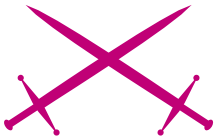

Attacco

Bluetooth Malware

Luca Carettoni

Grado di difficoltà

Anno 2007. Non passa giorno in cui non si senta l'annuncio di nuovi dispositivi che integrano connettività Bluetooth: cellulari, palmari, stampanti, macchine digitali, automobili, navigatori satellitari, ecc.

I dispositivi portatili sono sempre più paragonabili a veri e propri elaboratori, sia in termini di potenza computazionale che di capacità di memorizzazione. L'utilizzo quotidiano di dispositivi portatili è ormai una realtà nella nostra società: moltissime persone usano questi strumenti per il lavoro ed il tempo libero gestendo quindi informazioni riservate.

Vogliamo connettività tra dispositivi portatili (PAN – *Personal Area Network*), vogliamo condividere informazioni tra dispositivi eterogenei, vogliamo scambiare dati velocemente, apprezziamo soluzioni plug&play...come potrebbero non esserci rischi?

Al di là delle singole vulnerabilità del protocollo e dei bug nelle implementazioni sviluppate dai produttori di dispositivi, esiste un altro pericolo per tutti gli apparecchi con interfacce Bluetooth: i malware.

Con il termine malware, contrazione delle parole malicious e software, si identifica tutto il software creato appositamente per arrecare danno negli elaboratori su cui viene eseguito. Il codice maligno può quindi servire ad un aggressore per rubare informazioni riservate o per danneggiare completamente il sistema. Se per i tradizionali personal computer siamo abituati a convivere con il pericolo di infezione da parte di worm, virus, trojan horse, nel caso dei dispositivi portatili è una minaccia reale ancora poco considerata sebbene ritenuta dagli esperti la prossima sfida nel campo della sicurezza informatica.

L'evoluzione degli strumenti portatili e la loro conseguente diffusione sono un primo importante fattore da considerare per stimare realmente il rischio di propagazione di questi software dannosi.

Gli smartphone acquistabili oggi permettono l'invio e la ricezione di SMS, MMS, email, la navigazione su Internet, l'ascolto di file MP3, la

Dall'articolo imparerai...

- come funzionano i worm Bluetooth,
- quanto possono essere pericolosi,
- nuovi paradigmi di attacco tramite la tecnologia Bluetooth.

Cosa dovresti sapere...

- conoscenze della tecnologia Bluetooth,
- conoscenze di base sul sistema operativo Linux,
- conoscenze utente avanzato di dispositivi mobili.

visione di filmati, la sincronizzazione con i computer fissi ed altre funzionalità avanzate che rendono questi strumenti i più a rischio di infezione. Ma i malware Bluetooth non attaccano solo i cellulari: il noto worm *Inqtana.A* ha ben dimostrato come la diffusione di codice virale e l'utilizzo di una nota vulnerabilità nella tecnologia Bluetooth su OS X 10.4 (Tiger) possano essere sfruttati per realizzare attacchi diffusi ben più gravi.

Il caso OSX/Inqtana.A

Inqtana.A è un worm Bluetooth *proof-of-concept* realizzato in Java, che attacca sistemi Apple OS X 10.4 (Tiger) senza l'aggiornamento di sicurezza relativo alla vulnerabilità CAN-2005-1333.

Per un errore di implementazione dello stack Bluetooth – nei sistemi OS X vulnerabili – risulta possibile effettuare un attacco di tipo directory traversal tramite una particolare richiesta al servizio *Object Exchange* (OBEX); in questo modo un aggressore può leggere file arbitrari sul dispositivo remoto.

Il worm *Inqtana* sfrutta questa vulnerabilità del sistema operativo per copiarsi all'interno di una particolare directory del file system, consentendo l'esecuzione automatica del worm stesso durante i successivi avvii del sistema.

In dettaglio il worm copia tre file, in specifiche posizioni: *w0rm-support.tgz* che contiene la classe e le componenti che costituiscono il worm stesso, com.openbundle.plist e com.pwned.plist che rappresentano file di configurazione utili per l'avvio automatico del codice, allo startup del sistema operativo.

