CERIAS Tech Report 2005-15

THE TROJAN HORSE DEFENSE IN CYBERCRIME CASES

by Susan W. Brenner, Brian Carrier, and Jef Henninger

Center for Education and Research in
Information Assurance and Security,
Purdue University, West Lafayette, IN 47907-2086

ARTICLES

THE TROJAN HORSE DEFENSE IN CYBERCRIME CASES

Susan W. Brenner[†] & Brian Carrier[‡]
with Jef Henninger[*]

TABLE OF CONTENTS

† NCR Distinguished Professor of Law & Technology, University of Dayton School of Law. Email: Susan.Brenner@notes.udayton.edu.

‡ Research Assistant at Purdue University's Center for Education and Research in Information Assurance and Security (CERIAS). Email: carrier@cerias.purdue.edu.

* J.D. University of Dayton School of Law (2004). Email: jef@1stcounsel.com.

I. INTRODUCTION

> *Aaron Caffrey walked free from Southwark Crown Court last week after being cleared of launching a DdoS attack on one of the busiest ports on the United States, even though both the prosecution and defense agreed that Caffrey's machine was responsible for launching the attack.*[1]

---

1. Munir Kotadia, *The Case of the Trojan Wookie*, ZD Net UK, *at* http://comment.zdnet.co.uk/0,39020505,39117240,00.htm (Oct. 20, 2003). A "DdoS" or "DDos" attack is

> an explicit attempt by attackers to prevent legitimate users of a service from using that service. A distributed denial-of-service attack deploys multiple machines to attain this goal. The service is denied by sending a stream of packets to a victim that either consumes some key resource, thus rendering it unavailable to legitimate clients, or provides the attacker with unlimited access to the victim machine so he can inflict arbitrary damage.

JELENA MIRKOVIC ET AL., A TAXONOMY OF DDOS ATTACKS AND DDOS DEFENSE MECHANISMS § 2, D-WARD - Laboratory for Advanced Systems Research, University of California, Los Angeles (CSD Technical Report No. 020018) (footnote omitted), *at* http://www.lasr.cs.ucla.edu/ddos/ucla_tech_report_020018.pdf (last visited Aug. 1, 2004). For a description of a DDos attack, see Steve Gibson, *The Strange Tale of the Denial of Service Attacks against GRC.COM*, *at* http://grc.com/dos/grcdos.htm (last modified June 28, 2004). A British newspaper offered this description of the attack allegedly launched by Aaron Caffrey:

> A lovesick hacker brought chaos to America's busiest seaport after launching a computer attack on an internet chatroom user who had made anti-American comments, a court heard yesterday.
>
> Aaron Caffrey, 19, is alleged to have brought computer systems to a halt at the Port of Houston, in Texas, from his bedroom in Shaftesbury, Dorset, in what police believe to be the first electronic attack to disable a critical part of a country's infrastructure.
>
> Paul Addison, prosecuting, told a jury at Southwark crown court that the teenager's intended target was a female chatroom user called Bokkie with whom he had argued over remarks she had made about the US.
>
> The court heard that Caffrey . . . had an American girlfriend called Jessica and when Bokkie started criticising the country and its people, he became upset and allegedly launched the electronic sabotage.
>
> The jury heard that the attack had to go via various intermediary computers to build strength before finally reaching Bokkie's PC.
>
> One of those intermediary servers was the Port of Houston, the eighth biggest shipping port in the world.
>
> The "denial of service" bug meant the port's web service was not accessible to provide crucial data for shipping pilots, mooring companies and support firms responsible for helping ships to navigate in and out of the harbour, placing shipping at risk.
>
> Mr Addison told the court that the attack could have had 'catastrophic repercussions to life and limb' but he added that it was not the prosecution case that the defendant intentionally targeted the Port of Houston server.

The "Trojan horse defense" surfaced in 2003 in several cybercrime cases brought in the United Kingdom. A Trojan horse program, a variety of malware,[2] is "a program that appears to have some useful or benign purpose, but really masks some hidden malicious functionality."[3] Malicious functionality could include anything from downloading contraband files to attacking other computers.

In what is perhaps the best-known of these cases, nineteen-year-old Aaron Caffrey was charged with "carrying out a denial of service attack on the computers of the port of Houston, Texas on September 20, 2001—less than two weeks after the 9/11 attacks."[4] The attack froze the port's webserver.[5] The denial of service attack,

---

> "The primary target is a female person he met on an internet chatroom service. He became disillusioned after an argument concerning citizens of the United States and anti-American sentiments.
>
> "The defendant's girlfriend was an American called Jessica. The defendant was deeply in love with her - in fact somewhat obsessed with her. He named his computer after her and he dedicated parts of the attack script to her rather like the way some adolescents draw graffiti on walls with 'I love so-and-so'. This defendant managed to weave into the script a sentence about his girlfriend Jessica."
>
> . . . .
>
> The jury heard that an investigation of the port's computer system found evidence the attack had come from Caffrey's computer. "There is a clear link between the defendant's computer here in England and the Bokkie computer which was also in America, as well as the Port of Houston's computer in Texas," Mr Addison told the court.
>
> Caffrey was arrested in January last year . . . . He denied targeting the port's system but admitted to knowing what a "denial of service" attack was and that they were "easy to perform".
>
> Mr Addison said Caffrey had told police he believed other hackers launched the attack and planted evidence in his hard drive.
>
> "The prosecution say [sic] it was him that launched the attack and not anybody else via his computer," he added. He said a search of Caffrey's hard drive showed he had the "wherewithal" to launch the attack.

Rebecca Allison, *Hacker Attack Left Port in Chaos,* Guardian Unlimited, *at* http://www.guardian.co.uk/online/news/0,12597,1057454,00.html (Oct. 7, 2003).

2. We define *malware* as "a set of instructions that run on your computer and make your system do something that an attacker wants it to do." ED SKOUDIS & LENNY ZELTSER, MALWARE: FIGHTING MALICIOUS CODE 3 (2003). *See infra* Part III.A.

3. SKOUDIS & ZELTSER, *supra* note 2, at 251.

4. Mark Rasch, *The Giant Wooden Horse Did It!,* Security Focus, *at* http://www.securityfocus.com/columnists/208 (Jan. 19, 2004). For a description of the attack, *see supra* note 1.

5. *See* Rasch, *supra* note 4; *see also* John Leyden, *Caffrey Acquittal A Setback for Cybercrime Prosecutions*, The Register, *at*

> which was traced to a computer at Caffrey's home by U.S. police, was allegedly aimed at taking a South African chatroom user called 'Bokkie' offline after she had made comments on IRC attacking the United States. Caffrey allegedly took offense at the comments because his girlfriend at the time, Jessica, was American.[6]

Caffrey admitted Jessica was his girlfriend at the time but denied any knowledge of the attacks.[7] At trial, Caffrey admitted being "a member of a hacker group called Allied Haxor Elite"[8] but claimed the evidence against him

> was planted on his machine by attackers who used an unspecified Trojan [horse program] to gain control of his PC and launch the assault.
>
> A forensic examination of Caffrey's PC found attack tools but no trace of Trojan infection.

---

http://www.theregister.co.uk/content/archive/33460.html (Oct. 17, 2003) ("Prosecution and defence in the case both agreed an attack that slowed the massive American sea port's Web systems to a crawl was launched from Caffrey's home PC.").

6. Munir Kotadia, *Teen Rides Trojan Horse Defense*, ZD Net UK, *at* http://zdnet.com.com/2100-1105_2-5092745.html (Oct. 17, 2003). "IRC" refers to Internet Relay Chat, "a multi-user, multi-channel chat system" that "gives people all over the world the ability to talk (type) to one another in real time. Each user has a nickname (handle) and converses with other users either in private or on a channel (chat room)." *An Introduction to Internet Relay Chat (IRC)*, NewIRCUsers.com, *at* http://www.newircusers.com/ircchat.html (last visited Aug. 1, 2004). Hackers, among others, often use IRC to communicate. As one article noted,

> IRC is largely unregulated—a Wild West of chat that has a special appeal for hackers.
>
> "Hackers obviously want anonymity when they're looking to trade personal information that they've obtained via identity theft, so Internet Relay Chat is a commonly used mechanism," says [Chad] Harrington.
>
> . . . .
>
> The unfettered nature of IRC is also appealing to hackers. . . .
>
> "It's older, it's not tied to Microsoft or AOL or a big company, it's one of the Internet protocols . . . so if you're running Windows or Linux or Macintosh or another flavor of Unix, you can use it," says [Bruce] Schneier. "So it's not that it's more suitable for hackers to use, it's just a more basic service and people who are anti-big-corporation are going to be more likely to use something like IRC."

Renay San Miguel, *Experts: Chat Rooms A Haven for Hackers,* cnn.com, *at* http://www.cnn.com/2002/TECH/internet/04/10/hackers.chat.rooms/ (Apr. 10, 2002).

