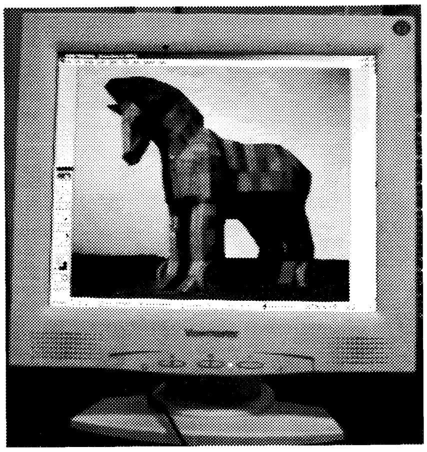
feature

Unknownuser and the SubSeven Trojan

A tale of computer crime.

By Mark Hunter*



This story is about a shy computer hacker who lived in Istanbul. He claimed that he could speak English fluently or afford to make overseas telephone calls. In 2000 this man came to be known by the FBI and the Alabama Police Department as "Unknownuser."

Unknownuser was also a vigilante, determined to identify purveyors of child pornography and provide their details to law enforcement agencies.

On 16 July 2000, officer Kevin Murphy was at the Police Department in Montgomery, Alabama. He found on his office computer an unsolicited e-mail and pornographic image, sent from Turkey by Unknownuser. The message contained the following text:

> I found a child molester on the net. I'm not sure if he is abusing his own child or a child he kidnapped. He is from Montgomery, Alabama. As you can see he is torturing the kid...I know his name, internet account, home address and I can see when he is online. What should I do? Can I send all the pics and info I have...Regards P.S. He is a doctor or paramedic.

How had Unknownuser hacked into the suspect's computer? He uploaded to a child porn newsgroup a pornographic image/file which contained the SubSeven (or "backdoor") program. SubSeven is in computer speak called a Trojan horse ("Trojan"). Trojans are malicious (and often destructive) programs which masquerade as benign applications. For example, during 2001 a hacker focused on some people's morbid curiosity and attached SubSeven to a file which posed as a video of the execution of Timothy McVeigh, the Oklahoma Bomber.[1]

When the user attempted to download the video, SubSeven automatically came in the "back door", silently executing itself. Once installed on a hard drive, trojans such as SubSeven permit unauthorized people like Unknownuser to secretly upload or download images and other files to the infected (and other networked) computers, and collect sensitive information such as passwords. Unlike viruses, Trojans do not replicate themselves but they can be just as destructive.[2]

Officer Murphy realized that the police could be in a bit of a bind, because computer hacking is a crime, and the Fourth Amendment (U.S. Constitution) protects against unreasonable searches and seizures by government officials and private individuals acting as instruments or agents of the government.

When Unknownuser refused Murphy's request for a telephone conversation, the two men continued to exchange e-mails. Murphy requested the suspect's e-mail address, and Unknownuser promptly also provided the suspect's name, address and facsimile number. The FBI then executed a search warrant on the residence of Dr. Bradley Steiger. When they found that his computer was password-encrypted, Murphy asked Unknownuser for the password. Steiger was arrested and charged with child exploitation and possessing child pornography.

By mid-2001 Steiger had been convicted and sentenced to 17 years imprisonment. The FBI had by this time managed to speak with Unknownuser by telephone, but he insisted upon maintaining his anonymity. The FBI thanked him for his assistance, and Unknownuser then divulged that he had used SubSeven to access Steiger's computer. Police reminded Unknownuser that the FBI would be "available" if he wanted to bring "other information" forward.

In December 2001, Murphy received from Unknownuser a series of e-mails attaching 45 files of child pornography "evidence" against William Jarrett, who Unknownuser said lived in Richmond, Virginia. Jarrett was soon arrested and charged.

The FBI again thanked Unknownuser for his continuing assistance, and by e-mail assured him that:

> ...you are not a citizen of the United States and are not bound by our laws...you have not hacked into any computer at the request of the FBI...*you have not acted as an agent for the FBI or other law enforcement agency.* (emphasis added)

Senior District Court judge Richard Williams upheld a challenge by Jarrett to this last contention, and suppressed the files provided by Unknownuser. His Honour's decision, however, was overturned on appeal. In July 2003, the US 4th Circuit Court of Appeals[3] determined

continued next page...

