare file mp3, guardare filmati, navigare in Internet, giocare, gestire l'agenda, sincronizzare i dati del telefono con quelli del proprio PC e molto altro. In taluni casi, possono diventare anche navigatori GPS, attraverso un ricevitore satellitare e un software specifico.

Quello degli smartphone per il momento **è ancora un mercato di nicchia, che cresce però a un tasso del 100% annuo da ormai 5 anni**, limitato per il momento da fattori quali prezzo elevato o, in taluni casi, dimensioni e peso. **Ma proprio il 2006 potrebbe essere l'anno della svolta**: secondo la società di ricerche di mercato ABI Research, **quest'anno gli smartphone conquisteranno il 15% del mercato globale dei telefoni cellulari**, pari a 123 milioni di unità vendute, grazie alla crescente richiesta di applicazioni quali mobile email (secondo Gartner, nel 2006 sarà usata da 20 milioni di persone), ai prezzi in calo (grazie alla crescita dei volumi), alle più ampie possibilità di scelta tra diversi modelli. Secondo le stime di Gartner, nella sola Europa, il tasso di crescita nelle vendite di cellulari intelligenti sarà del 49% annuo tra il 2005 e il 2009 e **tra 5 anni, 1 cellulare venduto su 3 sarà "smart"**.

Ecco perché **F-Secure** – società finlandese prima a rendere disponibile una tecnologia antivirus per la protezione dei telefoni cellulari – ha deciso di commissionare la realizzazione del primo esperimento *on the road* italiano mirato a verificare le potenziali vulnerabilità dei dispositivi dotati di Bluetooth oltre che la realizzazione di una mini-guida alla comprensione della tecnologia Bluetooth contenente anche indicazioni sulle precauzioni minime per utilizzarla in tutta sicurezza. **Conoscere le vulnerabilità dei dispositivi con tecnologia Bluetooth, infatti, è tanto importante quanto capirne le potenzialità a livello della tecnologia stessa**: da parte nostra, con questo lavoro, intendiamo fare un primo importante passo in questa direzione.

Per questa prima verifica sul campo, si è deciso di concentrarsi su Milano e dintorni. In parallelo, un esperimento analogo è stato condotto direttamente da F-Secure in occasione dell'ultimo CeBIT, la fiera dell'informatica e delle telecomunicazioni che si è svolta ad Hannover tra il 9 e il 15 marzo scorsi. Per tutta la durata della manifestazione, i tecnici di F-Secure hanno attivato all'interno del loro stand un sistema di rilevamento simile a quello messo a punto dagli esperti di Secure Network per i rilievi condotti a Milano e dintorni, in grado di individuare dispositivi Bluetooth attivi presenti nel raggio di 100 metri. I risultati sono stati impressionanti: nell'arco della settimana, sono stati rilevati ben 12.500 dispositivi che utilizzavano Bluetooth, lo avevano abilitato e lo avevano in modalità visibile. Scoprite nelle pagine seguenti quali sono stati i risultati delle prove condotte a Milano e dintorni!

Miska Repo
*Country Manager di F-Secure Italia*

# Introduzione

Il *mobile computing* sta rapidamente assumendo un ruolo importante nella nostra esperienza quotidiana; per questo motivo è fondamentale rendersi conto degli eventuali rischi legati all'utilizzo di qualsiasi dispositivo basato sulla tecnologia wireless.

Se solo tre anni fa soltanto gli esperti di virologia iniziavano a parlare timidamente di virus per telefoni cellulari, oggi vulnerabilità come ad esempio BlueBug e BlueBump dei dispositivi basati su tecnologia Bluetooth stanno portando alla luce nuove problematiche che non possono essere sottovalutate.

**Gli smartphone**, grazie alle funzionalità avanzate che li caratterizzano, **si avvicinano ormai a dei veri e propri personal computer: per questo, sono contemporaneamente più vulnerabili, più preziosi e target più interessanti per potenziali attacchi.** Questa maggio vulnerabilità nasce proprio dalla presenza sul dispositivo di un sistema e di applicazioni evolute di connettività che espongono il telefono e i dati in esso contenuti a una serie di rischi derivanti da attività quali l'invio di messaggi email, il trasferimento di dati via Internet, lo scambio di messaggi MMS e WAP nonché l'utilizzo di accessori e strumenti quali ad esempio le memory card. In particolare, le comunicazioni che avvengono attraverso connessioni Bluetooth diventano potenziali veicoli di virus, nonché bersaglio di insidiosi attacchi che possono estrarre informazioni dallo smartphone.

I virus per cellulari diffusi fino ad oggi non hanno per fortuna causato danni significativi agli utenti, al di là di ovvi disagi dovuti a malfunzionamenti del telefono. Tuttavia la situazione non va sottovalutata, perché vi sono tutti i presupposti perché questa minaccia continui a crescere di pericolosità.

Per il futuro, ci si può aspettare un aumento degli attacchi volti a rendere il dispositivo mobile inutilizzabile, ma anche di quelli destinati ad effettuare, ad esempio, connessioni verso numeri a pagamento in grado di generare guadagni illeciti per gli autori, nonché di nuove minacce tese ad esempio a realizzare azioni di spamming via SMS o MMS. La minaccia forse più preoccupante rimane comunque quella legata alla privacy dell'utente: il telefono cellulare rappresenta infatti una preziosa fonte di dati personali con la rubrica, i messaggi, l'agenda e molto altro. Informazioni, queste, che possono essere cancellate, modificate o rubate, anche al di fuori di un'epidemia virale, utilizzando attacchi ormai ben noti ed in continua evoluzione.