7. *See* Kotadia, *supra* note 6.

8. Joshua, *UK Hacker Acquitted*, Geek.com, *at* http://www.geek.com/news/geeknews/2003Oct/gee20031021022289.htm (Oct. 21, 2003).

> The case therefore hinged on whether the jury accepted the defence argument that a Trojan could wipe itself or expert testimony from the prosecution that no such technology existed.[9]

While the prosecution was reportedly confident as to the strength of its case,[10] the jury acquitted Caffrey—who faced up to three years in prison—after deliberating for only a few hours.[11] The defense counsel apparently convinced the jurors that "a [T]rojan horse armed with a 'wiping tool' was responsible, enabling the computer to launch the DoS attack, edit the system's log files, and then delete all traces of the trojan—despite prosecution claims that no such technology existed."[12]

A reporter who covered the Caffrey trial gave his assessment of why the prosecution failed:

> Had the jurors been technology experts, or even computer-literate, I wonder if the ruling would have been the same. I spent most of the first week of the trial in the public gallery and found it didn't take long before the jury's eyes glazed over because the technical arguments sounded like a Russian version of Moby Dick that had been translated into English using Babelfish. By the third day, one of the jury members had to be discharged because of a severe migraine, which was indubitably brought on by the jargon.
>
> The prosecution was confident they had enough evidence to prove their case, which in my own opinion was justified. However, it was the jury that had to be convinced and it was impossible to do so unless they could present the evidence in a manner that made sense—but however they tried, they could not.
>
> . . . .

9. Leyden, *supra* note 5; *see also* Andy McCue, *Jury Out in UK Teen Hacker Case*, Silicon.com, *at* http://www.silicon.com/management/government/0,39024677,10006426,00.htm (Oct. 15, 2003) (Caffrey "claimed his computer had been hijacked by two hackers, known as dryice and frixion, using a Trojan horse to remotely control his PC without his knowledge"); Munir Kotadia, *The Case of the Trojan Wookie*, Computer Cops, *at* http://www.computercops.biz/modules.php?name=News&file=print&sid=3809 (Oct. 27, 2003).

10. *See* Kotadia, *supra* note 9.

11. *See, e.g.*, Kotadia, *supra* note 1.

12. *The "Trojan Defence—Bringing Reasonable Doubt to A Jury Near You*, SIFT Notes *at* http://www.iia.net.au/SIFTNote2003_17.pdf (last visited July 31, 2004); *see also* John Leyden, *Suspected Paedophile Cleared by Computer Forensics,* The Register, *at* http://www.theregister.co.uk/content/archive/33636.html (Oct. 28, 2003) ("The prosecution argued that no trace of Trojan infection was found on Caffrey's PC but the defence was able to counter this argument with testimony from Caffrey that it was possible for a Trojan to wipe itself.").

> The problem this kind of case presents is that, however improbable the scenario, it is possible that a Trojan opened a back door for a hacker and then removed any evidence of itself and the uninvited guest. It is also possible that Caffrey decided to attack someone that insulted his virtual girlfriend in a chatroom, but didn't realize the damage his script would cause.[13]

A few months before Caffrey's acquittal, another United Kingdom defendant who relied on the Trojan horse defense was acquitted of possessing child pornography. Julian Green was arrested when "172 indecent pictures of children were found on his hard drive."[14] When Green's computer was examined by a defense expert, the computer forensics consultant found eleven Trojan horse programs on it.[15] Based on the forensic expert's subsequent trial testimony, Green's attorney, like Caffrey's counsel, argued that the Trojan horses could have put the child pornography on his computer without his knowledge.[16] The prosecution offered no evidence at all, apparently because the chain of custody for the computer did not exclude the possibility that the evidence could have been planted by someone else.[17]

---

13. Kotadia, *supra* note 9; *see, e.g.*, *Man Cleared Over Porn 'May Sue'*, BBC News, *at* http://news.bbc.co.uk/1/hi/england/devon/3114815.stm (July 31, 2003):

> Julian Green, 45, was cleared in court earlier this month of 13 charges after pleading not guilty to making indecent images, claiming a computer virus was responsible.
>
> The prosecution offered no evidence at Exeter Crown Court against Mr Green, of Shiphay Lane, Torquay.
>
> . . . .
>
> During the court hearing, defence counsel Peter Ashman said "The defence case is that Mr Green had no knowledge of the images on his computer and was it possible they could have been put there without him knowing about it."
>
> Prosecutor David Sapieca said investigations had been carried out on the computer involved and how the images got there.
>
> "We don't accept the conclusions of the defence expert report but there were already other issues in the case regarding the history of the computer itself."
>
> "We cannot show that Mr Green downloaded the images on to the computer, so the Crown reluctantly offer no evidence in this case."

Id.

14. *Man Blames Trojan horse For Child Pornography, Sophos Anti-Virus Reports*, Sophos, *at* http://www.sophos.com/virusinfo/articles/porntrojan.html (Aug, 1, 2003).

15. *See id*.

16. *See id*.

17. *See* John Schwartz, *Acquitted Man Says Virus Put Pornography on Computer*, Mindcontrolforums.com *at* http://www.mindcontrolforums.com/virus-put-pornography-computer.htm (Aug. 11, 2003).

> [T]he prosecutor in the case, David Sapieca, told the BBC: "We don't accept the conclusions of the defense expert report but there were already other issues in the

A few months prior to the Green case, in what is believed to have been the first time the Trojan horse defense was used, prosecutors dismissed charges of possessing child pornography against another United Kingdom man, Karl Schofield.[18] A forensic expert found a Trojan horse program on Schofield's computer and concluded it was responsible for the images found on the computer's hard drive.[19] Prosecutors accepted the expert's testimony and dismissed the charges against Schofield, concluding they could not establish, beyond a reasonable doubt, that he was responsible for downloading the images.[20]

Finally, in a U.S. case, an Alabama accountant, who blamed a virus for tax fraud, was acquitted.[21] Eugene Pitts was prosecuted on nine counts of tax evasion and of filing fraudulent tax returns with the Alabama state revenue department.[22] The prosecution claimed he "knowingly underreported more than $630,000 in income over a three-year period."[23] Pitts, facing a fine of $900,000 and up to 33 years in prison, asserted that the errors on his returns were caused by a virus that "wasn't detected until after state revenue investigators alerted him in 2000 of problems with his personal and corporate returns." [24] Interestingly, none of the returns he filed on behalf of his clients were affected by the virus.[25] After deliberating for three hours, the jury acquitted Pitts of all charges.[26]

> case regarding the history of the computer itself. We cannot show that Mr Green downloaded the images on to the computer, so the Crown reluctantly offer no evidence in this case."

Id.

18. *See, e.g.*, John Leyden, *Trojan Defence Clears Man on Child Porn Charges*, The Register, *at* http://www.theregister.co.uk/content/archive/30385.html (Apr. 24, 2003).

19. *See, e.g.*, *Program Put Child Porn Pics on My PC*, READING EVENING POST, *at* http://www.getreading.co.uk/story.asp?intid=6541 (last visited July 17, 2004).

20. Charles Farrar, *Trojan Horse Clears Man of Child Porn Charges*, AVN, *at* http://www.avn.com/index.php?Primary_Navigation=Articles&Action=View_Article&Content_ID=17414 (Apr. 25, 2003).

21. *See, e.g.*, *Computer Virus Blamed As Man Cleared of Tax Evasion and Fraudulent Returns*, Sophos, *at* http://www.sophos.com/virusinfo/articles/virustax.html (Aug. 28, 2003).

22. *See, e.g.,* Patricia Dedrick, *Auditor: Virus Caused Errors,* THE BIRMINGHAM NEWS, Aug. 26, 2003, *available at* LEXIS, Alabama News Sources.

23. *Id*.

24. *Id*.

25. *Id.*; *see also Computer Virus Blamed As Man Cleared of Tax Evasion and Fradulent Returns*, *supra* note 21.

> "Without knowing the name of the virus which infected Mr. Pitts' computer, it is difficult to describe how it might have affected his tax returns and not those of his clients. It is certainly curious that only his records were targeted by the virus," said Graham Cluley, senior technology consultant for Sophos Anti-Virus.

The common thread that links these four cases is that they represent the invocation of a new version of an old defense: the SODDI ("Some Other Dude Did It") defense which is a routine feature of real-world criminal prosecutions.[27] In real-world prosecutions,[28] while the SODDI defense is generally unreliable,[29] there have been notable exceptions.[30] The logic behind the SODDI defense is as follows:

> When defense counsel invites the jury to conclude that the defendant is not guilty because he did not actually do the physical acts charged, or at least that the government has not proved beyond a reasonable doubt that he did, defense counsel will almost inevitably have to present at least some suggestion as to who might have done the acts instead. The typical juror will be less likely to develop reasonable doubts in the abstract, than if the defense is able to sketch out some "reasonable" alternative theory that will permit jurors to satisfy their natural human curiosity about

---

Id.