Come per la totalità dei worm attuali, l'utente deve esplicitamente accettare la ricezione dei file. Una volta che il sistema viene riavviato, l'esecuzione del worm comporta la ricerca continuativa di dispositivi Bluetooth visibili e l'eventuale invio del codice dannoso.

Kevin Finisterre, noto esperto di mobile security, ha dimostrato come una piccola modifica su Inqtana possa essere sfruttata per arrivare a compromettere addirittura un'intera rete interna aziendale.

L'idea di Kevin è quella di utilizzare la propagazione e l'esecuzione di Inqtana per lanciare un exploit che permetta l'instaurazione di una connessione sul canale rfcomm dando luogo ad un accesso completo al sistema (*tty over rfcomm*). Dall'esterno un aggressore potrebbe quindi tentare di infettare dei sistemi vulnerabili all'interno, magari grazie ad un'antenna direzionale, ed accedere all'infrastruttura aziendale tramite il singolo client compromesso.

I worm Bluetooth oggi...

Come accennato, i worm Bluetooth attuali realizzano il trasferimento del codice virale tramite il semplice invio di file sul canale OBEX Push. Questo particolare servizio, disponibile in gran parte dei profili delle specifiche Bluetooth, permette il trasferimento di file in maniera non autenticata.

In un sistema Linux, opportunamente configurato con Bluez e con un'interfaccia Bluetooth compatibile, possiamo visualizzare il record relativo al servizio OBEX Push di un particolare dispositivo tramite il comando:

```
~ $ sdptool browse <bt address>
```

ottenendo il seguente output (in rosso si evidenzia il canale usato dal servizio):

