

DMO**data manager on line**

>> il portale dell'ICT professionale

[< home](#) | [cerca](#)| [registrati](#) | [redazione](#) | [pubblicità](#) | [f.a.q.](#) |[Sezioni](#)**MILANO, 8 GIUGNO / ROMA, 15 GIUGNO****CLICCA QUI** per saperne di più e per registrarti.[Hot line](#)[Mappa del sito](#)**La Rivista**[Sommaro](#)[Grandangolo](#)[Cover Story](#)[Focus](#)[Dossier](#)[Primo Piano](#)[Top 2005](#)[Ceo Suite \(New!\)](#)[TechKnow\[How\]](#)**(New!)****Le rubriche**[Ricerche di](#)[mercato](#)[Off-Topic](#)[Scelti in libreria](#)[Bacheca](#)[Corsi e](#)[seminari ICT](#)**Archivio**[Best cover](#)[Link utili](#)[Strumenti](#)**Forum**

Discuti con i nostri esperti i temi caldi dell' ICT

Sezione security dedicata al mondo dello spyware e alle tecniche per combatterlo
A cura di**Esperimento Bluetooth: i nostri cellulari sono al sicuro dai cybercriminali?**

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. Pubblichiamo il Report integrale del test: la metodologia, gli esperimenti, le conclusioni.



Le comunicazioni che avvengono attraverso connessioni Bluetooth possono diventare potenziali veicoli di virus, nonché bersaglio di insidiosi attacchi che possono estrarre informazioni dallo smartphone. Il rischio è molto più che teorico, come dimostra una prova sul campo

promossa da F-Secure e condotta da Secure Network che in circa 24 ore complessive di test (nell'arco di 7 giorni) ha individuato oltre 1300 tra cellulari e smartphone Bluetooth potenzialmente indifesi rispetto a svariati attacchi, in molti casi già noti e diffusi. Il test è stato condotto in momenti e punti diversi - tutti ad alto passaggio - dislocati in più aree di Milano e dintorni: 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. Un itinerario scelto per verificare se e come variasse la presenza di dispositivi potenzialmente vulnerabili in contesti frequentati da un'utenza eterogenea e valutare quindi i possibili danni che un aggressore o un ignaro utente infettato potrebbe causare. L'esperimento è stato pensato per creare anche in Italia una

maggior attenzione e consapevolezza sui rischi e sulle potenziali vulnerabilità dei dispositivi dotati di Bluetooth. Lo studio è corredato da un vademecum redatto dagli esperti di Secure Network con l'obiettivo di suggerire le precauzioni minime per proteggersi da questa minaccia.

Pubblichiamo di seguito copia del rapporto integrale del BlueBag e una mini-guida stilata da [F-Secure](#) e Secure Network per aiutare gli utenti a proteggersi dai virus dei cellulari.

A SPASSO CON BLUETOOTH IN TUTTA SICUREZZA (a cura di [F-Secure](#))

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, 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, 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. Lo stato attuale, il maggior livello di diffusione si ha nei cellulari di ultima generazione e nei cosiddetti smartphone, apparecchi che, oltre a 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 musicali, 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, limitatamente al momento da fattori quali prezzo elevato o, in taluni casi, dimensioni. Ma proprio il 2006 potrebbe essere l'anno della svolta: secondo le previsioni di ricerche di mercato ABI Research, quest'anno gli smartphone conquisteranno il 15% del mercato globale dei telefoni cellulari, per 100 milioni di unità vendute, grazie alla crescente richiesta di applicazioni 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, solo in 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 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 capire le potenzialità a livello della tecnologia stessa: da parte nostra per questo lavoro, intendiamo fare un primo importante passo in questa direzione.

Per questa prima verifica sul campo, si è deciso di concentrarsi su alcuni 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.

Security**Umberto**

Rapetto, forte di un'esperienza pluriennale di lotta al crimine informatico, indaga gli aspetti più inquietanti della sicurezza informatica.

Management

Riflessioni sul mondo dell'ICT.

e-Law

Le attualità legislative e giurisprudenziali più rilevanti in materia di nuove tecnologie e di nuovo mercato.

A cura **dello**

Studio Legale

Antonio Martino
– **Giulio Ferruti & Associati**

Knowledge**Management**

Rubrica mensile a cura di

Marco Bianchini**WEB USABILITY**

Ingegneria dell'usabilità in Internet

Rubrica mensile a cura di

Michele Visciola**Reti e tecnologie**

Connettività e networking.