Poche persone oggi sono consapevoli dei rischi in cui possono incorrere a causa di un utilizzo superficiale di dispositivi apparentemente innocui: lo dimostra il fatto che **in poche ore di "appostamenti", abbiamo rilevato migliaia di dispositivi con tecnologia Bluetooth in modalità *visibile* e quindi potenziali target per attacchi.**

Ma non ci siamo limitati a rilevare i dispositivi potenzialmente vulnerabili: insieme a F-Secure, infatti, abbiamo messo a punto una guida aggiornata sulle possibili minacce alla sicurezza e una serie di suggerimenti agli utenti sulle precauzioni – comportamentali e tecniche – che possono adottare affinché questa tecnologia sempre più diffusa non si trasformi nell'ennesimo motivo di preoccupazione.

Stefano Zanero,
*CTO di Secure Network S.r.l.*

Luca Carettoni,
*Senior Consultant di Secure Network S.r.l.*

Claudio Merloni,
*Senior Consultant di Secure Network S.r.l.*

# Come funziona la tecnologia Bluetooth

La tecnologia Bluetooth consente di effettuare connessioni senza fili fra dispositivi elettronici (computer desktop e notebook, cellulari, palmari, video camere, ecc.. utilizzando onde radio alla **frequenza di 2,4 GHz** (la stessa usata dalla tecnologia Wi-fi 802.11), mettendo in comunicazione tra loro dispositivi coperti dal segnale. Le frequenze utilizzate variano da paese a paese, in relazione alle normative nazionali.

Nel momento in cui un utente connette tra loro diversi dispositivo basati su Bluetooth, crea intorno a sé ciò che viene chiamata **PAN** (Personal Area Network), ovvero una piccola rete con la possibilità di scambiare dati e informazioni come normalmente avviene in una comune LAN (Local Area Network) aziendale.

La tecnologia Bluetooth è caratterizzata da una **bassa potenza** (da 1 a 100 mW, mille volte inferiore alla potenza di trasferimento di un cellulare GSM) e da una **velocità di comunicazione** che si aggira intorno a **1 Mbps**.

In relazione alla potenza, i dispositivi Bluetooth vengono distinti in classi, a ciascuna delle quali corrisponde una relativa portata di ricezione:
- *Classe 1* – in grado di comunicare con dispositivi Bluetooth inclusi in un raggio fino a 100 m
- *Classe 2* – in grado di comunicare con Bluetooth inclusi in un raggio fino a 10 m
- *Classe 3* – in grado di comunicare con Bluetooth solo se si trovano al di sotto dei 10 m

Attualmente la maggior parte dei dispositivi di uso comune appartiene alle Classi 2 e 3: ad esempio notebook e telefoni cellulari utilizzano normalmente la tecnologia di comunicazione Bluetooth di Classe 2.

Verso la fine del 2004 sono state effettuate implementazioni della tecnologia Bluetooth che nelle nuove versioni può consentire velocità di trasferimento anche di 2 e 3 Mbps oltre che un minor consumo energetico. La cosa importante, però, è che i cellulari possono comunque dialogare tra loro anche se implementano versioni del protocollo Bluetooth differenti, più o meno recenti.

## Tecnologia Bluetooth e sicurezza: quali i rischi?

Le prime falle di sicurezza relativamente a questa tecnologia vennero scoperte nel novembre 2003: alcune implementazioni del protocollo Bluetooth, infatti, sembravano consentire l'accesso a dati e informazioni personali da parte di estranei non autorizzati.

Nell'aprile 2004 cominciò poi a circolare la notizia relativa alla possibilità di forzare alcune delle implementazioni di Bluetooth per poi accedere a una serie di dati personali: il tutto analizzando i dispositivi Bluetooth e recuperando il codice utilizzato per cifrare la trasmissione dei dati.

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 rubriche di 300 cellulari di ignari passanti nella strada sottostante con il solo ausilio di un'antenna direzionale collegata a un portatile: una scoperta che ha esteso in modo significativo il raggio di azione di un potenziale aggressore.

Una serie di debolezze, quindi, che hanno portato a riflettere da vicino sull'esistenza di un problema che, anche in considerazione della rapida diffusione della tecnologia Bluetooth, non può più essere sottovalutato.

Se prendiamo in considerazione i telefoni cellulari di nuova generazione, **possiamo identificare 4 tipologie di minacce a cui questi dispositivi possono essere soggetti**:

1. contenuti dannosi quali virus, worm o trojan horse, che possono essere trasmessi sui terminali dell'utente tramite Bluetooth, SMS o MMS, oppure tramite pagine WAP. Sfruttando delle vulnerabilità (ad esempio tramite attacchi al protocollo Bluetooth, o tramite particolari SMS o MMS "malformati") tali applicazioni possono anche essere installate sul device;

2. episodi di *denial of service* o interruzione del sistema, causati dalla propagazione di malware, o da altri tipi di attacchi;

3. accesso non autorizzato alle informazioni sfruttando trojan horse, spyware, attacchi di eavesdropping...

4. cancellazione, corruzione o modifica dei dati contenuti sul dispositivo

Ciò significa che, a parte la propagazione di malware e virus, ad un utente ignaro e totalmente inconsapevole dell'attacco a cui il suo dispositivo è soggetto, **potrebbero essere sottratte la rubrica e l'agenda dal telefono** con relativi contatti, numeri telefonici e appuntamenti a calendario. Sempre che l'aggressore non vada oltre, prendendo il controllo del dispositivo e effettuando chiamate o mandando messaggi a carico della vittima.