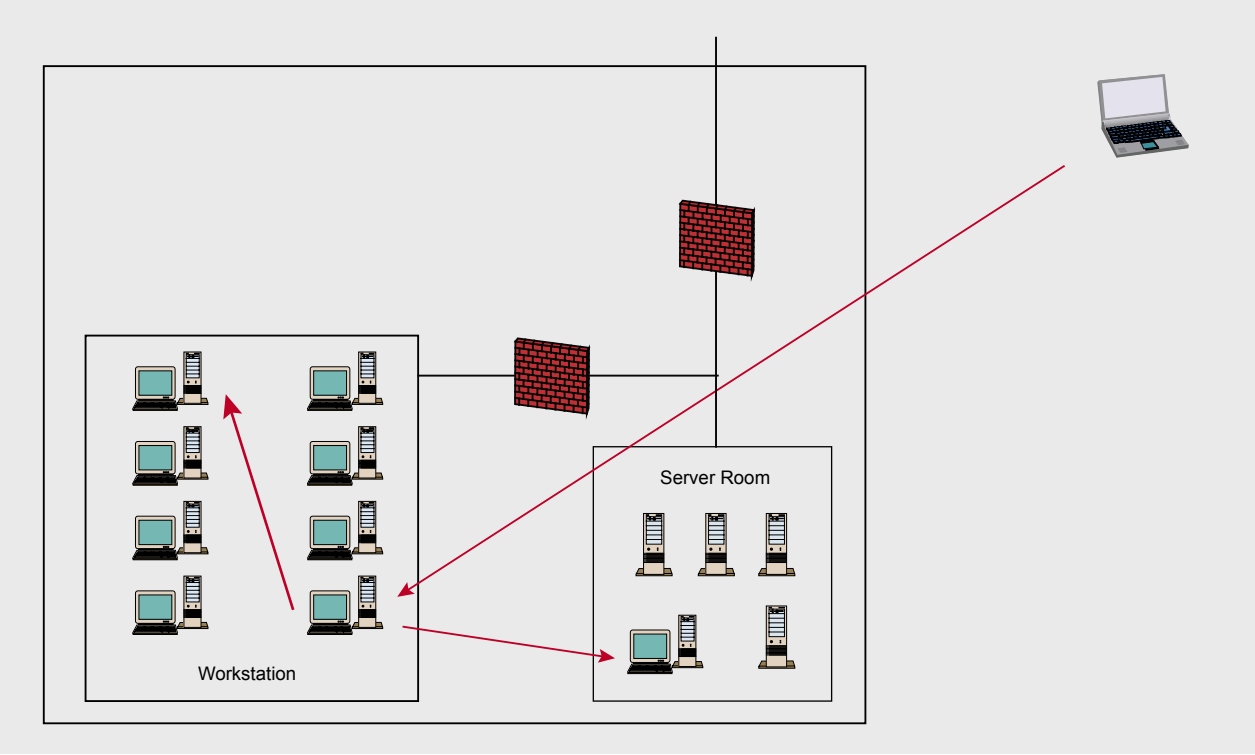

Fig. 1: *Schema di un attacco alla rete interna tramite un dispositivo Bluetooth vulnerabile*

```
Service Name: OBEX Object Push
Service RecHandle: 0x1000b
Service Class ID List:
  "OBEX Object Push" (0x1105)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 9
  "OBEX" (0x0008)
Language Base Attr List:
  code_ISO639: 0x656e
  encoding:    0x6a
  base_offset: 0x100
Profile Descriptor List:
  "OBEX Object Push" (0x1105)
    Version: 0x0100
```

Anche per chi non conosce approfonditamente la tecnologia è facile comprendere il significato di servizi e canali della tecnologia Bluetooth in quanto, attraverso una diretta analogia, è possibile paragonare i servizi esposti dai dispositivi Bluetooth con quelli normalmente presenti nei server di rete ed associati ad una specifica porta TCP/IP; il particolare servizio OBEX Push può essere quindi associato a diversi canali, a seconda del particolare dispositivo analizzato.

Per chiarire le idee, questa funzionalità è quella che viene utilizzata nei dispositivi cellulari per lo scambio di immagini, filmati e biglietti da visita elettronici (vcard).

Questo canale non autenticato è utile per il trasferimento di risorse quando non vogliamo effettuare il pairing tra due dispositivi; d'altra parte deve essere l'utente stesso ad accettare le connessioni ritenute sicure e a rifiutare quelle provenienti da soggetti sconosciuti.

Sebbene può risultare difficile da credere, l'efficacia della propagazione tramite questa modalità di connessione è molto alta: i worm attuali utilizzano semplici tecniche di social engineering, sfruttando l'inconsapevolezza e la curiosità delle persone.

Bluetooth worm molto semplici, come *Cabir.A* (2004, Symbian series 60), effettuano un'operazione di inquire alla ricerca di altri dispositivi Bluetooth; una volta trovata una potenziale vittima (un dispositivo quindi con Bluetooth acceso e visibile!) effettuano ripetutamente la richiesta di invio del worm stesso verso quest'unico apparecchio. Worm più evoluti utilizzano delle modalità di propagazione più efficienti, effettuando l'invio verso tutti i dispositivi visibili presenti *Cabir.H* (2004, Symbian series 60) oppure utilizzando diversi canali di propagazione *Commwarrior.A* (2005, Symbian series 60) disponibili dal particolare dispositivo (Bluetooth e MMS in questo caso specifico).

Fig. 2: *La BlueBag (interno)*

Come detto, l'utente deve però accettare esplicitamente il trasferimento; nessun worm attualmente in the wild (*BlueBug*, *HeloMoto*, etc.) sfrutta vulnerabilità dello stack protocollare Bluetooth.

Per invogliare le potenziali vittime ad accettare il codice malevolo si sfruttano semplicemente nomi particolari dei file e ripetuti tentativi di invio. In un classico scenario di propagazione il cellulare infetto cercherà continuamente di inviare il worm obbligando i possessori dei dispositivi vittima ad un'azione di forza: spegnere l'interfaccia Bluetooth, uscire dal range di trasmissione oppure – come accade nella maggioranza delle volte – accettare di buon grado il file in maniera da poter usare il dispositivo senza continue segnalazioni sonore e visive che limitano l'usabilità dell'apparecchio.