* Mark Hunter is a barrister at Darwin Chambers.

Unknownuser and the SubSeven trojan cont...

that the accused's Fourth Amendment rights had not been infringed by the police, because any agency relationship with Unknownuser did not come into existence until *"...after the fruits of Unknownuser's hacking had been made available to the FBI."*

Trojan Issues

Computer science is complex. Investigating, prosecuting, defending and trying computer crimes will often be a very challenging task.

Ted Coombs is a computer scientist and forensic software analyst based in California, with 25 years experience in the computer industry. Coombs believes that computer operating systems, and in particular the Windows operating system, are so insecure that it can be impossible to say that one individual has had control of their computer. Coombs explains:

> The number of viruses, worms, spyware, key loggers and other types of computer vulnerabilities is endless. The abilities of these 'malware' programs range from destroying the actual computer hardware to merely making copies of themselves and sending themselves onto the next desktop. Making changes to programs, capturing information such as passwords, or leaving behind files, like child pornography, falls into a mid-range capability.[4]

It is in this scientific context that the Northern Territory Government has seen fit to introduce legislation which shifts the burden of proof for the offence of possessing child pornography. The *Criminal Code Amendment (Child Abuse Material) Bill 2004* was passed by parliament on 14 October 2004. The bill introduces s125B into the Code. Under s125B, "child abuse material" is deemed to be in the possession of a person if at the material time it was in or on premises or a place occupied, managed or controlled by that person. In court, s125B shifts the burden of proof to the defendant, who must prove that he neither knew nor had reason to suspect that, in the case of illegal images, there was such material on his computer.

Section 125B is modeled upon a similar provision in the *Misuse of Drugs Act* (NT). The new section will have a major impact upon child pornography prosecutions in the Territory.

Child pornography legislation is also being hurriedly reformed in other Australian jurisdiction, in conjunction with Operation Auxin – a national police operation targeting child pornography.

The *Crimes Amendment (Child Pornography) Bill 2004* (NSW) does not shift the burden of proof by introducing the concept of deemed possession of child pornography. Furthermore, cl 91H(5) of that bill provides an important defence which is absent from the Territory legislation. The proposed New South Wales legislation provides a defence in respect of the possession of unsolicited child pornography which the defendant has taken reasonable steps "to get rid of" once he or she became aware of its pornographic nature.

The presence of certain Trojan infections, on a networked or isolated computer containing illegal images, may make it impossible to prove that the defendant had knowledge of the illegal images. Opening a file which has been downloaded onto a hard drive will activate Windows "last access" date stamp. But this date stamp may also be updated when a file is moved, scanned for viruses, or even if the computer mouse briefly hovers over a file name.

In 2003, the Crown Prosecution Service (Eng.) discontinued child pornography prosecutions against two men, after the defence conducted forensic software analysis which established the presence of Trojans, including SubSeven, on the hard drives which contained the illegal images.[5]

The type of forensic software analysis undertaken by the defence in the two English cases is expensive. Without such expert analysis, and testimony, an innocent defendant who has been the victim of a Trojan will be unlikely to prove his or her innocence – unless Unknownuser or one of his fellow computer hackers comes forward and admits his guilt.

Endnotes

[1] See www.sophos.com/virusinfo/articles/mcveigh.html viewed 22 October 2004.

[2] Security and Private Research Center. See glossary at www.cio.com/research/security/edit/glossary.html viewed 22 October 2004.

[3] *United States v Jarrett* 2003 WL 21744122 (4th Circuit 2003). Go to http://pacer.ca4.uscourts.gov/opinion.pdf/024953.P.pdf viewed 22 October 2004.

[4] See www.science.org/tedc/ (click "Child Pornography"), viewed 22 October 2004.

[5] The cases of Julian Green and Karl Schofield received widespread publicity in Europe. For example, see article from Le Monde (24/10/03, English translation) at www.anargratos.com/Privacy/Virusmakesyouguilty.htm viewed 22 October 2004.

Correction

In the October edition of *Balance* an article, "Tort law regression", by Tony Young was published on page 9.

The article included examples of potential damages under the new personal injuries laws. Two of the examples stated that the potential damages were $1050. These figures should have both been $10,500.