R&D

Danny Bradbury

Stealth attacks may be covert, but there's one thing the perpetrators can't hide, and that's the expertise and the funding that they must have at their disposal

Catch me if you can

These days, malware writers are in it for the money. In order to maximise profit, discretion is imperative and therefore stealth technology has been adopted as a rule, rather than an exception. Danny Bradbury looks to the cat and mouse game that researchers and attackers are playing to see who's coming out on top

Mikko Hyppönen had played right into the malware writers' hands. But what could he do? The chief research officer at F-Secure was one of many researchers who had worked hard to spot the weaknesses in the MBRoot trojan, which was one of the first pieces of malware to rekindle an old, but effective, stealth attack.

"The authors had released a limited distribution of MBRoot to small audiences, so that the antivirus companies would see it. And so we started to figure out how to detect it," Hyppönen says.

MBRoot was a tough nut to crack. The malware writers, working as far apart as Italy, Russia and the Ukraine, had developed code that would write its files to the MBR - master boot record - (the sector of the hard drive that the computer looks at first when it tries to boot the operating system).

The programme also writes its own backdoor Trojan to another supposedly unreadable part of the hard drive. It patches the Windows loader so that in addition to loading the kernel, it also loads another driver in an area of the disk that would otherwise not be used by any files. It then intercepts the system's attempts to look at the contents of the MBR and returns the original contents, which are stored elsewhere on the disk.

"It's very hard to detect things like that, because whatever executes first has the upper hand," says Hyppönen. F-Secure and others came up with various techniques; they checked the area of the disk where they knew that MBRoot stored the copy of the original MBR that it overwrote. They compared the drivers being used in memory for both the hard drive and the CD Rom drive. In Windows XP they're normally the same, but MBRoot patched the hard drive driver with its own modified code.

> **"The best way not to be discovered is simply not to persist on the machine**

Don Jackson, SecureWorks

"We shipped standalone tools to detect the MBR rootkit, and we played into their hands. That is what they expected us to do," he recalls. As soon as the malware writers worked out what the researchers were doing, they re-engineered the code to avoid the fixes. The security vendors knew this would happen, but they still had to analyse the malware and develop countermeasures — that's what they do.

Sign of the times

Malware developers haven't always been this smart. This product testing with the security research community constitutes a level of quality assurance that you wouldn't normally see in the malware world, but things have changed in the last few years. Malware writers used to enjoy making their presence known, when joke payloads were all the rage. Teens writing viruses in their bedrooms reveled at the prospect of teasing their