26. *See Accountant Escapes Tax Charges by Blaming Virus,* The Age, *at* http://www.theage.com.au/articles/2003/08/29/1062050651422.html (Aug. 29, 2003). It appears that the defendant in *People v. Dominguez*, No. D041946, 2004 WL 1068809 (Cal. Ct. App. May 13, 2004), may have tried to assert a variation of the Trojan horse defense.

> Appellant did not place child pornography on his computer. He is not knowledgeable about computers . . . . He had no explanation for how child pornography got on his computer and denied searching Internet sites for such material.
>
> Appellant testified that he could not have conducted the searches for child pornography on the evening of May 24, 2001, because he was at a union meeting. Union members testified appellant was present at the meeting on the evening of May 24, 2001.
>
> A computer expert testified that because several of the favorite files were added to appellant's computer at the exact same time, it was possible they were added by a computer program and noted that searches may be run without the computer user authorizing them.

Id. at *2–*3. Two viruses were found on the computer, but the appellate court dismissed them, noting that "neither had anything to do with . . . the pornographic images found on the computer." *Id*. at *2.

27. Rasch, *supra* note 4.

28. In this article, "real-world crime" is used to refer to traditional crime, i.e., crime the commission of which does not involve the use of computer or computer-related technology. "Cybercrime" is used to refer to crime the commission of which *does* involve the use of computer or computer-related technology. *See, e.g.*, Susan W. Brenner, *Is There Such a Thing as "Virtual Crime"?*, 4 CAL. CRIM. L. REV. 1 (2001),

available at http://www.boalt.org/CCLR/v4/v4brenner.htm (last visited Aug. 12, 2004).

29. *See, e.g.*, Jim O'Hara, *Jury Decides That Defendant's Alibi Sounds Far-Fetched*, SYRACUSE POST STANDARD/HERALD-J., Aug. 29, 2003, *available at* 2003 WL 5847229.

30. *See, e.g.*, *Moment Of Truth: O.J Simpson Is Set To Have His Say Today In Open Court*, ST. LOUIS POST-DISPATCH, Nov. 22, 1996, *available at* 1996 WL 2805134; s*ee also infra* Part II.B.4.

> dramatic events, and also their sense that real events must have some real-life explanation.[31]

As its moniker ("some other dude") implies, the SODDI defense usually attributes the commission of the crime to some unknown perpetrator.[32]

The Trojan horse defense could, perhaps more accurately, be characterized as the "malware" [33] defense, since it can be based on the activities of a virus as well as those of a Trojan horse.[34] As the

31. W. William Hodes, *Seeking The Truth Versus Telling The Truth At The Boundaries Of The Law: Misdirection, Lying, And "Lying With An Explanation"*, 44 S. TEX. L. REV. 53, 59 n.18 (2002) (emphasis omitted).

32. *See, e.g.*, BLACK'S LAW DICTIONARY 1396 (7th ed. 1999) ("The some-other-dude-did-it defense; a claim that somebody else committed a crime, usu[ally] made by a criminal defendant who cannot identify the third party.").

33. "Malware" is a catch-all term for malicious software i.e., for programs that can be disseminated and damage the computers they infect. *See, e.g.*, James P. Cavanaugh, *Computer Malware: What You Don't Know Can Hurt You, at* http://www.telus.com/downloads/Malware.pdf (2002). Malware includes viruses, worms and Trojan horses. *See id*. Viruses, essentially, infect other files, either program or data files; worms "are malicious programs that copy themselves from system to system, rather than infiltrating legitimate files." Mary Landesman, *What Is A Virus?*, *at* http://antivirus.about.com/cs/tutorials/a/whatisavirus.htm (last visited July 31, 2004). Trojan horses, as explained above, are remote access programs that allow computers to be compromised and used for illicit purposes. *See, e.g., id*.

34. Some defendants are also blaming browser hijackers for putting illegal material on their hard drives. In one widely reported case, a former citizen of the Soviet Union who prefers to be known only as "Jack" was charged with possession of child pornography after twelve pictures were found on the hard drive of his personal laptop. *See* Brian Rothery, *Mitsubishi Abandons Employee*, Inquisition 21st Century, *at* http://www.inquisition21.com/article~view~7~page_num~3.html (last visited July 17, 2004); *see also* Michelle Delio, *Browser Hijackers Ruining Lives*, Wired News, *at* http://www.wired.com/news/infostructure/0,1377,63391-2,00.html (May 11, 2004). Jack claims a browser hijacker must have downloaded the files to his laptop, pointing to the fact that police found no pornography—"not even a *Playboy* magazine"—when they searched his house. *Id*. Jack eventually pled guilty because, he says, no one would listen to his claims of innocence and his lawyer told him he would receive a much harsher sentence if he went to trial; he received three years felony probation and now has a felony sex conviction, which will make it difficult for him to find employment. *See id*. The evidence in Jack's case is somewhat ambiguous because "[s]ome of the images were found in unallocated file space, and would have to have been placed there deliberately since cached images from browsing sessions wouldn't have been stored in unallocated space." *Id*. It is clear, though, that browser hijackers can leave traces of embarrassing or illegal content on hard drives:

> Browser hijackers are malicious programs that change browser settings, usually altering designated default start and search pages. But some, such as CWS, also produce pop-up ads for pornography, add dozens of bookmarks—some for extremely hard-core pornography websites—to Internet Explorer's Favorites folder, and can redirect users to porn websites when they mistype URLs.

Doomjuice worm demonstrated, it can no doubt be based on worms as well. In February of 2004, the Doomjuice worm began spreading to computers that had been infected by the MyDoom or the MyDoom.B virus.[35] The Doomjuice worm put "the source code for the original MyDoom virus on victims' hard drives," which was the equivalent of planting evidence of virus creation on those computers.[36]

In this article, the phrase "Trojan horse defense" will be used to denote the presentation of any defense based on the alleged effects of malware, whether a Trojan horse, virus, worm or other program. This phrase is used both for efficiency's sake and because, so far, most of the successful Trojan horse defenses have been based on the operation of alleged Trojan horses.

In whatever form, the Trojan horse defense is an online version of the SODDI defense. Instead of blaming "some other dude," the defendant—like Pitts, Green, Caffrey, and Schofield—blames malware for the unlawful conduct that is being attributed to him or her.[37] Unlike the real-world SODDI defense, however, the Trojan

---

> Traces of browsed sites can remain on computers, and it's difficult to tell from those traces whether a user willingly or mistakenly viewed a website. When those traces connect to borderline-criminal websites, people may have a hard time believing that their employee . . . hasn't been spending an awful lot of time cruising adult sites.
>
> In response to a recent Wired News story about the CWS browser hijacker, famed for peddling porn, several dozen readers sent e-mails in which they claimed to have lost or almost lost jobs, relationships and their good reputations when their computers were found to harbor traces of pornography that they insist were placed on their computers by a browser hijacker.

Id.; *see also* Michelle Delio, *Nasty Malware Fouls PCs with Porn,* Wired News, *at* http://www.wired.com/news/infostructure/0,1377,63280,00.html (Apr. 30, 2004).

35. *See, e.g.*, Robert Lemos, *MyDoom Author May Be Covering Tracks*, CNET News, *at* http://news.com.com/2100-7349_3-5156836.html (Feb. 10, 2004).

36. *See id*.

> The author may be using the tactic to create a crowd of PC users in which to hide. . . .
>
> . . . .
>
> Doomjuice's possession of the source code for the original MyDoom virus suggests that the creator of the worm is also the writer of the original virus . . . .
>
> [A]ntivirus researchers agree that the latest hostile program could be intended to confuse investigations into who created the viruses.
>
> "It stands to reason that the author might be hiding his tracks," said Craig Schmugar, virus research manager for Network Associates. "He might be trying not to get caught."

Id.

37. *See, e.g.*, Schwartz, *supra* note 17.

> Mr. Green's case could point the way to a new defense in courts in the United States, said Andrew Grosso, a . . . former federal prosecutor in Washington. The

horse defense presents unique and difficult problems for the prosecution.

In a criminal prosecution, at least in the United States, the government must prove the defendant's guilt beyond a reasonable doubt.[38] This means that if a defendant like Eugene Pitts raises the possibility that a Trojan horse or other variety of malware is responsible for the crime with which he is charged, the prosecution must, in effect, prove a negative beyond a reasonable doubt.[39] That

---

> presence of a Trojan could mean that the computer is "not entirely under your control," he said, and a defendant could "legitimately point a finger elsewhere."

Id. Defendants in cybercrime cases can, of course, claim that an identifiable "someone else" is responsible for the unlawful activity being attributed to them. *See, e.g.*, State v. Cook, 777 N.E.2d 882, 888 (Ohio Ct. App. 2002) (noting that defense's theory in child pornography prosecution was that Cook's brother-in-law—Brown—planted child pornography on Cook's computer because of his "dislike of his sister's husband"). Such a claim is usually easier to rebut than the anonymous SODDI defense discussed in the text above.