Tra gli attacchi esistenti a danno dei dispositivi con tecnologia Bluetooth - classificati dagli esperti di sicurezza di tutto il mondo – ve ne sono alcuni particolarmente conosciuti e diffusi:

- **BlueSnarf** – Questo tipo di attacco sfrutta il servizio OBEX Push, ovvero quel tipo di servizio comunemente usato per scambiarsi i bigliettini da visita elettronici. Facilmente attuabile nel caso in cui un cellulare abbia impostato Bluetooth in modalità visibile, il BlueSnarf consente di collegarsi a un cellulare e accedere a rubrica e agenda: il tutto senza ovviamente alcuna autorizzazione.

- **Bluejacking** – Sfruttando i nomi identificativi che due dispositivi si scambiano all'inizio di una connessione – si pensi a quando associamo il nostro telefono a un computer – potrebbero essere trasmessi brevi testi ingannevoli. Un utente potrebbe ad esempio essere invitato a digitare un codice per risolvere problemi alla rete e, inconsapevolmente, autorizzerebbe un aggressore ad acquistare tutti i privilegi necessari per accedere a rubrica, agenda e file ed eventualmente compromettere informazioni e dati residenti sul dispositivo.

- **BlueBug** – Questa vulnerabilità consente di accedere ai *Comandi AT* del telefono cellulare – set di comandi che impartiscono istruzioni al cellulare - consentendo all'aggressore di sfruttando a insaputa dell'utente tutti i servizi telefonici: dalle chiamate in uscita e in entrata agli SMS spediti, ricevuti o cancellati, oltre a molte altre operazioni intrusive inclusa la possibilità di modificare dei parametri di configurazione del dispositivo.

- **BlueBump** – Un tipo di attacco che sfrutta la vulnerabilità legata al tipo di collegamento Bluetooth che rimane attivo dando la possibilità ai cellulari non più autorizzati di continuare ad accedere come se fossero ancora inclusi nell'elenco dei dispositivi con accesso consentito.

Questo tipo di attacco, oltre a portare al furto dei dati presenti sul cellulare, può portare gli aggressori a sfruttare i servizi WAP e Gprs senza che il proprietario ne sia consapevole.

## Bluetooth e worm: come avviene concretamente la propagazione di virus tra telefoni cellulari?

Le modalità di propagazione dei virus sono molteplici nonché destinate a variare e ad automatizzarsi sempre più e **spesso sfruttano tecniche di *social engineering***: il malcapitato, trovandosi sul telefonino un messaggio "attraente" con accluso invito a scaricare un allegato o installare un programma, non esita a procedere con l'operazione, infettando il proprio dispositivo e dando il via alla propagazione del worm.

Esempi eclatanti di questa tecnica di attacco li abbiamo visti con **Cabir**, uno dei primi virus per cellulari ad aver conquistato le pagine della cronaca nell'estate del 2004, nonché primo caso di virus a replicarsi per semplice vicinanza tra cellulari con collegamento Bluetooth attivo.

Un altro caso ad aver suscitato clamore è stata l'identificazione di **Commwarrior**, un virus dal comportamento curioso dal momento che dalle 8 a mezzanotte si diffondeva sfruttando le connessioni Bluetooth mentre da mezzanotte alle 7 di mattina si "dedicava" agli MMS. E se si pensa che l'invio di MMS ha un certo costo, è facile capire l'impatto economico che questo tipo di virus ha avuto per chi ne è stato vittima!!

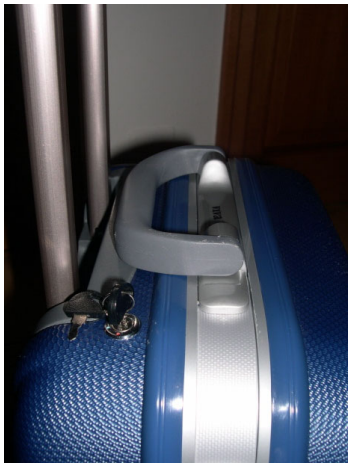

Un'altra modalità di propagazione può avvenire attraverso l'invio di messaggi infetti, aprendo connessioni TCP/IP direttamente dalle applicazioni e offrendo così ai malware ulteriori possibilità di diffondersi.

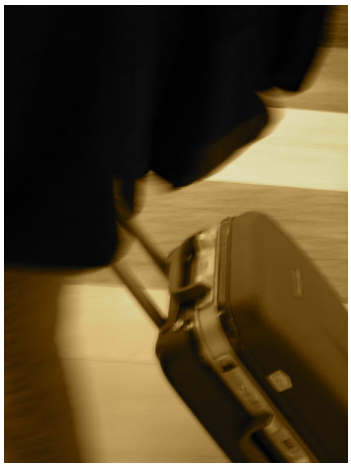
Dall'estate 2004 ad oggi, i casi di epidemie di virus che hanno interessato dispositivi mobili identificati in tutto il mondo sono andati aumentando, utilizzando svariate tecniche: **si pensi che a fine maggio 2006 i laboratori di ricerca di F-Secure avevano classificato oltre 200 virus esistenti**!! Un elenco che si allunga giorno per giorno e che si può vedere, puntualmente aggiornato, al link *http://www.f-secure.com/wireless/threats/*

# A spasso con la *Blue*Bag a Milano e dintorni

Nello svolgimento del nostro esperimento, ci siamo concentrati sull'identificazione del numero di dispositivi con **Bluetooth - attivo - in modalità visibile.** E' questa infatti la condizione di maggiore rischio potenziale per gli utenti. Teoricamente sono possibili attacchi anche a dispositivi che abbiano impostato Bluetooth in modalità nascosta, ma sono più complicati da realizzare.[1] Per questo motivo, il nostro test si è concentrato esclusivamente sul rilevamento dei dispositivi in modalità visibile, che sono quelli più facilmente attaccabili. Il nostro intento non era quello di stabilire la percentuale di utenti "distratti" rispetto al totale dei possessori di telefoni cellulari, ma semplicemente di valutare i danni potenziali che un aggressore – o anche un ignaro utente infettato – potrebbe fare.

