The Trojan Defence
The Trojan Defence

David M:
The term Trojan is borrowed from history and the idea of the Trojan horse which the Greeks used to try and get into the city of Troy. So they had this thing that looked benign, it looked like a gift, it looked like something nice but inside the belly of the wooden horse were Greek soldiers. The idea is it looks good, it smells good but actually there's a hidden agenda which is going to do you some harm.

Ian Kennedy:
My name's Kennedy, I'm a computer forensic investigator and in the course of this Podcast I shall be looking at how one type of malicious software, the so called Trojan horse, can get onto your computer. The anti-virus company Kaspersky's Lab deals with 35,000 threats every day. So how do they get into your computer? Senior researcher David M.

David M:
One of the most common methods and it is increasing is what's called a drive by download. In this case you go into a particularly ordinary website and you get infected automatically. The way it works is because the cyber criminals will look on the internet for websites that haven't been patched. They've got a loophole in there which allows them to kind of hide their malicious code on the website.

[Ian] Kennedy:
There are lots of other ways too of getting viruses onto your computer, through attachments or file sharing for example. It was in 2001 that Julian Green discovered to his horror that his computer had begun automatically connecting to unknown websites. These then downloaded child pornography images to his PC but worse was to come. Rob Newman of the solicitors [Kitsons 0:02:08.9] describes how a few months later there was a knock on the door. It was the Police with a warrant to remove Mr Green's computer for a forensic examination.

Rob Newman:
He felt very vulnerable of course and very lost and extremely anxious about what to do. Particularly because they'd found images there which he could simply not account for. He Knew he was innocent, he knew he'd done nothing wrong but of course establishing that was a major task for him and us.

[Ian] Kennedy:
[Kitsons] commissioned forensic investigator Martin Gibbs to investigate Mr Green's computer.

Martin Gibbs:
There were no search terms, there were no typed URLs or anything like that which suggested somebody had been looking for child pornography so as a result of that I extracted all the files and ran a virus scan across the files and identified that, I believe there was 10 or 11, that had various malicious code in them.

[Ian] Kennedy:
Julian Green's lawyers were able to argue the Trojan Defence. This means that unknown to him a virus had got onto his computer and downloaded these pictures. Julian Green was proved innocent but the stress of the whole incident caused him to lose custody of his daughter and possession of his house. Rob Newman.

Rob Newman: He came to us as a man in his 40s who had never been in trouble before, a family man. Life had been turned upside down. It was a horrendous experience for him, it was unlike anything he'd ever known before.

[Ian] Kennedy:
But it's not only individuals whose lives can be devastated by the Trojan horse. Whole companies and systems can crash. That's because cyber criminals can take control of not just one but multiple computers, giving them huge capability. September 20th, 2001. The entire computer system crashed at one of North America's biggest ports, the Port of Houston in Texas. David [Morrell 0:04:02.8], Port of Houston's computer analyst who first spotted the glitch recalls the damage.

David [Morrell]:
It can cause a delay in making a decision as to positioning a ship, getting a tug boat to a certain place or tying a ship up to a specific dock or knowing if a dock's available.

[Ian] Kennedy:
Along with other types of cyber attacks the Trojan Horse says David M "Is a game of cat and mouse" which shows no signs of going away.

David M:
It's a bit like that classic thing of painting the Forth Road Bridge, you know, you're never done in one sense. It's a continually moving target. If we were to go back 20 years and talk to the people who started developing anti-virus programmes and tell them that in 20 years time there would be millions of threats and they would be as sophisticated as they are now they would be amazed. So the problem keeps developing, keeps evolving and solutions to deal with it keep evolving as well and that will continue I think in the future.

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