> To prove that theory, the defense attempted to discredit the date and time of creation of the picture folders and files. The defense also introduced testimony about ill will between the two men and the fact that some pornographic files were created on April 20, 1999, when Cook was admittedly out of town . . . . Brown's own statement to the police indicated that he discovered the pictures of children while looking through some of the adult pornographic pictures on Cook's computer.
>
> On the other hand, the state presented evidence that Cook could have accessed his home computer from a remote location and that the computer's clock was correct. Moreover, Detective Driscoll testified that over 14,000 child pornography pictures with many varied dates were on the computer. To change the dates of these files, Brown would have had to access and change the date on each individual file. Given the brief time that Brown had access to the Cook computer, such a scenario appears unlikely.

Id. at 888.

38. *See, e.g.*, WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE § 24.6(c) (2d ed. 1999).

39. *See, e.g.*, Catherine Everett, *Viruses Bottleneck Prosecutors*, Compsec Online, *at* http://www.compseconline.com/analysis/030915computerevidence.html (Sept. 15, 2003).

> Trojan horses . . . installs [sic] a so called backdoor on a computer that enables hackers to take control of the machine in order to upload information, access personal data, or even use the machine as a proxy for spam so that such usage cannot be traced back to them.
>
> Trevor Mascarenhas, a partner at Philippsohn Crawford Berwald, explains: "Trojan horses have the potential to call into question the whole system of evidence for computer cases."
>
> While in a civil case, prosecutors have to show that the defendant is guilty on a balance of probability, in a criminal suit, they have to demonstrate this beyond all reasonable doubt.
>
> As a result, Mascarenhas warns: "A defendant might well be able to produce enough evidence to cast doubt over the prosecution's case and effectively destroy it."

Id.

is, to survive a directed verdict of acquittal and persuade the jury to convict such a defendant, the prosecution must disprove the possibility the defense has raised beyond a reasonable doubt.[40] As the Caffrey case demonstrated, this can be very difficult to do.[41] At least

40. *See, e.g.*, LAFAVE ET AL., *supra* note 38, § 24.6(c).

41. *See, e.g.*, Rasch*, supra* note 4.

> [A] forensic audit of Caffrey's computer showed no trace of a Trojan. At his trial, Caffrey simply argued that a Trojan could have been responsible, and that the government could not prove its case beyond a reasonable doubt. The jury agreed, and acquitted . . . .

Id.; *see also* Neil Barrett, *Scary Whodunit Will Have Sequels*, VNUnet, *at* http://www.vnunet.com/comment/1145835 (Oct. 27, 2003).

> I was one of the prosecution expert witnesses in the case of Aaron Caffrey. His computer was used to launch a distributed denial-of-service (DoS) attack. One of the computers used for the DoS attack belonged to the Port of Houston, and it crashed as a result of the DoS script intrusion. On Caffrey's computer there were IRC logs in which he apparently discussed the launching and probable effect of the DoS attack; there was the DoS script itself; and there were logs of the program being run. It seemed an open and shut case, in which a love-struck 17-year-old defended his American girlfriend's honour by responding to insulting IRC behaviour by launching a DoS attack.
>
> . . . .
>
> I analysed the seized computer and found no viruses or Trojan programs infecting any of the applications loaded on it. There was no evidence of any backdoor services having been enabled; there was no evidence of any logs having been altered; there was no evidence of any vulnerable services that could have been used to hack into the computer; and there was no trace of any secure deletion tool having been used. In short, there was no evidence that the computer had ever been remotely controlled. Though the defence effectively claimed a big boy did it and ran away, I could find no footprints where I would expect to have found them.
>
> Caffrey's defence was that such footprints could have been completely erased; the prosecution's assertion was that it is not possible to erase all the footprints, and that the attempt to do so would leave distinctive remains. For the defence, no computer expert witness was called to offer support to the claim. Caffrey himself served as his own expert witness.
>
> Despite no evidence beyond Caffrey's assertion that running programs could delete themselves without a trace, the jury found him not guilty.
>
> This leaves the prosecution of computer crime in the UK in a difficult position. Every case will now offer the defence of an untraceable Trojan horse program having been responsible. As a result of this decision, internet paedophiles and careless hackers have been offered a "get out of jail free" card that we will have to work very hard to counter. We will have to find better ways of presenting our arguments and of explaining how computers work - it's not going to be easy, but it is going to be necessary.

Id. *See generally* Sean Adam Shiff, Comment, *The Good, The Bad and The Ugly: Criminal Liability For Obscene and Indecent Speech on the Internet,* 22 WM. MITCHELL L. REV. 731, 739 (1996) (noting that it was "almost impossible to prosecute obscenity cases" under prior Supreme Court standard that "required [the prosecution] to prove a negative beyond a reasonable doubt—that the material was utterly without redeeming social value").

for the present foreseeable future, the availability of the defense raises concerns that defendants will be able to use a jury's ignorance, and likely suspicion, of technology to obtain an acquittal even when the evidence overwhelmingly supports a conviction.[42]

The question of how the prosecution can prove a negative beyond a reasonable doubt, especially in a computer crime prosecution where technology is an integral part of the evidence, is yet to be fully determined. In real-world trials, prosecutors often rebut the SODDI defense by establishing the defendant's motive to commit the crime and a lack of any plausible alternative suspects.[43] However, in prosecutions involving real-world crimes, jurors can rely on their common sense and their knowledge of how physical reality, and human beings, function; their common sense and grounding in empirical reality may be of little, if any, use in assessing the merits of a virtual SODDI defense in a cybercrime trial.

This article examines how the prosecution can respond to the invocation of a Trojan horse defense in a cybercrime case. Section II examines the legal issues raised by the defense; section III examines the technical issues involved; and section IV presents a brief conclusion.

II. LEGAL ISSUES

> *[A]ctual child pornographers could arm themselves with a new alibi that would be difficult to disprove. Or, unknowing Web*

42. *See, e.g.*, Silicon.com, '*Trust Me, I'm an IT Expert'*, Silicon.com, *at* http://www.silicon.com/comment/0,39024711,10006460,00.htm (Oct. 17, 2003).

> We are not questioning the jury's verdict in Caffrey's trial but the complex technical nature of some of the evidence and arguments highlights a growing issue for both prosecutors and defendants in high-tech crime cases.
>
> Computer forensics experts have expressed . . . concerns that even the most rock-solid of prosecution cases where all technical forensics procedures have been carried out to the letter of the law rest on the ability of the jury to understand the evidence.
>
> That's a jury where the range of knowledge probably goes from never having touched a computer to those who type a few letters and surf the net at work. If there's any doubt the jury must . . . acquit. Then there's the cost of pursuing the investigation and the trial. In this case it was over two years after the crime that the case was brought to court following a lengthy, and probably costly, police investigation. . . .
>
> [T]here has to be a better way of ensuring public money and police time isn't wasted pursuing technical cases where there is little chance of getting a guilty verdict.

Id.

43. *Cf. Moment of Truth, supra* note 30 and accompanying text.

> *surfers could find themselves charged with possessing illegal material that a lurking software program has acquired.*[44]

The Trojan horse defense creates great difficulties for investigators and prosecutors.[45] This section examines the legal issues the defense raises: section A reviews how a Trojan horse defense can be used defensively to negate elements of the prosecution's case; section B analyzes how the prosecution can respond to the assertion of such a defense.

Before explaining how the defense can be invoked and rebutted, it is important to note that the invocation of the Trojan horse defense may not be merely, as some maintain, a "defense tactic."[46] It is quite possible for the defense to be empirically valid. As Mark Rasch, former head of the Department of Justice's Computer Crime and Intellectual Property Section, explained,

> it is relatively easy to manufacture and plant electronic evidence consistent with guilt. In fact, with a few skills and tools, not only could you plant such evidence, but you could do so in such a way as to be virtually undetected, and so that it would be virtually impossible to determine that your target was not guilty.
>
> The very Trojan planted to launch the attack or download the incriminating files may be designed to self destruct and wipe itself from the hard drive. It would be almost impossible to overcome the circumstantial evidence pointing to your guilt. With sentencing guidelines becoming ever more draconian for computer related offenses, it is only a matter of time before . . . cyber set-ups become reality, if they aren't already.[47]

Indeed, cybercriminals are already exploiting our fears of being the victim of such a set-up. In 2003, online extortionists were "shaking down" office workers in the United Kingdom, "threatening to delete computer files or install pornographic images on their work PCs" unless they paid "a ransom."[48] Many workers paid the extortionists because they were afraid of being framed for possession

44. Schwartz, *supra* note 17.

45. *See Trust Me, I'm an IT Expert, supra* note 42 and accompanying text.