Per effettuare i rilevamenti senza "dare nell'occhio", il team di ricercatori di Secure Network ha messo a punto quella che abbiamo battezzato "***Blue*Bag"**, ovvero un vero e proprio **laboratorio di ricerca viaggiante *travestito* da trolley**!





Apparentemente una valigia qualunque, la BlueBag conteneva al suo interno un sistema di rilevamento in grado di identificare dispositivi Bluetooth presenti nel raggio di 150 metri.

---

[1] *Un attacco brute-force per scoprire eventuali cellulari con la tecnologia Bluetooth abilitata ma in modalità "nascosta" NON è attuabile in contesti generici dato l'enorme dispendio di tempo che richiederebbe. Un attacco con queste modalità risulta possibile soltanto qualora si voglia colpire uno specifico dispositivo e anche in questo caso è necessario prima scoprire marca ed eventuale modello del dispositivo e poi avere la possibilità di eseguire l'attacco per un periodo di tempo piuttosto lungo (es: tramite contatto visivo si scopre marca e modello di cellulare e poi, durante le ore lavorative, in cui il soggetto lascia il dispositivo sulla scrivania, si esegue l'attacco). Dalle considerazioni precedenti, appare evidente quindi come la modalità "nascosta" sia una soluzione preventiva che assicura una certa sicurezza poiché allunga considerevolmente i tempi di un'eventuale aggressione. Attraverso questa modalità si è inoltre al sicuro da eventuali infezioni dovute a worm che utilizzano la tecnologia Bluetooth per replicarsi poiché spesso la ricerca dei dispositivi vittima avviene attraverso una semplice scansione degli apparecchi presenti in zona.*

## I luoghi dove sono stati effettuati i rilevamenti

Si è deciso di condurre i rilevamenti in momenti e punti diversi – tutti ad alto passaggio - dislocati in più aree di Milano e dintorni:

- ***Fiera MilanoCity*** durante ***Infosecurity 2006***
- Centro Commerciale ***Orio Center***
- Stazione Metropolitana ***MM2 Cadorna***
- Centro Direzionale ***Assago MilanoFiori***
- ***Stazione Centrale*** di Milano
- Aeroporto di ***Milano Malpensa***
- ***Politecnico di Milano***, Sede Leonardo

La scelta è stata fatta con l'obiettivo di verificare se e come variasse la presenza di dispositivi potenzialmente vulnerabili in contesti frequentati da persone diverse: alla *Stazione Centrale*, ad esempio, più alta è la presenza di un'utenza eterogenea; all'*Orio Center* di sabato ci sono molti giovani e famiglie, soggetti che potenzialmente dovrebbero essere prede più facili per i cybercriminali perché meno consapevoli dei pericoli legati alle nuove tecnologie, al contrario di come si supponeva fossero i visitatori e gli espositori della fiera *Infosecurity* dedicata alla sicurezza IT.

Più nel dettaglio, al Centro Commerciale OrioCenter si è scelto di effettuare una prima sessione in un giorno feriale per poi decidere di far seguire altre due sessioni durante un paio di sabati pomeriggio. Anche per Infosecurity 2006, che si è svolta a Milano dall'8 al 10 Febbraio, si è scelto di fare due tappe in due giorni diversi: il giorno dell'apertura e quello di chiusura.

Va inoltre precisato che, nei casi dove i rilevamenti sono stati condotti su più giorni, dispositivi Bluetooth di tipo "stanziale" (tipo PC o stampanti), sono stati inclusi nel calcolo finale una sola volta, quindi **i dati finali del test sono relativi a dispositivi unici.**

## I risultati dei rilievi *on the road*

**I dispositivi unici con Bluetooth attivo e in modalità visibile rilevati nei 7 giorni dell'esperimento sono stati in totale 1405** tra cellulari e smartphone (1312), PC/notebook (39), palmari (21), navigatori satellitari (15), stampanti (5) e altri dispositivi vari (13).

| ***Tipologia*** | ***Quantità*** |
|---|---|
| Cellulari/Smartphone | ***1312*** |
| PC/Notebook | ***39*** |
| Palmari *(senza funzionalità di telefonia)* | ***21*** |
| Navigatori Satellitari | ***15*** |
| Stampanti | ***5*** |
| Altro | ***13*** |

Il dato non **solo sottolinea la diffusione capillare della tecnologia Bluetooth nella realtà di tutti i giorni** - dagli uffici ai negozi alle nostre borse dove teniamo cellulari di ultima generazione – ma evidenzia anche che se al nostro posto ci fossero stati dei cybercriminali, anche con questi