Nel caso di infezione è poi molto difficile accorgersi tempestivamente dell'avvenuta esecuzione del codice malevolo in quanto gli unici effetti riscontrabili sono una diminuzione della durata della batteria dell'apparecchio e un consumo eccessivo di risorse.

Il progetto BlueBag

Comprendere la reale diffusione della tecnologia significa determinare il reale rischio di fronte ad un possibile attacco.

Per una corretta valutazione è importante determinare il numero di dispositivi presenti, il range di trasmissione (ovvero la classe delle interfacce Bluetooth) ma anche moltissimi altri fattori spesso difficili da determinare sperimentalmente: il tempo di esposizione, azioni e reazioni della vittima, limitazioni *ambientali* e/o tecnologiche, etc...

Ma come valutare tutti questi parametri? come acquisire queste ed altre informazioni utili a valutare il rischio di esposizione verso aggressori umani e malware?

Per rispondere a queste domande, incuriositi dai nuovi fenomeni di Bluetooth malware, abbiamo realizzato il primo survey1 italiano dei

Fig. 3: *La BlueBag (esterno)*

dispositivi Bluetooth avvalendosi di un particolare strumento realizzato ad hoc: la *BlueBag*.

Utilizzando un sistema Linux all'interno di un normale trolley da viaggio – rigorosamente blu! – abbiamo costruito uno strumento versatile che ci permettesse di avere una grande autonomia, una considerevole portata radio ma che nello stesso tempo fosse comodo da trasportare e da utilizzare durante delle scansioni Bluetooth su larga scala.

La *BlueBag* è basata su un sistema *mini-ITX* al fine di ridurre al minimo i consumi avendo comunque una discreta potenza computazionale; durante la progettazione del sistema sono state ampiamente considerate le problematiche di consumo e l'ottimizzazione delle prestazioni.

A livello hardware, la BlueBag è composta dai seguenti componenti:

- Motherboard Via EPIA Mini-ITX (il modello fanless PD6000E),
- 256MB DDR400 DIMM,
- EPIA MII PCI Backplate (estensione per altre 4 USB 2.0),
- Hub USB 2.0 alimentato,
- iPod 20GB 1.8in Hard Drive,
- 8 dongle DIKON class 1 (chipset Broadcom Corporation),
- 1 dongle LINKSYS class 1 (chipset Cambridge Silicon Radio),
- Antenna NETGEAR omnidirezionale 5dBi,
- PicoPSU power supply,
- Accumulatore al piombo (12V-26Ah) che consente un'autonomia superiore alle 8 ore,
- interruttore a chiave,
- cavetteria varia.

L'hardware, acquistabile online e nei comuni negozi di elettronica, è facilmente reperibile ad un cifra che non supera i 600 euro.

Il dongle LINKSYS è stato scelto appositamente per la facilità con cui è possibile sostituire l'antenna integrata con una esterna, consentendo quindi portate maggiori; i lettori interessati posso reperire online un'ottima guida alla modifica: *http://trifinite.org/trifinite_stuff_bluetooone.html*.

A livello software, la *BlueBag* utilizza un sistema GNU/Linux Gentoo con kernel 2.6 e lo stack protocollare *BlueZ*, l'implementazione più nota e diffusa per Linux.

Al di sopra di questo normale sistema Linux è stato predisposto un software Python, sviluppato appositamente, che gestisce la scansione e le altre attività per cui la *BlueBag* è pensata.

Il software permette di gestire in maniera multithreaded i dongle Bluetooth disponibili al fine di migliorare l'efficacia della scansione; la *BlueBag* utilizza il dongle modificato con l'antenna per rilevare i dispositivi a distanza maggiore (intorno ai 150 metri), per poi allocare dinamicamente i rimanenti dongle che si occupano della scansione dei singoli servizi.

Per realizzare uno strumento versatile, senza dare troppo nell'occhio, è possibile configurare e monitorare la BlueBag attraverso un palmare o uno smartphone collegato alla borsa tramite una connessione TCP/IP over Bluetooth. In questo modo è possibile intervenire alla configurazione della scansione e delle analisi in maniera online, senza dover necessariamente aprire il trolley quando si è giro.