46. *See, e.g.*, Robert Vamosi, *It Wasn't Me; It Was the Trojan Horse*, CNET News, *at* http://reviews.cnet.com/4520-3513_7-5108036.html (Nov. 19, 2003) ("Remember the Twinkie defense? Well, now there's the Trojan horse defense.").

47. Rasch, *supra* note 4.

48. *Cyber Blackmail Targets Office Workers*, cnn.com (London), *at* http://edition.cnn.com/2003/TECH/internet/12/29/cyber.blackmail.reut/ (Dec. 29, 2003).

of child pornography.[49] While this extortion scam does not itself implicate the Trojan horse defense, it does contribute to a climate in which jurors will be receptive to the defense. If a juror has heard about people receiving emails that threaten to frame them by using a Trojan horse to plant evidence on their computer, that juror is likely to be far less skeptical of a Trojan horse defense than he/she might otherwise have been.

Our goal, then, is to explain how to negate the defense when it *is* simply a "defense tactic": a technologically-based SODDI defense. It is not our intention to discredit the Trojan horse defense, as there will no doubt be instances in which its invocation will be well-founded. Therefore, we seek only to explain how it can be negated when it is being used in an attempt to prevent the conviction of someone who is demonstrably guilty.

A. How the Trojan Horse Defense Is Used

The Trojan horse defense is used to negate the prosecution's claims that the defendant committed the crime(s) charged. As Part II(A)(1) explains, the defense can be used to establish a defendant's claims that he or she did not commit the crime (i.e., did not engage in the conduct that constitutes the crime). In this alternative, the defense concedes that the crime was committed but attributes its commission to someone other than the defendant. As Part II(A)(2) explains, the defense can also be used to show that, while the defendant may "technically" have committed the crime(s) charged, he or she lacked the *mens rea* required for conviction. In this alternative, the defense concedes that the defendant engaged in the conduct constituting the crime but uses the Trojan horse defense to rebut the prosecution's claims that he or she acted with the intent required for conviction. Part II(A)(3) explains how the defense proceeds to establish the Trojan horse defense.

1. Raise Reasonable Doubt

The Trojan horse defense is used to raise reasonable doubt in the same way the real-world SODDI defense is used.[50] That is, the defense gives the jury an alternative theory of the crime, an "it wasn't me, it was him" theory. The defendant disavows any involvement in the crime charged and claims it was committed entirely by someone

49. *See id*.

50. *See supra* Part I.

else.[51] Jurors can therefore acquit the defendant without feeling they have left a crime "unsolved"; they can acquit without remorse because they are confident someone other than the defendant committed the crimes charged. For example, the jurors in the Aaron Caffrey case could acquit Caffrey even though no one denied that his laptop was used to attack the Port of Houston computers because they presumably accepted the defense's argument that "some other dude" used his computer to carry out the attacks.[52]

As with real-world SODDI defenses,[53] the "other dude" is generally not identified. To date, he has been an unidentified, faceless perpetrator; a "hacker" whose depredations are beyond the jury's understanding, but in which they come to believe.[54] Ironically, the anonymity of the threat, which is usually fatal to the assertion of a SODDI defense in a prosecution for real-world crimes, works to the defense's advantage.[55] When the defense attorney presents evidence concerning the nature and manipulation of Trojan horses or other relevant types of malware, the prosecution cannot rebut this evidence because the existence and possible exploitation of these programs are not subject to dispute.[56] To negate the defense, the prosecution must show that malware was not responsible for the commission of the crimes charged in this particular case. But how can the prosecution

51. *See supra* note 31 and accompanying text.

52. *See supra* Part I.

53. *See supra* Part I.

54. *See supra* Part I.

55. *See, e.g.*, Hodes, *supra* note 31, at 59–60 n.18 ("The 'SODDI' defense is rarely successful . . . because competent prosecutors who have marshaled solid evidence can usually ridicule the strained inferences offered by the defense, and argue that the simple explanation—that 'the defendant dude did it'—cannot reasonably be called into question.") (emphasis omitted).

56. In a sense, the defense is introducing "'reverse 404(b)' evidence." *See* Dennis Prater & Tammy M. Somogye, *Some Other Dude Did It (But Will You Be Allowed to Prove It?)*, 67 J. KAN. B. ASS'N 28, 30 (May 1998); *see also,* United States v. Lewis, 92 Fed. Appx. 354, 356 (7th Cir. 2004). Federal Rule of Evidence 404(b) and similar state provisions allow the introduction of "bad acts" evidence for certain limited purposes, such as to show motive or identity. *See infra* Part II.B.2. "Reverse 404(b) evidence" denotes a defendant's using the prior bad acts of a "third person as exculpatory evidence" to establish that person as the perpetrator of the crime(s) charged against the defendant. Prater & Somogye, *supra*, at 30; *see also* United States v. Hamilton, 48 F.3d 149, 155 n.8 (5th Cir. 1995) ("When a defendant seeks to introduce 'prior bad acts' evidence against a government witness, this is often called 'reverse 404(b)' evidence, because it is being used against the government rather than against the defendant.") One who asserts a Trojan horse defense does this in a generic sense, i.e., without identifying a specific person. He introduces evidence that unidentified individuals have created, disseminated and used Trojan horses or other malware to take over computers for various purposes. Since the dissemination and use of malware is a crime in most jurisdictions, such evidence would constitute "reverse 404(b) evidence."

prove beyond a reasonable doubt that what *could have* happened in fact *did not* happen? These questions are addressed in Parts II(B) and III.

2. Negate *Mens Rea*

In the cases we have seen so far, defendants have used the Trojan horse defense to deny any involvement in the criminal activity with which they are charged. This will no doubt continue to be the primary way in which the defense is used; negating the *actus reus* and *mens rea* is, after all, the strongest possible defense. Soon, however, we may see some defendants use the Trojan horse defense merely to negate *mens rea*, a useful alternative for those who cannot deny that they engaged in conduct that constitutes the *actus reus* of the crime.

For example, an accountant who is charged with tax fraud for filing false returns might admit that he compiled and filed the returns but deny that he did so knowing the entries on them were false. The accountant could use a modified version of the defense to claim that the errors on the returns were the product of a Trojan horse or some other variety of malware.[57] A similar claim could be raised in a hacking case. In the Aaron Caffrey case, for example, Caffrey claimed the attack on the Port of Houston computers resulted from his unintentionally triggering scripts that had been installed on his laptop without his knowledge.[58]

3. Establishing the Defense

To establish a real-world SODDI defense, the defendant either points to an identified "other dude" as the perpetrator of the crime with which he is charged or essentially says "I did not commit this crime, therefore someone else did."[59] However, to establish a Trojan horse defense, the defendant has to introduce at least some evidence establishing that (a) a Trojan horse program or other malware was installed on his computer (b) by someone else (c) without his knowledge. The presentation of such a defense is likely to rely on the second alternative used to establish a traditional SODDI defense, i.e.,

57. *See supra* Part I.

58. *See, e.g.*, *Teen Hacker Acquitted in Port of Houston Case*, THE FORT WORTH STAR-TELEGRAM, Oct. 18, 2003, *available at* 2003 WL 65816842.

59. *See, e.g.*, Henry Weinstein, *Legal Strategy Being Formed in Blake Case*, L.A. TIMES, Apr. 21, 2002, at B1, *available at* 2002 WL 2470119; *Editorial: Conduct of McVeigh Trial, Jury Shows Justice System at Most Professional*, SUN-SENTINEL FORT LAUDERDALE, June 3, 1997, at 10A, *available at* 1997 WL 3107512; *see also* Prater & Somogye, *supra* note 56, at 30–31.

on the defendant's claims that he certainly did not commit the crime so it had to have been committed remotely by some unidentified person who exploited the capacities of malware.[60]

Ideally, the defense will be able to support these claims, at least in part, by pointing to the presence of malware on the defendant's computer.[61] The defendant may take the stand to disavow responsibility and emphasize that the malware found on his computer was responsible for the conduct being attributed to him.[62] This approach works when malware is found on the defendant's computer; police have found traces of Trojan horses in many of the cases we have seen so far.[63] In the Aaron Caffrey case, on the other hand, no malware was found on his laptop;[64] Caffrey's testimony was the only

60. *See, e.g.*, Munir Kotadia, *UK Port Hacker: 'I Was Framed'*, Silicon.com, *at* http://management.silicon.com/government/0,39024677,10006327,00.htm (Oct. 8, 2003).

61. *See supra* Part I. *See also*, John Leyden, *Suspected Paedophile Cleared by Computer Forensics*, The Register, *at*
http://www.theregister.co.uk/2003/10/28/suspected_paedophile_cleared_by_computer/ (Oct. 28, 2003).