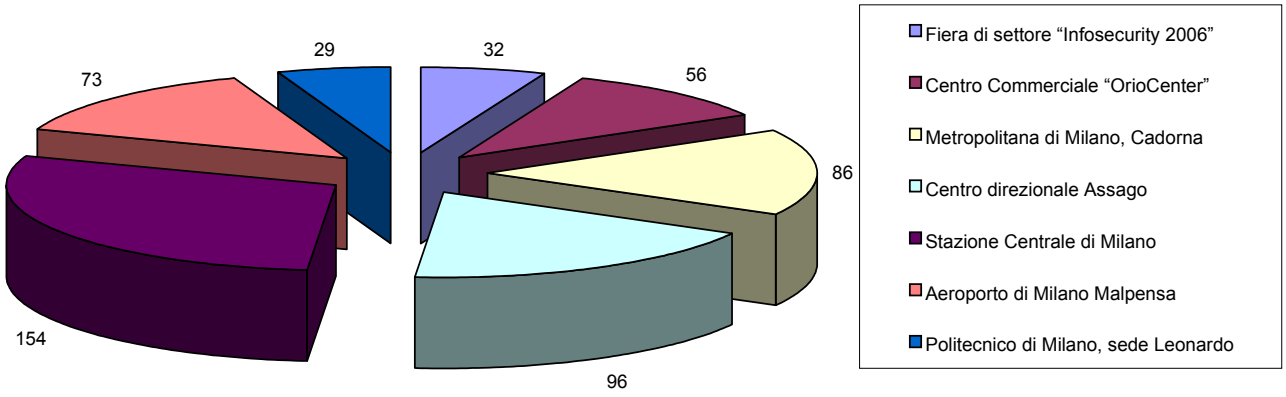
brevi appostamenti condotti con l'ausilio di un'attrezzatura "fatta in casa", avrebbero avuto a disposizione **oltre 1300 tra cellulari e smartphone Bluetooth che potevano essere attaccati in meno di 24 ore[2], che poi a loro volta avrebbero potuto andare in giro ad infettare altri cellulari non protetti…**

Nella tabella qui di seguito sono elencate le **sessioni di scansione** effettuate, riportando la data e l'intervallo di tempo durante il quale sono stati effettuati i rilevamenti.

| *Luogo* | *Sessioni di rilevamento* | *Orario della scansione* | *Durata della scansione* | *Numero di dispositivi unici rilevati* | *Media oraria di dispositivi unici rilevati* | *Numero di dispositivi rilevati ** |
|---|---|---|---|---|---|---|
| Fiera di settore "Infosecurity 2006" | 08/02 | 15:07-18:04 | 2:57 | ***94*** | ***32*** | ***94*** |
| | 10/02 | 15:01-16:46 | 1:45 | ***55*** | ***31*** | ***55*** |
| Centro Commerciale "OrioCenter" | 01/03 | 15:49-18:50 | 3:01 | ***23*** | ***8*** | ***23*** |
| Metropolitana di Milano, Cadorna | 09/03 | 08:43-09:22 | 0:39 | ***56*** | ***86*** | ***56*** |
| Centro direzionale Assago | 09/03 | 12:53-15:20 | 2:27 | ***236*** | ***96*** | ***236*** |
| Stazione Centrale di Milano | 09/03 | 15:40-16:52 | 1:12 | ***185*** | ***154*** | ***185*** |
| Centro Comm. "OrioCenter", sabato pomeriggio | 11/03 | 16:00-17:56 | 1:56 | ***212*** | ***110*** | ***216*** |
| | 11/03 | 18:20-20:08 | 1:48 | ***142*** | ***79*** | ***166*** |
| Aeroporto di Milano Malpensa | 13/03 | 09:15-10:41 | 1:26 | ***123*** | ***86*** | ***123*** |
| | 13/03 | 11:01-14:00 | 2:59 | ***198*** | ***66*** | ***219*** |
| Politecnico di Milano, sede Leonardo | 14/03 | 10:56-13:44 | 2:48 | ***81*** | ***29*** | ***82*** |
| **TOTALE** | **11** | | **22:58** | ***1405*** | | ***1455*** |

** Questo numero NON è riferito ai dispositivi unici ma consiste nel numero complessivo di dispositivi rilevati al termine di ogni sessione.*

Sulla base dei dati raccolti, è stato possibile calcolare **il numero medio dei dispositivi unici con Bluetooth attivo rilevati nell'arco di un'ora in ognuno dei luoghi esaminati:**




**Salta subito all'occhio come tutto sommato non vi siano grandi differenze in termini di consapevolezza dei rischi potenziali nei diversi ambienti e contesti in cui sono stati condotti i rilevamenti**: tanto alla Stazione Centrale o all'aeroporto di Malpensa - prevalentemente

[2] *I rilievi, globalmente, sono durati 22 ore e 58 minuti, come si può vedere dalla tabella alla pagina seguente*

affollati da un pubblico eterogeneo – quanto al Centro Direzionale di Assago, dove la maggior parte degli utenti si presume essere composta da persone che questi apparati li usano per lavoro, il numero medio di dispositivi Bluetooth potenzialmente vulnerabile rilevato nell'arco di una singola ora è risultato elevato. Dove invece la situazione è risultata decisamente migliore – e quindi maggiore la consapevolezza delle persone relativamente ai potenziali rischi per la sicurezza – è stato a Infosecurity e al Politecnico.

Sui 1405 dispositivi univoci rilevati, poi, è stata fatta **un'ulteriore analisi volta a definire quanti dispositivi avevano attivi alcuni tra i servizi a più ampia diffusione**, che sono proprio quelli maggiormente presi di mira come veicoli di trasmissione di worm (vedi tabella qui sotto)

| ***Tipologia*** | ***Numero*** |
|---|---|
| **OBEX Object Push / OBEX File Transfer**<br>*servizio che consente il trasferimento di file* | ***313*** |
| **Headset/Handfree Audio Gateway**<br>*servizio che consente di collegarsi agli auricolari Bluetooth* | ***303*** |
| **Dial-up Networking**<br>*servizio che permette di collegarsi e navigare in Internet tramite cellulare* | ***292*** |