La BlueBag permette di svolgere diverse attività di scansione ed analisi:

Rilevamento di dispositivi Bluetooth attivi e visibili. Tutti i dispositivi vengono catalogati all'interno di un database con un preciso riferimento sul luogo e sull'istante in cui sono stati identificati. Per ogni apparecchio viene effettuata una scansione dei servizi (sdptool browse, psm scan, rfcomm scan) oltre al reperimento di ulteriori informazioni (identificativo, potenza del segnale). In maniera automatica il software della BlueBag cerca di associare anche la precisa tipologia e il particolare modello dell'apparecchio; per quest'ultima operazione viene utilizzata una particolare tecnica denominata *BluePrinting*.

Ogni dispositivo Bluetooth possiede determinate caratteristiche che, se considerate globalmente, rendono il dispositivo unico e identificabile: ogni apparecchio ha un indirizzo fisico univoco, una determinata casa produttrice (i primi 3 byte dell'indirizzo) e particolari servizi e canali abilitati. Attraverso il *BluePrinting* è possibile combinare tutte queste informazioni e realizzare una sorta di *impronta digitale* del dispositivo, in maniera molto simile al fingerprinting dei sistemi operativi utilizzato dal noto port scanner nmap.

Rilevamento dei dispositivi Bluetooth attivi ma *non-discoverable*. Attività svolta tramite una ricerca bruteforce sull'indirizzo fisico dell'interfaccia Bluetooth, in maniera analoga a quanto svolto dal tool *RedFang*.

Misurazione del tasso di successo rispetto a semplici tecniche di social engineering (OBEX Pusher). Attraverso questo task, la *BlueBag* ricerca tutti i dispositivi presenti nell'ambiente e cerca di effettuare il trasferimento di un file grazie al servizio OBEX PUSH, valutandone il tasso di successo. Le caratteristiche del file usato durante il trasferimento, l'identificativo del dispositivo ed i tempi di ritrasmissione sono completamente configurabili; in questo modo è possibile determinare empiricamente il numero di potenziali vittime da Bluetooth malware.

Ma quanto è diffusa la tecnologia in Italia?

Lo strumento realizzato è quindi servito per determinare sul campo la reale diffusione della tecnologia, in

differenti contesti (aeroporti, stazioni ferroviarie, centri commerciali, banche, università) avendo a che fare con differenti tipologie di utilizzatori (manager, teenager, ….).

In meno di 24 ore totali di scansione nella città di Milano, la *BlueBag* ha identificato 1405 dispositivi con una distribuzione del 93% per i telefoni cellulari, 3% notebook, 2% pda, 2% antenne GPS e altro.

In un simile esperimento, condotto in maniera parallela ed indipendente, *F-Secure*, durante la grande manifestazione CeBIT2006, ha identificato con un normale laptop circa 12500 dispositivi univoci durante l'intera settimana dell'expo.

Senza entrate nel dettaglio sulla validità statistica dei campioni è evidente come queste cifre supportino l'idea di un reale rischio per la propagazione di worm tramite questa tecnologia, considerando anche che la completa totalità dei dispositivi cellulari espone il servizio di trasferimento tipicamente usato dai malware.

Dalle misurazioni effettuate tramite l'OBEX Pusher è stato inoltre possibile stimare il tasso medio di successo, valutando al 7.5% il numero delle persone che senza conoscere la sorgente ed il contenuto del trasferimento hanno accettato di buon grado un file potenzialmente dannoso.

Infine, un altro dato interessante che è stato possibile recuperare è quello relativo al tempo medio di visibilità dei dispositivi che può essere letto come il tempo utile ad un eventuale aggressore per portare a termine un attacco; parlando di worm è proprio durante questo intervallo di tempo che il malware deve trasferire se stesso, prima dell'uscita della vittima dal range di trasmissione.

