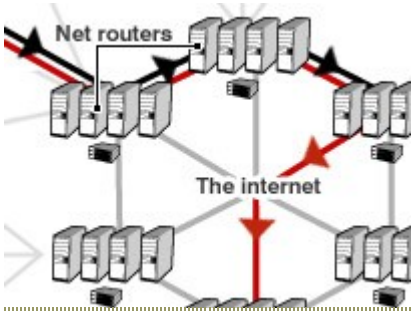
Trapping hackers in the honeypot



How the trap was sprung.

STAYING SAFE ONLINE

- Use anti-spyware and anti-virus programs
- On at least a weekly basis update anti-virus and spyware products
- Install a firewall and make sure it is switched on
- Make sure updates to your operating system are installed
- Take time to educate yourself and family about the risks
- Monitor your computer and stay alert to threats.

In this second part of our investigation using the BBC honeypot we recount what happened when we let the machine get infected rather than just log attacks. It is rare that you would willingly let vandals and burglars into your home but a controlled environment like a honeypot computer lets you do the technological equivalent in relative safety. The idea of letting the PC get infected was to see exactly what nasty programs hit our machine and how easy it was to recover from infection. Firstly, we visited a few of the websites mentioned in the many fake security warnings that pop-up unprompted thanks to loopholes in Windows Messenger. Much of the software available via these bogus warnings turned out to be a nuisance rather than downright malicious. The programs offered a free scan of the honeypot machine looking for spyware and adware. Every one we installed found a huge amount of spyware lurking on the computer. This was a surprise: The honeypot machine had only been used to visit the websites from which the bogus software had been downloaded. Checking the results with a bona fide spyware spotter revealed that most of the spyware identified by the fake software was benign. If this was not bad enough, all the fake security programs demanded money before they handed over the full results of the scan or tried to fix problems that were not there.

Spyware storm

One of the websites sending out fake security spam looked particularly interesting, as it was listed on several "block lists" net service firms use to spot junk mail. A visit to this website prompted an

immediate re-direct to another site which popped up a box asking if we wanted to download the bogus security program. Sneakily, this was an image rather than a Windows dialogue box so clicking anywhere on it, even the "cancel" button, got the download going. The download installed automatically and kicked off a tsunami of background downloading. The forensic software we had installed on the honeypot saw it connect to three or four other sites and start downloading from them - one was from a Thai hospital that was doubtless acting as an unwitting host. The software was so sneaky that it tried to stop this traffic being seen by injecting it into the processes usually used by the Internet Explorer. We knew this was the case because IE's homepage had been set to be blank – that is to say, when it was running there would be no net traffic. The result of the installation was new toolbars on the IE browser, a whole list of new unwanted favourites, all web searches were hijacked and redirected plus pop-up adverts populated the desktop.

The machine was becoming unusable because it was so busy so we were forced to cut the net connection. The bogus download went into overdrive trying to get back online. The meter clocking processor usage zoomed to 100% as it desperately tried to drag more stuff into the PC. The machine became hard to shut down and we could only shut it off by pulling the virtual plug. The end result of that single download was a PC that was unusable as it was so clogged with adware and spyware. A quick scan of the machine revealed that seven viruses, mostly trojans, had been installed during the orgy of downloading. We reverted back to the original configuration of the honeypot machine to get rid of the problems but this particular chunk of spyware was not done yet. On the honeypot a USB drive was being used to take backups of the attack logs. This had been plugged in to the machine while the fake security program installed itself. The USB drive had gained a new passenger - the core program of the fake spyware. If we had let this continue, doubtless it would have fired off next time the drive was plugged in to any other machine. It was a close escape. Cleaning up the PC proved impossible. It was lucky we could just revert to an earlier configuration. If the honeypot had been a home PC almost everything stored on it, pictures, e-mails, might have been lost.