Come si può vedere dalla tabella, su ben **313 dispositivi è risultato attivo il servizio OBEX Push,** normalmente usato per il trasferimento di informazioni (ad esempio biglietti da visita) o di file e applicazioni. In realtà, **tutti** i cellulari / smartphone (cioè **1312 dispositivi**) dispongono del servizio OBEX Push; **313** sono quelli che si sono trovati nel "raggio di azione" della BlueBag per un tempo sufficientemente lungo a consentirne il riconoscimento. Un dato comunque preoccupante se si considera che proprio questo servizio, per le sue peculiarità, **può diventare un pericoloso canale di propagazione di attacchi virus.**

Ciò ovviamente non significa che il servizio non deve essere attivato: scopo del nostro esperimento, infatti, era piuttosto quello di creare consapevolezza sui rischi legati a comportamenti talvolta superficiali. **Basterebbe infatti impostare la connessione Bluetooth del proprio dispositivo in modalità non visibile per rendere la vita di potenziali aggressori già più complicata**! Questa minima precauzione, pur non essendo abbastanza per eliminare totalmente i rischi, consente infatti di ridurre o per lo meno rendere più difficili gli attacchi.

# Considerazioni finali

Da una prima analisi dei risultati emersi nel corso dell'esperimento, emerge in primo luogo la larga diffusione dei dispositivi basati su tecnologia Bluetooth: una tecnologia che, a una prima occhiata, pare essere sempre più a portata di tutti nonché pare integrante della vita di ognuno, non solo per impieghi professionali ma anche per utilizzi di carattere personale. Una considerazione che rende ancora più importante sensibilizzare gli utenti in merito ai vantaggi ma anche ai rischi che possono celarsi dietro un uso sconsiderato di queste tecnologie del futuro.

Non va dimenticato, inoltre, che i dispositivi di ultima generazione rappresentano spesso uno strumento di lavoro di uso quotidiano per molte persone con livelli di responsabilità medio/alta all'interno della propria azienda. Ciò implica che spesso su cellulari all'ultimo grido o innovativi palmari risiedono informazioni particolarmente appetibili per eventuali aggressori alla ricerca di dati sensibili o interessati a fare dello spionaggio industriale.

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 potenziali aggressori più o meno pericolosi.

E' importante segnalare che alcuni telefoni cellulari vengono lanciati sul mercato con una configurazione che prevede che la connessione Bluetooth, se attivata, entri per default in modalità visibile: deve quindi essere l'utente a modificare manualmente l'impostazione, abilitando la modalità "nascosta". In altri casi, più opportunamente, la modalità visibile deve essere richiesta esplicitamente dall'utente, e viene in ogni caso reimpostata automaticamente ad invisibile dopo un breve periodo di tempo. Questo si rivela efficace: molti utenti, altrimenti, non effettuerebbero questa facile e rapida operazione, lasciano il proprio dispositivo visibile a tutti.

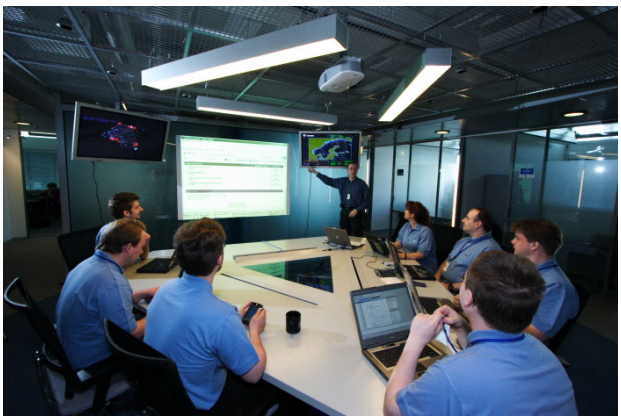
Un'altra cosa da sapere, sempre legata alle impostazioni di default dei telefoni cellulari, riguarda il nome identificativo del dispositivo stesso: nella maggior parte dei casi, infatti, la nostra indagine ha evidenziato che l'utente non si era preoccupato di modificare i parametri configurati dal produttore, consentendo così l'identificazione immediata del modello del telefono in oggetto. Un'informazione apparentemente così banale, consente però di associare eventuali vulnerabilità note ai diversi modelli di dispositivi dando così la possibilità a un potenziale aggressore di effettuare un attacco ben mirato con alte probabilità di riuscita.

Infine, una curiosità: oltre ai dati raccolti, il sistema costruito per effettuare questa ricerca potrebbe essere utilizzato con efficacia anche per "catturare" eventuali worm Bluetooth presenti nell'ambiente. La *Blue*Bag, utilizzata in modalità *honeypot*, rimane infatti visibile nell'ambiente e in ascolto, pronta a ricevere qualsiasi richiesta di connessione effettuata da dispositivi infetti. In taluni momenti della ricerca, prove di questo tipo sono state effettuate, ma non hanno fatto registrare nessun worm. Future ricerche potrebbero approfondire la reale minaccia di questo tipo di attacco, mediante sessioni appositamente pianificate con questo obiettivo.

# L’impegno di F-Secure

Sebbene ancora non esistano dei veri e propri database con l’elenco delle vulnerabilità in base ai modelli dei dispositivi, esperti di sicurezza e appassionati del settore si stanno unendo per rendere disponibili – tramite forum e siti dedicati – l’elenco delle vulnerabilità rilevate e le eventuali soluzioni per far fronte ai problemi che ne possono derivare. Un atteggiamento che contribuisce a creare consapevolezza e cultura in merito a una problematica che cresce di gravità ogni giorno che passa.

La ricerca nell’ambito della sicurezza dei telefoni cellulari richiede risorse e strumentazioni dedicate.



