

Cerca

[Punto Informatico](#) [PI Telefonia](#) [PI Download](#) [PI Forum](#)

[HOME PI](#) > [Notizia](#)

[STAMPA](#) [SEGNALA VIA EMAIL](#)

Sommario di giovedì 8 giugno 2006

- [Calcio pirata, nessuna responsabilità per gli ISP](#)
- [Spariti i dati dell'esercito americano](#)
- [AllOfMp3.com esce dal silenzio stampa](#)
- [PQI spara un disco flash da 64 GB](#)
- [Il Computex si colora di Blu...ray](#)
- [Toshiba, 2,5 pollici con densità record](#)
- [AMD innesta la trazione integrale](#)
- [Microsoft vuole e-mail aziendali più sicure](#)
- [HP richiama le cam a rischio incendio](#)
- [F-Secure: bello Bluetooth, ma occhi aperti](#)
- [Zork diventa un'avventura telefonica](#)
- [Rosen: RIAA sbaglia. E apre al P2P](#)
- [Brin \(Google\): abbiamo tradito i nostri valori](#)
- [Editoria, fuoco incrociato su Google Book Search](#)
- [Computex, l'assedio di Greenpeace](#)
- [Siti per navigare](#)

Anno XI n. 2555 di giovedì 8 giugno 2006 ([PI Telefonia](#) - News)

## F-SECURE: BELLO BLUETOOTH, MA OCCHI APERTI

Da un test commissionato dalla celebre società di sicurezza sembra emergere che nel nostro paese le precauzioni per la sicurezza sui dispositivi Bluetooth sono pressoché ignorate

Milano - La tecnologia Bluetooth può essere foriera di virus, chi legge Punto Informatico [lo sa](#). A conferma, [F-Secure](#) pubblica ora gli esiti di un test di 24 ore condotto proprio in Italia, che ha individuato oltre 1300 dispositivi Bluetooth potenzialmente attaccabili da malware.

<b>Forum</b>
<a href="#">Scrivi nuovo</a>   <a href="#">Leggi (3)</a>
<a href="#">mica tanto..</a>

L'esperimento è stato commissionato da F-Secure a [SecureNetwork](#), i cui tecnici hanno condotto una operazione di "intelligence" nascondendo i propri strumenti in un trolley per effettuare alcuni test in aree ad alta frequentazione in Lombardia, come FieraMilanoCity, il centro commerciale Orio Center (Bergamo), la stazione Cadorna della metropolitana milanese, il centro direzionale Assago MilanoFiori, l'aeroporto di Malpensa.

Nell'indagine sono stati rilevati 1405 dispositivi unici con Bluetooth attivo e in modalità visibile, suddivisi in cellulari e smartphone (1312), PC/notebook (39), computer palmari (21), navigatori satellitari (15), stampanti (5) e altri dispositivi (13).

La società afferma che un virus writer sarebbe stato in grado di avere a propria disposizione oltre 1300 apparecchi per diffondere un'eventuale infezione in meno di 24 ore, provocando una sorta di epidemia. "Sono oltre 200 i virus per dispositivi mobili classificati a oggi dai laboratori di ricerca di F-Secure, che segnalano anche una graduale e progressiva accelerazione rispetto al 2004" riferisce Miska Repo, Country Manager di F-Secure Italia.

Un dato poco confortante, se raffrontato al numero di virus per cellulari Bluetooth rilevato fino a dicembre 2005. [Meno di sei mesi fa](#), infatti, la stessa F-Secure dichiarava di averne identificati 102. Una crescita decisamente rapida che preoccupa gli esperti.

"Una delle ragioni dell'incremento di questa tipologia di minacce - aggiunge Repo - sta nel fatto che gli smartphone costituiscono sempre più spesso uno strumento di lavoro e ciò implica che spesso vi risiedono informazioni più appetibili per eventuali aggressori alla ricerca di dati riservati da utilizzare, ad esempio, per fare dello spionaggio industriale".

Ultimato l'esperimento, F-Secure e SecureNetwork hanno compilato un breve vademecum di suggerimenti per aiutare gli utenti a non cadere nelle trappole tese dai malware writer:

Gli ultimi telefonini: ▼



LG A7150



LG F3000



Samsung SGH-i300



Nokia 6125



Sony-Ericsson W900i



Samsung SGH-D600



[Iscriviti alle newsletter di PI](#)

**Offerte Speciali** ▼

**[Il server privato virtuale da oggi è VIRTUO, da 18? mese](#)**

**[Cartucce.it - il punto di riferimento della tua stampante ...](#)** ora anche Carta fotografica, Pen Drive, Cd/dvd Vergini... e tanto altro in arrivo

**Oltre 50.000 Clienti ci hanno scelto**  
**[Mettici alla prova](#)**

www  
**aruba.it**

aruba.it: spazio web illimitato  
dominio a scelta+5 e-mail+spazio  
illimitato a solo ?20,66+iva l'anno

"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. È 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)".

Prevenire è meglio che curare. Una regola da applicare soprattutto nel mondo dell'Information & Communication Technology, dove l'utenza sembra spesso ancora impreparata di fronte a certe minacce.

*Dario Bonacina*

**Notizia seguente:** [Zork diventa un'avventura telefonica](#)  
**Notizia precedente:** [HP richiama le cam a rischio incendio](#)



Tutti i contenuti di Punto Informatico sono pubblicati secondo la [licenza di utilizzo di Creative Commons](#), salvo diverse indicazioni.

L'editore non assume alcuna responsabilità nel caso di eventuali errori contenuti negli articoli o di errori in cui fosse incorso nella loro riproduzione sul sito. Tutte le pubblicazioni su Punto Informatico avvengono senza eventuali protezioni di brevetti d'invenzione; inoltre, i nomi coperti da eventuale marchio registrato vengono utilizzati senza tenerne conto.

**RSS** [Email](#) [Info](#) [Pubblicità](#) [RSS feed](#) [Newsletter](#)

Punto Informatico è testata giornalistica registrata al Tribunale di Roma al n. 51 del 7.2.1996 - De Andreis Editore S.r.l.  
Fondato da Andrea De Andreis

Powered by  
**aconet**