Fig. 4: *La BlueBag (dettaglio)*

In rete:

- Bluetooth SIG technical reference – *https://www.bluetooth.org*,
- Official Linux Bluetooth protocol stack – *http://www.bluez.org*,
- Bluetooth security – *http://trifinite.org*,
- OBEX OpenSource implementation – *http://openobex.triq.net*,
- Java/Bluetooth Tutorials – *http://wireless.klings.org/main.php*,
- Bluetooth technology overview (ITA) *http://bluetooth.interfree.it*,
- Bluetooth security (ITA) *http://www.ikkisoft.com/bluetooth.html*.

Questi valori si attestano intorno ai 12.3 secondi per il centro commerciale, 10.1 sec. per il campus universitario, 23.1 sec. per l'aeroporto e 14.4 sec. per gli uffici generali di una banca: tempi ridotti ma decisamente sufficienti per portare a compimento un attacco.

Worm evoluti. Il nuovo pericolo?

Sebbene i dati riportati sembrano evocare uno scenario tutt'altro che roseo, è anche vero che la gravità dei casi di infezione su ampia scala realmente avvenuti ridimensiona il pericolo.

Ma in futuro sarà sempre così?

Molti esperti concordano che le cose cambieranno e purtroppo in peggio.

Nel mondo del malware tradizionale stiamo assistendo ad un cambio del paradigma di attacco che ha portato i nuovi virus writer a concentrarsi su specifichi target, con scopi spesso a fini di lucro; siamo passati quindi da infezioni massive che vanno ad inficiare sulla qualità dei servizi e delle connessioni a software evoluti che servono per rubare informazioni o per creare botnet.

Anche nel campo del malware per dispositivi portatili è altrettanto probabile che si inneschi un meccanismo evolutivo che porti alla diffusione di software malevolo esplicitamente sviluppato per realizzare attacchi mirati. Non parliamo quindi di *semplice*

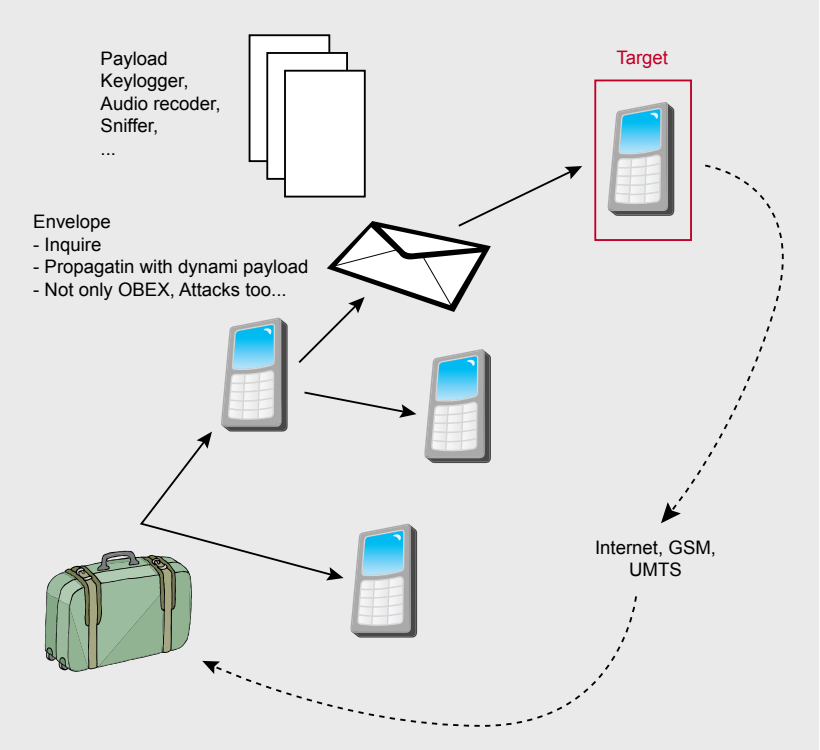

Fig. 5: *Schema di un attacco mirato tramite worm Bluetooth evoluti*

propagazione di worm ma di attacchi mirati verso determinati dispositivi vittima. Sfruttando i miglioramenti tecnologici dei nuovi dispositivi e l'evoluzione dei sistemi operativi mobile, i nuovi worm potrebbero adoperare tecniche di propagazione altrettanto evolute; da alcuni *proof-of-concept* sviluppati è ipotizzabile come i worm del futuro possano utilizzare vulnerabilità dello stack protocollare per agevolare l'infezione.