Un impegno che F-Secure porta invece avanti da diverso da tempo e che si è ulteriormente concretizzato a seguito del rinnovamento dei laboratori di ricerca situati presso il quartier generale di Helsinki. Fiore all’occhiello dell’azienda finlandese, il nuovo centro di ricerca rappresenta ciò che di meglio la tecnologia può offrire in termini di infrastrutture all’avanguardia per consentire alla *task force* di ricercatori F-Secure di fronteggiare nuove emergenze 24 ore su 24.

Dal giugno 2005 F-Secure ha poi scelto di implementare all’interno dei nuovi laboratori un’area appositamente strutturata per consentire lo studio e l’analisi non solo dei virus tradizionali ma anche delle nuove, emergenti minacce alla sicurezza tra le quali, appunto, i virus dei telefoni cellulari. Questo tipo di analisi, infatti, richiede innanzitutto la disponibilità di ampi spazi che consentano di studiare accuratamente le modalità di diffusione dei virus via Bluetooth, con la garanzia di un totale isolamento da frequenze radio. A questo scopo F-Secure ha predisposto all’interno del nuovo laboratorio una stanza che consente di bloccare qualsiasi tipo di segnale radio, favorendo così l’analisi di ogni possibile minaccia destinata ad attaccare l’ambiente *mobile*.

A preoccupare gli esperti di sicurezza non sono tanto gli sporadici attacchi messi a segno da teenager autori di virus in cerca di fama, quanto piuttosto il continuo emergere di vere e proprie organizzazioni criminali sempre più diffuse e incontrollabili. Un fenomeno che se finora ha preso di mira soprattutto il mondo dei PC potrebbe ripetersi anche nel mondo mobile.

Niente panico, ma solo maggiore attenzione e consapevolezza: l’avvento di nuove tecnologie non deve mettere a rischio la nostra privacy. E per potersi proteggere, è quanto mai fondamentale conoscere l’esistenza dei rischi e, soprattutto, le possibili soluzioni per evitare di cadere nelle trappole degli aggressore del mobile! **L’esperimento che F-Secure ha promosso in Italia con il supporto di Secure Network ha proprio questo scopo.**

# Qualche consiglio per non cadere in trappola

F-Secure e Secure Network, grazie alla loro ampia esperienza in materia di sicurezza informatica, hanno stilato una breve lista di consigli per non cadere vittime di potenziali attacchi da parte degli aggressore del mondo mobile. Eccola di seguito.

1. **Attenzione a scaricare applicazioni da Internet o nuovi software:** prima di procedere all'installazione di nuovi software o scaricare nuove applicazioni da Internet, verificare sempre l'affidabilità della fonte.

2. **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.

3. **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.

4. **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.

5. **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. E' 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.

6. **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).

# Come funziona l'antivirus per cellulari di F-Secure

Dopo che il software è stato installato e dopo che è stata attivata la sottoscrizione al servizio di aggiornamento, le funzionalità di scansione e di aggiornamento del database diventano automatiche e l'utente non deve più preoccuparsi di nulla.
Un buon antivirus analizza infatti automaticamente tutti i file del telefono ogni volta che sono utilizzati e - per prevenire infezioni - grazie alla funzionalità di *scanner real time* intercetta e analizza tutti i file in modo automatico non appena questi vengono salvati, copiati, scaricati o altrimenti modificati, senza richiedere nessun intervento da parte dell'utente. Tutti i virus rilevati vengono poi messi automaticamente in quarantena.

Site opened by Commwarrior.C

mobile.f-secure.com

Nei casi critici, l'aggiornamento dell'antivirus può essere inviato agli utenti tramite messaggi SMS (F-Secure Mobile AntiVirus è l'unica soluzione disponibile sul mercato che, agli utenti aziendali, consente un aggiornamento a livello incrementale attraverso messaggi SMS). Nella maggior parte dei casi, comunque, la protezione è attiva già molto tempo prima che il dispositivo possa infettarsi.

## Gli autori dell'esperimento

**F-Secure** (www.fsecure.com) è leader mondiale nel settore degli antivirus e della prevenzione delle intrusioni: secondo ricerche indipendenti, nel 2004 e nel 2005 il tempo di risposta di F-Secure alle nuove minacce è stato in maniera significativa più veloce di quello di tutti i suoi concorrenti. F-Secure protegge i pc di casa e le reti aziendali dai virus informatici e da altre minacce alla sicurezza veicolate attraverso Internet e le reti mobili. Le soluzioni offerte da F-Secure sono disponibili per workstation, gateway, server e telefoni cellulari e comprendono antivirus e desktop firewall con funzionalità di intrusion prevention, antispam e antispyware così come soluzioni per il controllo delle reti indirizzate agli IPS. Fondata nel 1988, F-Secure è quotata alla Borsa di Helsinki dal 1999 ed è una delle aziende che ha registrato la crescita più sostenuta nel settore. La società ha sede centrale a Helsinki, in Finlandia, e uffici in tutto il mondo. La protezione della tecnologia F-Secure è disponibile anche come servizio tramite ISP quali France Telecom, TeliaSonera, PCCW e Charter Communications. F-Secure è leader mondiale nella protezioni dei telefoni cellulari e ha partnership con realtà quali T-Mobile, Swisscom e Nokia. Il team dei laboratori di ricerca di F-Secure mette a disposizione uno scenario costantemente aggiornato sulla situazione di virus a livello mondiale mediante il weblog http://www.f-secure.com/weblog/

**Secure Network** (www.securenetwork.it) è specializzata in consulenza, formazione e servizi di sicurezza informatica. Il team di ricerca di Secure Network è alla frontiera dell'innovazione nelle tecniche di Ethical Hacking e nelle tecnologie di Intrusion Detection. I Penetration Test di Secure Network combinano le migliori competenze dei nostri analisti con le tecniche di analisi più all'avanguardia, garantendo non solo un servizio sempre aggiornato, ma addirittura in anticipo rispetto al mercato. Nel 2005 Secure Network ha lanciato SecureGuard, ad oggi il primo ed unico IDS con strumenti di apprendimento non supervisionato. Nel 2006 Secure Network ha introdotto il primo strumento di cifratura trasparente per tutelare la sicurezza dei disegni CAD. CryptoCAD è la risposta alla lunga attesa del mondo della progettazione, che da tempo reclamava un aiuto per difendersi dallo spionaggio industriale.Secure Network propone un'offerta di servizi di sicurezza completa, in grado di rispondere sia ai problemi dalla piccola azienda che alle esigenze della grande impresa a tutti i livelli: strategico, tattico e operativo.