> IT forensics firm Vogon has explained how its work helped clear a man accused of storing child pornography on his computer by proving his PC was contaminated by Trojan horse infection capable of downloading illicit images onto his machine.
>
> Julian Green was arrested . . . after police raided his home and found 172 indecent pictures of children on his hard drive. His solicitor, Chris Bittlestone . . . called in one of Vogon International's forensic investigators, Martin Gibbs, to help.
>
> A clone of Green's hard drive was sent to Vogon International in Bicester, where it was imaged and processed in the forensic laboratory using Vogon's specialist software. The data was then extensively examined and a report prepared, which highlighted that the Trojans were most likely to have come from unsolicited emails that Green opened before he deleted them.
>
> Gibbs identified 11 Trojan horse programs on Green's computer which were set to log onto "inappropriate sites" without Green's permission whenever he loaded up a browser to access the Internet.
>
> These findings were decisive in clearing Green of the 13 charges of making indecent images he faced at Exeter Crown Court this summer. On receiving evidence from Vogon the prosecution decided to drop the case.
>
> "The prospects of my client being able to effectively defend himself without Vogon's help were very remote," said Bittlestone. "The stakes for him were extremely high - if he had been convicted, prison was a strong likelihood.["]

Id.

62. *See, e.g.*, *Teen Hacker Acquitted in Port of Houston Case*, *supra* note 58 ("A jury at Southwark Crown Court in London accepted . . . Aaron Caffrey's contention that unidentified vandals had installed an attack script on his computer . . . .").

63. *See supra* Part I.

64. *See, e.g.,* Drew Cullen, *Teen Hacker Is Not Guilty,* The Register, *at* http://www.theregister.co.uk/2003/10/17/teen_hacker_is_not_guilty/ (Oct. 17, 2003).

evidence introduced to establish that some unknown remote actor committed the crime attributed to him.[65]

The Caffrey case differed from the other cases in which the defense has been raised in yet another respect: other defendants made a point of asserting their lack of sophistication with regard to computer technology and the hazards that lurk online.[66] Logically, this seems a basic component of the defense. The defendant says, in effect, "I am completely blameless in this matter because I did not commit the crime and I did not realize that by leaving my computer unsecured I was giving someone else, who is quite unknown to me, the opportunity to use my computer for unlawful purposes." Tactically, such a claim is likely to resonate with jurors who are themselves ignorant about computers and malware because they can identify with the defendant, perhaps shuddering as they contemplate the risks they have run by not installing anti-virus software or taking other measures to protect their own computers. The Caffrey defense, however, took the opposite approach. Caffrey admitted to being a member of a hacker group—Allied Haxor Elite—and hacking into other computers, though he claimed he only did so with permission from their owners.[67] The defense strategy seems to have suggested that Caffrey's flirtation with hacking resulted in his being "set up" by members of the hacking community.[68]

---

65. *See supra* Part I; *see also* Alison Purdy, *Hacker Cleared of Causing Biggest US Systems Crash*, BIRMINGHAM POST, Oct. 18, 2003, at 5, *available at* 2003 WL 64977219.

> During three days in the witness box, Caffrey protested his innocence, maintaining he knew nothing about the attack until police turned up on his doorstep to arrest him . . . .
>
> The teenager's ordeal began when officers who had traced the source of the attack to a computer at Caffrey's home . . . confiscated his computer and arrested him on suspicion of unauthorised modification of computer material.
>
> When computer experts who forensically examined his machine could find no trace of the Trojan horse, he was charged and brought before the court.
>
> He told the jury that it would have been impossible for the police computer experts to have tested every file on his PC for evidence of the Trojan.
>
> He also said the Trojan might have had a built-in facility to self-destruct, leaving no trace of its existence.

Id. Caffrey also "produced evidence from a systems administrator that showed hackers could have planted a Trojan programme on his computer, launched the denial of service attack and deleted all traces of their activities, leaving Caffrey to take the blame." Bill Goodwin, *Courts Urged to Replace Juries with Expert Panels of Judges in IT Cases*, COMPUTER WEEKLY, Nov. 4, 2003, at 4, *available at* 2003 WL 60336802.

66. *See supra* Part I.

67. *See, e.g.*, *Teen Hacker Acquitted in Port of Houston Case*, *supra* note 58.

68. *See, e.g.*, Kotadia, *supra* note 60.

It is also conceivable that someone could create the conditions required to invoke the defense by deliberately leaving their computer unsecured.[69] While it might seem inconceivable that someone would intentionally run the risk of having their computer attacked, this would be a clever way to establish the foundation for using the Trojan horse defense to avoid liability for one's own misdeeds.

B. How Can the Prosecution Respond?

As was noted earlier, a defendant's invocation of the Trojan horse defense essentially requires the prosecution to prove a negative—that malware and a remote perpetrator were *not* responsible for the commission of the crime charged—beyond a reasonable doubt.[70] As the Caffrey case demonstrates, this can be very difficult. In that case, there was no evidence that Trojan horse programs had been put on Caffrey's laptop; there was, however, evidence that he was a hacker who had a history of breaking into computer systems.[71] Notwithstanding this seemingly damning evidence, the jury acquitted him of all charges after deliberating only three hours.[72]

The result in the Caffrey case—indeed, the entire Trojan horse defense—may be a product of the public's general ignorance of computer technology and consequent willingness to believe that

69. *See, e.g.*, Micah Joel, *Safe and Insecure*, Salon.com, *at* http://www.salon.com/tech/feature/2004/05/18/safe_and_insecure/ (May 18, 2004).

> Last week, I turned off all the security features of my wireless router. I removed WEP encryption, disabled MAC address filtering and made sure the SSID was being broadcast loud and clear. Now, anyone with a wireless card and a sniffer who happens by can use my connection to access the Internet. . . .
>
> What's wrong with me? Haven't I heard about how malicious wardrivers can use my connection from across the street to stage their hacking operations? . . . Yup.
>
> . . . .
>
> In mid-April, Comcast sent letters to some of its subscribers claiming that their IP addresses had been used to download copyrighted movies. . . . [I]t's probable the letter was a result of pressure from the Motion Picture Association of America . . . .
>
> I've already composed my reply in case I receive one of these letters . . . . "Dear Comcast, . . . I had no idea that copyrighted works were being downloaded via my IP address; I have a wireless router at home and it's possible that someone may have been using my connection . . . ."
>
> If it ever comes down to a lawsuit, who can be certain that I was the offender?

Id.

70. *See supra* Part I.

71. *See supra* Parts I, II.A.3.

72. *See, e.g.*, Munir Kotadia, *Teen Cleared of Hacking Charge*, Silicon.com, *at* http://management.silicon.com/government/0,39024677,10006456,00.htm (Oct. 17, 2003).

strange and malevolent things are possible when one ventures into cyberspace. If this is true, it only exacerbates the difficulty prosecutors will face in attempting to rebut a Trojan horse defense. The strategy to be used will necessarily depend on the precise facts at issue. Accordingly, the sections immediately below examine legal issues that may prove helpful in countering a Trojan horse defense. Part III examines technical issues that may be helpful in the same regard.

1. Establish Defendant's Computer Expertise

Based on our experience with the defense to date, it seems likely that those who invoke the Trojan horse defense will claim they know little, if anything, about computer technology and were therefore vulnerable to being exploited by an unknown hacker who used their computer for unlawful purposes without their knowledge. If such a claim is part of a defendant's invocation of the defense, the prosecution may be able to rebut the defense by showing that the defendant is, in fact, knowledgeable about computers and what is required to protect them. Such evidence can be used to cast doubt on a defendant's claim that he must have been infected by Trojan horses or other types of malware when he opened suspicious emails or suspicious email attachments.[73]

The defense can, however, be a viable option even if the defendant has some computer expertise. Assume the prosecution's experts did not find malware during their initial analysis of the suspect's computer. Assume further that the defendant invokes the Trojan horse defense, that the computer is re-examined, and that this time, however, the prosecution's experts do find traces of malware. If law enforcement experts find malware only after someone asserts the Trojan horse defense, the defense may be able to show—using lab notes—that the prosecution's expert could not find the malware during the initial investigation. The defendant can then point out that, while he has some computer expertise, he is not an expert in computer forensics; he can then assert that if the prosecution's acknowledged expert could not locate the Trojan, there is no reason to expect the defendant himself to have identified it or realized it had been installed on his computer.

73. *See, e.g.*, *Program Put Child Porn Pics on My PC*, *supra* note 19.

2. "Character" Evidence

A different problem prosecutors can encounter in computer crime cases is a knowledgeable defendant. The defendant may have more computer expertise than the expert witnesses who will testify for the prosecution; he may, for example, be a black hat hacker[74] who started learning about computers in elementary school and has spent years honing his skills. He may, as an adult, work in the computer security field, which has only enhanced his expertise so that he is much more technically sophisticated than the prosecution's investigators and computer forensic experts. However, while a defendant's computer expertise can make prosecuting him more difficult, a prosecutor may still be able to use it to her advantage when the defendant invokes a Trojan horse defense by showing that the defendant either preplanned his Trojan horse defense or suggested it to his defense counsel.

