


You've got the training to work  
around a technology loss.  
(We just want to make sure you don't have to.)



visit [CDW.com](http://www.cdw.com)



[Back to article](#)  [Print this](#)

## 'BlueBag' PC sniffs out Bluetooth flaws

**In just under 23 hours of travel, BlueBag was able to spot more 1,400 devices with which it could have connected**

**By Robert McMillan, IDG News Service**

June 07, 2006

If you happened to fly through Milan's Malpensa Airport last March, your mobile phone may have been scanned by the BlueBag.

Billed as a research lab on wheels, BlueBag was created by Milan's Secure Network SRL to study how malicious software might be able to spread among devices that use the Bluetooth wireless standard.

Basically, it's a [Bluetooth-sniffing computer hidden in a suitcase](#) (Note: PDF file) that was rolled through train stations, a shopping center, and even a computer security conference show floor this year to see how many Bluetooth-enabled devices attackers could potentially infect with a worm or a virus.

The answer: quite a lot. In just under 23 hours of travel, BlueBag was able to spot more 1,400 devices with which, in theory, it could have connected. Among the discoverable devices were a number of Nokia Corp.'s mobile phones and TomTom International BV's Go global positioning systems, said Stefano Zanero, Secure Network's co-founder and chief technology officer.

"Most of the devices that we found were from the same manufacturers because their default Bluetooth connection setup is to be discoverable, which is very good for ease of use, but very bad for security," he said.

Though many Bluetooth devices are designed to be hidden or detectable for very short periods of time, some manufacturers make their products detectable by default to simplify hook up with other Bluetooth-enabled machines -- a car sound system for example. Unfortunately, this practice also makes life easier for hackers, Zanero said. "Any discoverable device is potentially vulnerable to attacks," he said.

For example, BlueBag found 313 devices with the OBEX (Object Exchange) vCard and vCalendar exchange service enabled, making them prey for known Bluetooth virus attacks.

BlueBag's data is going to help Zanero and his researchers understand how attackers might use Bluetooth's ability to connect with other devices to create a targeted attack.

In a scenario they've envisioned, the bad guys could infect Bluetooth devices in a train station one morning, telling them to infect other equipment and seek out specific pieces of information. "You can deliver your malware, leave it for a few hours, and then catch it when [the user] goes home," Zanero said. "This makes it possible to perform the targeted attack that we have in mind."

At the August Black Hat USA 2006 conference in Las Vegas, the Secure Network team plans to unveil some proof of concept malware showing how this type of attack might work.

The hard part has been devising a protocol that will allow the malware to report back to an attacker. And since the researchers can't actually infect a bunch of Bluetooth phones, they need BlueBag to provide them with data so they can estimate how such malware might spread. "This gives you the figures you need for creating some small, not-very-reliable models of how these worms could interact," Zanero said.

Secure Network's research, which was co-sponsored by antivirus vendor F-Secure Corp. is not the first to highlight Bluetooth's security vulnerabilities.

A year ago, [hackers showed how they could connect to hands-free Bluetooth systems in some cars](#) to eavesdrop on telephone conversations and even talk to unsuspecting drivers. The software, called Car Whisperer, took advantage of poor security programming techniques on the part of the car manufacturers.

And variants of the [Cabir Bluetooth viruses](#) have been around for two years now. Cabir, which has never become widespread, preys on the kind of discoverable phones that BlueBag measured.

To avoid being bitten by Bluetooth attacks, Zanero says users should check their settings and make sure their device is set to be "hidden" or "non-discoverable."

This isn't a panacea, but it will make things harder for attackers. Using Bluetooth is "like sex," Zanero said. "It's better with precautions."

 [Print this](#)