# Glossario

**Antivirus** - Programma che, mediante la scansione della memoria e della memoria di massa di un computer, identifica, isola ed elimina i virus eventualmente presenti.

**Backdoor -** Meccanismo che consente di accedere a un programma attraverso l'utilizzo di privilegi normalmente noti solo all'amministratore di sistema. Il termine inglese significa letteralmente *porta di servizio*.

**Denial of Service** – Attacco mirato a impedire l'uso di una risorsa piuttosto che a prenderne possesso.

**Dropper -** Programma che installa un virus o un cavallo di Troia all'insaputa dell'utente.

**Eavesdropping –** Tentativo di intercettazione di un messaggio prima che raggiunga il destinatario (attacco di tipo "*man-in-the-middle*")

**Firme di virus** - Contengono informazioni sui virus conosciuti per poterli poi individuare su un computer quando si effettua una scansione. E' fondamentale un aggiornamento costante delle firme al fine di poter riconoscere anche i nuovi virus che vengono man mano aggiunti all'insieme delle firme.

**IMEI (International Mobile Equipment Identity)** – Numero di serie dei telefoni cellulari che identifica in modo universale il dispositivo, il modello e il costruttore.

**Malware -** Termine che indica un qualsiasi software ritenuto pericoloso per un sistema (virus, cavalli di Troia, ecc.). Il nome deriva dal termine inglese *Malicious Software*, letteralmente tradotto come software malizioso.

**Pairing –** associazione di un dispositivo cellulare a un altro

**Patch antivirus -** Programmi in grado di individuare e rimuovere dal sistema un singolo e specifico virus, solitamente messi a disposizione gratuitamente dai produttori di software antivirus per affrontare situazioni di emergenza in attesa dell'aggiornamento dei loro prodotti.

**Piconet**: piccole reti wireless costituite da due o più periferiche che condividono un canale di comunicazione utilizzando Bluetooth, fino ad un massimo di 8 dispositivi

**Quarantena -** Misura di sicurezza in base alla quale un antivirus che individua un file infetto o sospetto viene isolato in modo da essere reso innocuo per il sistema. L'isolamento può avvenire per svariati motivi: l'antivirus non è in grado di rimuovere il virus dal file, il virus è sconosciuto, il file è sospettato di contenere un virus, ecc. Generalmente l'utente ha la possibilità di vedere i file in quarantena per decidere se eliminarli definitivamente.

**Shareware** – Tipologia di distribuzione di software che dà la possibilità di copiare liberamente un programma o una versione limitata di esso per poter effettuare una valutazione per un periodo limitato.

**Smartphone** - Termine generico per indicare l'unione tra cellulare e palmare. Si tratta infatti di un telefonino con funzionalità da palmare dotato di un sistema operativo completo come Symbian OS, Smartphone 2002, Palm OS, Crossfire o Linux.

**Spamming** – Invio massiccio indiscriminato e non richiesto di grosse quantità di messaggi di posta elettronica a carattere pubblicitario e commerciale, senza alcuna preventiva richiesta da parte del destinatario.

**Spyware –** un software (in genere un worm o un trojan horse) in grado di rilevare e catturare di nascosto dagli utenti le abitudini di navigazione, la sequenza di tasti battuti sulla tastiera e perfino le password di accesso alle informazioni riservate delle aziende.

**Trojan Horse o Cavallo di Troia** – Programma che contiene al suo interno del codice atto ad eseguire funzioni nascoste che l'utente ignora. In genere, lo scopo di un *Trojan Horse* è quello di permettere un accesso, ovviamente non autorizzato, al sistema su cui viene eseguito (una *backdoor*) per poi effettuare particolari funzioni. A differenza dei virus, i Cavalli di Troia non si autoreplicano, ma vengono installati dagli utenti che ignorano il vero proposito del programma.

**Virus -** Software capace di autoreplicarsi e diffondersi tra sistemi informatici in diversi modi (in genere mediante lo scambio di software infetto), infettando altri programmi. Alcuni virus possono provocare gravi danni ai sistemi.

**Vulnerabilità -** Si intende il verificarsi di una falla di sicurezza che può consentire ad altre applicazioni di connettersi al sistema senza previa autorizzazione o senza che il destinatario ne sia a conoscenza

**WAP (Wireless Application Protocol)** - Protocollo standard di comunicazione globale fra telefoni cellulari e Internet che dà la possibilità a utenti di telefoni cellulari GSM o GPRS di accedere a contenuti Internet opportunamente predisposti per essere visualizzati nei piccoli schermi dei telefonini.

**Worm** – Programma in grado di autoreplicarsi e trasmettersi tra sistemi, spesso tramite posta elettronica o (nel caso dei cellulari) sfruttando tecnologie di interconnessione come Bluetooth. A differenza dei virus, i worm non infettano altri programmi, ma sono autonomi. Alcuni worm sono in grado di danneggiare seriamente i sistemi informatici. Il termine inglese significa letteralmente *Verme*.