Nella definizione di queste nuove forme di malware evoluto è possibile ipotizzare l'uso di payload dinamici che consentano il deploy di codice virale differente a seconda del dispositivo che si sta infettando. In worm con queste caratteristiche possiamo identificare due componenti principali che abbiamo definito con il termine di envelope e payload. La prima componente è responsabile della ricerca dei dispositivi visibili e della propagazione dei diversi payload, a seconda dell'indirizzo Bluetooth o dell'identificativo dei dispositivi vittima. Il secondo elemento contiene invece il vero e proprio codice malevolo che può implementare diverse funzionalità (keylogger, sniffer, audio recorder) e che potrà utilizzare qualsiasi altro canale di trasmissione per far ritornare le informazioni rubate all'aggressore.

Come è facilmente intuibile, in una situazione di questo tipo il rischio di aggressione è molto più alto poiché non è necessario che l'aggressore sia effettivamente nel range di trasmissione con la vittima, cosa che sino ad ora ha reso di fatto impossibile la sottrazione di informazioni. Tra gli scenari ipotizzabili è possibile citare quello di un aggressore che infetti i dispositivi di alcuni dipendenti di un'azienda, con lo scopo di recuperare informazioni riservate dal palmare dell'amministratore delegato senza mai entrare in contatto radio con quel dispositivo.

Dallo sviluppo di alcuni *proof-of-concept* realizzati con Java 2 Micro Edition (J2ME) e compatibile con moltissimi cellulari aderenti allo standard MIDP 2.0 e JSR82 (Java Bluetooth API) è possibile mostrare come queste future evoluzioni non siano solamente fantasie. Alcune simulazioni, realizzate utilizzando parte dei dati sperimentali raccolti sul campo, hanno dimostrato inoltre l'estrema velocità di propagazione di queste nuove forme virali.

Tanti standard, poca compatibilità

I worm Bluetooth attuali e le futuribili evoluzioni fanno presagire un futuro incerto rispetto alla sicurezza dei dispositivi mobili anche per la riscontrata disattenzione degli utenti, che sembrano non essere pienamente consapevoli dei possibili rischi a cui vanno incontro.

Se da un lato l'aumento del numero di dispositivi dotati di connettività Bluetooth è in forte crescita, dall'altro la mancanza di standard generali sul software e sulle piattaforme limita fortemente la creazione di malware universale ed obbliga i virus writer a scrivere specifiche versioni per ogni tipologia di sistema.

Per un volta quindi la mancanza di standard rappresenta un elemento di vantaggio per la sicurezza degli apparecchi portatili: problemi di compatibilità rendono tecnicamente difficile la creazione di codice malevolo che sia installabile ed eseguibile sulle diverse piattaforme.

Ancora per qualche tempo i nostri dispositivi saranno quindi al sicuro da questo genere di worm, lasciando il tempo agli esperti di ricercare nuove soluzioni di difesa e ai normali utenti di comprendere i possibili rischi intrinseci nell'uso di questi apparecchi. ●

Cenni sull'autore

Luca Carettoni è laureato in Ingegneria Informatica al Politecnico di Milano con una tesi sulla sicurezza delle applicazioni web. I suoi interessi professionali sono collegati alla sicurezza delle applicazioni, al mobile computing e alla libertà digitale. Dal 2005 è invitato come relatore in tema di information security ai principali eventi italiani ed internazionali, in qualità di esperto in Bluetooth Security, Web Application Security ed Ethical Hacking. È autore di numerosi articoli sulla sicurezza informatica per le principali riviste italiane ed ha già pubblicato numerose advisory su vulnerabilità software.