While malware is becoming more sophisticated, it usually succeeds in attacking a computer because of user neglect (e.g., the user's not maintaining a firewall, downloading unknown attachments, not installing appropriate software patches or leaving the computer unsecured). Those who are knowledgeable about computers, and especially computer security, are less likely to fall victim to such an attack. If a knowledgeable user blames a Trojan horse for the unlawful conduct with which he is charged, the prosecution can use evidence of his computer expertise in an effort to rebut the claim. Such evidence can include testimony about his general computer expertise, as well as testimony from expert witnesses who can show that the computer was protected by a firewall and by up-to-date anti-virus software. This tactic is likely to be particularly effective when no evidence of malware was found on the computer. The lack of malware, coupled with the defendant's computer expertise and the steps taken to secure his computer, support the inference that there

74. Hackers are usually divided into "black hat hackers" and "white hat hackers":

> Black hat is used to describe a hacker (or, if you prefer, cracker) who breaks into a computer system or network with malicious intent. Unlike a white hat hacker, the black hat hacker takes advantage of the break-in, perhaps destroying files or stealing data for some future purpose. The black hat hacker may also make the exploit known to other hackers and/or the public without notifying the victim. This gives others the opportunity to exploit the vulnerability before the organization is able to secure it.

"Black Hat," SearchSecurity.com, *at* http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci550815,00.html (last visited Aug. 1, 2004). The term comes from old Western movies, where heros often wore white hats and the "bad guys" wore black hats.

was, in fact, no Trojan horse; therefore, the acts attributed to the Trojan horse were carried out by the defendant.

The defense may challenge an effort to introduce such evidence by claiming that the prosecution is improperly seeking to introduce character evidence.[75] Under Federal Rule of Evidence 404(a) and similar state rules, evidence of character "is not admissible for the purpose of proving action in conformity therewith on a particular occasion" except as set forth in the rule.[76] Although none of the exceptions in Rule 404(a) authorize the introduction of the type of evidence at issue here, that does not defeat the prosecution's strategy. Rule 404(a) and state analogues are meant to prevent a party from using character traits "as circumstantial evidence of behavior. The principle blocks resort to the 'general propensity' argument—the argument that since a person is . . . by disposition violent, it follows that he likely committed the violent act giving rise to the . . . charges."[77] These rules are therefore concerned with the defendant's personal qualities,[78] whereas the evidence the prosecution seeks to admit is not. Evidence of a defendant's computer expertise and the measures he has taken to secure his computer from attack do not go to his character,[79] so Rule 404(a) is not applicable.

The defense may then turn to Federal Rule of Evidence 404(b)[80] and comparable state provisions. Rule 404(b) states that "[e]vidence of other crimes, wrongs, or acts is not admissible to prove the character of a person in order to show action in conformity therewith." The defense may claim that the prosecution is

75. *See, e.g.*, *People v. Dominguez*, No. D041946, slip op., 2004 WL 1068809, at *7-*8 (Cal. Ct. App. May13, 2004).

76. *See* FED. R. EVID. 404(a).

77. 1 CHRISTOPHER B. MUELLER & LAIRD C. KIRKPATRICK, FEDERAL EVIDENCE § 100 (2d. 2004).

78. *See, e.g.*, FED. R. EVID. 404 Advisory Committee's Notes (1972 Proposed Rules, Note to Subdivision (a)) (addressing evidence of a violent disposition to prove that the person was the aggressor in an affray, or evidence of honesty in disproof of a charge of theft).

79. Under the Federal Rules of Evidence and state analogues, "character" evidence denotes an individual's personality traits, such as a "violent disposition" or honesty. *See, e.g., id.*; *see also* State v. McDaniels, No. CA487, 1993 WL 472903, at *3 (Ohio Ct. App. Nov. 9, 1993) ("'character' refers to a generalized description of a person's disposition or a general trait such as honesty, temperance or peacefulness. Generally speaking, character refers to an aspect of an individual's personality"). While computer expertise is certainly an individual attribute, courts have held that expertise in other areas does not qualify as "character" evidence under FED. R. EVID. 404. *See, e.g.*, United States v. Garcia, 77 F.3d 471 (4th Cir. 1996). And a defendant's efforts to secure his computer constitute acts, not character. *See, e.g.*, FED. R. EVID. 404(b) (noting that evidence of acts cannot be used to prove character).

80. *See* FED. R. EVID. 404(b).

impermissibly attempting to introduce evidence of "other crimes, wrongs, or acts" to prove an element of the crime with which the defendant is charged. The structure of this claim would presumably be that the prosecution's theory is as follows:

> (a) the defendant is charged with launching a denial of service attack;
>
> (b) he claims the attack was launched by a Trojan horse that was installed on his computer without his knowledge and ignorant as to its existence;
>
> (c) prosecution experts found no trace of a Trojan horse on his computer;
>
> (d) prosecution experts found he had installed a firewall and had up-to-date anti-virus software on his computer;
>
> (e) defendant has formal training in computer science, has worked with computers since he was twelve years old, and has been employed in the computer security field for the last five years; so, therefore,
>
> (f) he, not a Trojan horse, launched the denial of service attack.[81]

The defense's position would be that the prosecution is seeking to use evidence of the defendant's "acts" to prove an aspect of his character (e.g., computer expertise) by showing act in conformity with that character trait (e.g., since he secured his computer from attack, there was no Trojan; therefore, he is responsible for launching the denial of service attack).

The prosecutor can respond, conceding that although she is seeking to introduce evidence of "other acts," she intends to use the evidence not to establish conduct in conformity with some aspect of the defendant's character, but to prove "opportunity, intent, preparation, plan, knowledge, identity, or absence of mistake or accident" as allowed by Rule 404(b).[82] If we characterize the defendant's invocation of the Trojan horse defense as an assertion that the crimes attributed to him were the product of "mistake or accident," then evidence negating the possibility that a Trojan horse is responsible for the crimes should properly be admitted to rebut that

81. *See, e.g.*, *Teen Hacker Cleared by Jury,* Sophos, *at* http://www.sophos.com/virusinfo/articles/caffrey.html (Oct. 17, 2003); *see also supra* Part 1.

82. *See* FED. R. EVID. 404(b) ("Evidence of other . . . acts. . . . may . . . be admissible for other purposes, such as proof of motive, opportunity, intent, preparation, plan, knowledge, identity, or absence of mistake or accident . . . . ").

assertion.[83] The fact that the "other acts" the prosecution is offering are not criminal in nature is no impediment because Rule 404(b) "does not limit itself to the admission of evidence of other crimes."[84] The court may, however, want to give a limiting instruction to reduce the potential prejudice resulting from the introduction of such evidence.[85]

3. Negate the Factual Foundation of the Defense

There are two basic tactics law enforcement can use to negate the factual foundation of a Trojan horse defense: the first is, as Part III explains, to conduct a thorough technical analysis of the defendant's computer to determine the presence or absence of malware that could support the defense. If malware is found, the analysis should focus on whether it could have functioned as the defendant claims, that is, whether it could have contributed to the commission of the criminal activity with which he or she is charged. If malware is not found, the analysis should focus on whether there is evidence of wiping tools or other efforts to delete malware that was once installed on the computer.

The other investigative tactic law enforcement can use to rebut a Trojan horse defense is more traditional. As a National District Attorneys Association publication noted, "interrogation remains one of the three most critical pieces of the successful prosecution" of criminal cases.[86] So far, law enforcement investigators generally do not have to use skillful interviewing techniques to obtain admissions

83. *See, e.g.*, People v. Thatcher, No. 238361, 2003 WL 22092582, at *2 (Mich. Ct. App. 2003); Jackson v. State, 677 S.W.2d 866, 868-869 (Ark. Ct. App. 1984).

84. United States v. Hofstatter, 8 F.3d 316, 323 (6th Cir. 1993); *see also* State v. Benasutti, No. 95 CA 109, 1996 WL 402254, at *3 (Ohio Ct. App. 1996).

85. In *People v. Corbett,* 611 P.2d 965, 966 (Colo. 1980), for example, Corbett was charged with murder. The victim, who died from a stab wound, was seen in Corbett's company shortly before he died. *Id*. Corbett was convicted and appealed, arguing, in part, that the trial court had erred by allowing two witnesses to testify about his skill in martial arts, including the use of swords and knives. *Id*. at 967–968. The Colorado Supreme Court held that the admission of the testimony was not an abuse of discretion; it relied, in part, on the trial court's having given a limiting instruction which advised the jury that the evidence was admitted to show Corbett's physical accomplishments and that it was not to be considered as a reflection of his character. *Id*.

