The Trojan Horse Defense in Cybercrime Cases

Susan Brenner
U of Dayton Law School

Brian Carrier
Purdue University - CERIAS

Variation of the “Some Other Dude Did It” (SODDI) defense

Examples:

- Caffrey (UK) was a self admitted hacker and charged with a DOS attack on Port of Houston. He was acquitted with a defense that other hackers framed him and used malware that wiped the computer (which is why the police could not find evidence of it).

- Pitts (US) was an accountant and charged with tax evasion. He was acquitted with a defense that a virus changed his documents (but not those of his clients).

- Several have used the defense that a virus or malware placed contraband images on their computers and contraband is becoming a popular method of online blackmail.

Highlights the need for better:

- Digital crime scene event reconstruction
- Standard Operating Procedures (i.e. scan all systems for malware)
- Reverse engineering tools
- Databases to store malware and analysis reports
- Physical evidence to support cybercrimes
- Methods to clearly and easily explain malware to a jury

Santa Clara Computer & High Technology Law Journal
Volume 21 Issue 1, November 2004