9 e il 15 marzo scorsi. Per tutta la durata della manifestazione, i te F-Secure hanno attivato all'interno del loro stand un sistema di rile simile a quello messo a punto dagli esperti di Secure Network per i condotti a Milano e dintorni, in grado di individuare dispositivi Blue attivi presenti nel raggio di 100 metri. I risultati sono stati impres: nell'arco della settimana, sono stati rilevati ben 12.500 dispositivi (utilizzavano Bluetooth, lo avevano abilitato e lo avevano in modalità 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 import: nella nostra esperienza quotidiana; per questo motivo è fondamen rendersi conto degli eventuali rischi legati all'utilizzo di qualsiasi dis basato sulla tecnologia wireless.

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

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

I virus per cellulari diffusi fino ad oggi non hanno per fortuna caus danni significativi agli utenti, al di là di ovvi disagi dovuti a malfunzionamenti del telefono. Tuttavia la situazione non va sottov perché vi sono tutti i presupposti perché questa minaccia continui crescere di pericolosità. Per il futuro, ci si può aspettare un aumen attacchi volti a rendere il dispositivo mobile inutilizzabile, ma anche destinati ad effettuare, ad esempio, connessioni verso numeri a pagamento in grado di generare guadagni illeciti per gli autori, nor nuove minacce tese ad esempio a realizzare azioni di spamming vii MMS. La minaccia forse più preoccupante rimane comunque quell: alla privacy dell'utente: il telefono cellulare rappresenta infatti una fonte di dati personali con la rubrica, i messaggi, l'agenda e molto Informazioni, queste, che possono essere cancellate, modificate o anche al di fuori di un'epidemia virale, utilizzando attacchi ormai b ed in continua evoluzione.

Poche persone oggi sono consapevoli dei rischi in cui possono incori causa di un utilizzo superficiale di dispositivi apparentemente inno dimostra il fatto che in poche ore di "appostamenti", abbiamo rilev migliaia di dispositivi con tecnologia Bluetooth in modalità visibile e potenziali target per attacchi.

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

Stefano Zanero,

CTO di Secure Network S.r.l.

Luca Caretoni,

*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 dispositivi 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 biglietti 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 sfruttare 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 BlueBag 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 "BlueBag", 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 ore², che poi a loro volta avrebbero potuto andare in giro ad infettare altri cellulari non protetti...

[Continua la lettura, scaricando il report completo a cura di F-Secure \(file Adobe Pdf, 1.013 Kb\)](#)

Spot!

IBM. Riprendi il controllo del caos informativo.

Troppe fonti e formati diversi? Riprendi il controllo. Integra e fornisci i tuoi dati aziendali con il middleware IBM Information Management: potrai cogliere nuove opportunità.

[Scopri tutti i vantaggi http://www.ibm.com/software/info/takebackcontrol/it/nonflash/index.html](http://www.ibm.com/software/info/takebackcontrol/it/nonflash/index.html)

New!

[Visita Spyware Corner, la sezione di DMO interamente dedicata a Spyware ed Adware!](#)

Versione di **prova** di Symantec **Client Security**

[Scarica **gratuitamente** la versione di prova di Symantec Client Security!](#)

[Rilasciato l'**Internet Security Threat Report 2006**](#)

[Scarica gratuitamente la versione integrale del Report sulle tendenze della sicurezza IT](#)



[Altri...](#)

[Gruppo PRO e Kaitech e i sistemi di gestione documentale e archiviazione](#)

[Pirateria italiana: continua la Campagna Microsoft](#)

[Cremona wireless: per superare il Digital Divide](#)

[Sophos Endpoint Security: il tre in uno per la sicurezza totale](#)

[Il nuovo modo per risparmiare? Fare acquisti in Rete!](#)

[L'impatto sui Sistemi informativi della Legge Sarbanes-Oxley](#)

[Per i mondiali, l'aperitivo è wireless!](#)

[La tecnologia Rfid di Symbol si imbarca con Virgin Atlantic Airways](#)

Datamanager - 20149 Milano - Via L.B. Alberti, 10 - tel. ++39 02 33101836 - fax ++39 02 33101837
email: info@datamanager.it - Copyright © 1999. Fratelli Pini Editori S.r.l. Tutti i diritti riservati -

[privacy](#)
- Powered and [hosted](#) by [SinerVis](#)