The Trojan Defence
The Enemy Within

[Ian] Kennedy:
So what is this dark and mysterious underworld of computer malware and how much do we know about the extent of what it can do.
David M of Kaspersky's Lab says his virus analysts come up against some 35,000 threats a day which they track down using a number of methods such as web crawlers.

David M:
These are little programmes that download from websites and then we can analyse the code that's there to see if it's infected. We have things called honey pots. A lot of this malicious code comes through Spam e-mails. Well we have e-mail addresses that look perfectly normal and they attract Spam and we can then look at the Spam to see if there's any malicious code there. Most of those are analysed in an automated way. If we need to do any sort of hands-on analysis then we would typically be using de-bugging tools.

[Ian] Kennedy:
This is a very skilled process which a number of security companies undertake. Different companies give different names to the same viruses but David M says there is a degree of standardisation.

David M:
What we do have a fair degree of standardisation on is the overall categories of Trojan of Worm of virus and so you can normally tell from that what kind of threat it is and actually there are even mechanisms used across the industry so that people can check. We might call it Kido and somebody else calls it Conficker and somebody else calls it Downadup and you can see that we're using the same threat. Also what tends to happen is if we do a description for a threat on our website then it might well be if we know other people use different names we'll put them there as aliases so people know.

[Ian] Kennedy:
Understanding the structure is more important than actually naming the virus but that can be a problem too because viruses are often designed to hide their presence and behaviour from analysts.

David M:
One of the common methods used today is what's called a route kit and a route kit really is just an invisibility cloak for a computer programme. It stops you seeing the evidence that it's there. So what they try to do is to get their hooks into the system at as low level as possible so that they operate a bit like the operating system itself. You don't see it, it just does useful things and because it's an invisibility cloak you don't see what the Trojan is doing.

[Ian] Kennedy:
So given that most of us don't possess magical powers. What can mere mortals do to minimise their risk? As well as having up to date anti-virus software installed you should patch your system regularly and switch on automatic updates. Then there are basic rules of thumb.

David M:
Don't click on links in e-mails that have come from people you don't know. Don't click on the unsubscribe link because all you're doing is confirming to the spammer that you've got a live e-mail address. Don't respond to links in instant messages. They can create what are called chatbots which are robots but they start off sounding like a person. "Hello, how are you, thought you might like this link" and you think it's just somebody else but it isn't. Only respond

to people you know and all of those really are the rules. The final one I would say to people is if you are socialising or shopping online or banking online only do it on secure sites. Look in the bottom right-hand corner of your browser and see that there's a padlock. The key is really, this is not that different to the real world. You know in the real world there are muggers, there are pickpockets, there are people who could attack you with a knife but it doesn't mean that you're at imminent danger of that. We take precautions, you know, we don't go down dark alleys at night, we stay together with our friends when we come back from a party and the same is true online. Yes there is a threat and it is a real threat but you can at least minimise your exposure to that risk.

Voice Over:
The Trojan Defence was presented by Ian Kennedy, who is studying a Phd in the use of statistic and dynamic analysis to study the impact of malware on a forensic computer investigation at The Open University. You can find out more about research and courses in computer forensics by going to www.mcs.open.ac.uk