86. Brad Astrowsky & Susan Kreston, *Some Golden Rules for Investigating On-Line Child Sexual Exploitation*, UPDATE (Am. Prosecutors Research Inst., Alexandria, Va.), 2001, *available at*

http://www.ndaa-apri.org/publications/newsletters/update_volume_14_number_1_2001.html (last visited July 17, 2004); *see also* Vasili Polivanyuk, *Interrogation of Suspects in Investigating Computer Crime*, Computer Crime Research Center, *at* http://www.crime-research.org/eng/library/Polivan1003eng.html (last visited Aug. 1, 2004).

from those accused of computer crime. These suspects often confess readily and may even confess before being interrogated.[87] This is especially true of child pornography collectors, most of whom have no prior contact with law enforcement.[88] Their inexperience with the criminal justice system, coupled with the embarrassing nature of the crime, often prompts them to confess.[89] This may or may not be true of cybercrime suspects in general; so far, anyway, most of our experience with cybercrime investigations involves child pornography.[90] It is reasonable to anticipate, however, that inexperienced cybercriminals—such as juvenile hackers—will respond in a similar fashion, while those who have a history of committing crimes will not respond so readily to interrogation.

Officers often use a "logical approach" for "real world" crimes.[91] The suspect is locked into a story or alibi by the interrogator; the

87. *See, e.g.*, United States v. Froman, 355 F.3d 882, 886-887 (5th Cir. 2004); United States v. Puckett, 20 Fed. Appx. 471, 472 (6th Cir. 2001); United States v. Astley-Teixera, No. ACM 35161, 2003 WL 22495794, at *1 (A.F. Ct. Crim. App. Oct. 21, 2003).

88. *See, e.g.*, James F. McLaughlin, *Cyber Child Sex Offender Typology,* City of Keene Police Department, *at* http://www.ci.keene.nh.us/police/Typology.html (last visited July 17, 2004).

89. *See generally* People v. Timberlake, No. B163233, 2004 WL 928188, at *2 (Cal. Ct. App. April 30, 2004) (recounting how defendant testified that he was "'scared to death'" when police arrested him for, *inter alia*, having child pornography on his computer).

90. The disproportionate number of child pornography investigations is due to several factors, including the prevalence of child pornography online and the often foolish conduct of those who collect child pornography; many child pornography cases, for example, arise when a "collector" takes his computer in for repair and the technician finds child pornography on it. *See, e.g.*, United States v. Hill, 322 F. Supp. 2d 1081, 1083 (C.D. Cal. 2004); People v. Phillips, 805 N.E.2d 667, 669–70 (Ill. App. Ct. 2004). While conducting cybercrime training for an electronic crime task force, Professor Brenner was told about one suspect, who took his computer to the repair shop and cautioned them not to "harm" the 100 gigabytes of child pornography he had on its hard drive.

91. *See, e.g.*, BRUCE L. BERG, POLICING IN MODERN SOCIETY 162–63 (1999).

> The logical approach is based upon rational reasoning. One begins with the assumption that the suspect being interrogated is relatively reasonable and rational. If there is considerable evidence available, an officer using this approach will discuss these issues in fact with the suspect with the notion that once confronted with the overwhelming evidence, the suspect will likely discuss his or her involvement in the crime. When little evidence is at hand, this approach does not make false claims to the suspect. Such false claims are likely to be read as weaknesses . . . by a logical suspect. Instead, when little evidence is available, the logical approach dictates that the interrogating officer meticulously go over the suspect's statement, possible alibi, and explanations to assure consistency. When inaccurate or implausible statements or alibis are offered, the suspect should be challenged to indicate the flaws in his or her defense.

Id.; *see also id*. at 163–64 (explaining the emotional approach, indirect an direct line approaches, deflating or inflating ego approaches, and understating or overstating facts approaches).

interrogator then presents evidence to the suspect in an effort to convince him that his guilt is provable; therefore, he should cooperate with investigators.[92] Ideally, the suspect is overwhelmed by the evidence and offers to cooperate.[93]

A problem that arises more for cybercrime than for real-world crimes goes to an investigator's ability to confront a suspect with evidence, which establishes the suspect's guilt.[94] Evidence collection usually precedes an arrest for real-world crimes, so evidence is available for use in an interrogation.[95] For computer crimes, a suspect's arrest usually coincides with the seizure of the computer(s) he used to commit the offense(s).[96] Forensic examination of a computer is a time-consuming process that probably will not have

92. *See id*.; *see, e.g.*, Richard A. Leo, *Inside the Interrogation Room*, 86 J. CRIM. L. & CRIMINOLOGY 266, 278–79 (1996).

> [T]here is great variation in the distribution of the interrogation tactics I observed. A couple of the tactics were used in virtually all of the cases, several others were used in approximately one-third to one-half of the cases, a couple were used in approximately one-fifth of the cases, a few others were used only sparingly, and others virtually not at all. If a portrait of the typical interrogation emerges from the data, it involves a two-prong approach: the use of negative incentives (tactics that suggest the suspect should confess because of no other plausible course of action) and positive incentives (tactics that suggest the suspect will in some way feel better or benefit if he confesses). In my sample, detectives typically began the interrogation session by confronting the suspect with some form of evidence, whether true (85%) or false (30%), suggesting his guilt and then attempting to undermine the suspect's denial of involvement (43%), while identifying contradictions in the suspect's alibi or story (42%). But detectives relied on positive incentives as well, most often by appealing to the suspect's self-interest (88%), but also by frequently offering the suspect moral justifications or psychological excuses (34%), using praise or flattery (30%), minimizing the moral seriousness of the offense (22%), appealing to the importance of cooperation with legal authorities (37%) or appealing to the detective's expertise (29%), or appealing to the suspect's conscience (22%). In approximately 90% of the interrogations I observed, the detective confronted the suspect with evidence (whether true or false) of his guilt and then suggested that the suspect's self-interest would be advanced if he confessed.

Id. (note omitted).

93. *See, e.g.*, United States v. Slanina, 283 F.3d 670, 674 (5th Cir. 2002); United States v. Mohrbacher, 182 F.3d 1041, 1044 (9th Cir. 1999); United States v. Astley-Teixera, No. ACM 35161, 2003 WL 22495794, at *1 (A.F. Ct. Crim. App. 2003).

94. *See, e.g.*, *supra* note 92.

95. *See* BERG, *supra* note 91, at 162–63; *see also*, United States v. Hemmings, 64 Fed. Appx. 68, 70 (9th Cir. 2003); Miles v. State, 781 A.2d 787, 839 (Md. 2001).

96. *See, e.g.*, People v. Conover, No. G030463, 2004 WL 348967, at *2 (Cal. Ct. App. Feb. 25, 2004) ("During the afternoon of January 21, police officers returned to Conover's room with a search warrant. The officers arrested him, searched the room, and seized his computer, digital camera, video games, magazines, a three-page printout of naked young women, and several photographs of neighborhood children.").

begun by the time a suspect is interrogated.[97] Consequently, the interrogator will not be able to confront the suspect with evidence obtained from his computer; he may, however, be able to confront him with other evidence derived from executing a search warrant or a consent search.[98]

One of the biggest problems law enforcement faces is the growing "community nature" of child pornography collectors,[99] which may seem peculiar since those who are interested in child pornography often live alone and tend to be socially isolated.[100] When pedophiles first start to collect child pornography, they generally use static sites that do not involve interacting with others; when they move onto chat rooms, they tend to be more interested in trading images than chatting.[101] Eventually, they may move into a child pornography network; such networks are widespread and provide a source of support for those interested in child pornography.[102]

97. *See, e.g.*, Wade Davies, *Computer Forensics: How to Obtain and Analyze Electronic Evidence*, 27 CHAMPION 30 (June 2003), *available at* Westlaw, 27-JUN Champion 30 ("Our experience is that the examiner will require at least a whole week to complete a full forensic evaluation of a single computer."). *See generally* U.S. DEP'T OF JUSTICE, COMPUTER CRIME AND INTELLECTUAL PROP. SECTION, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS § II(D), *at* http://www.cybercrime.gov/s&smanual2002.htm#_IID_ (July 2002).

98. *See, e.g.*, United States *ex rel*. Martin v. Lane, No. 89 C 20226, 1990 WL 304259, at *4 n.1 (N.D. Ill. 1990).

99. *See, e.g.*, PHILIP JENKINS, BEYOND TOLERANCE: CHILD PORNOGRAPHY ON THE INTERNET 71–74, 88–91 (New York University Press 2001).

100. *See, e.g.*, Sentencing Decision at ¶ 7, Regina v. Pecciarich, [1995] O.J. No. 2238, *available at* http://www.efc.ca/pages/law/court/R.v.Pecciarich-sentence.html (last visited Aug. 1, 2004) (stating that defendant convicted of distributing child pornography was "a loner with a 'flat' affect, spending much time at his computer"); *see also* McLaughlin, *supra* note 88.

101. See McLaughlin, *supra* note 88.

102. *See, e.g.*, UNITED KINGDOM NATIONAL CRIMINAL INTELLIGENCE SERVICE, UNITED KINGDOM THREAT ASSESSMENT OF SERIOUS AND ORGANISED CRIME 2002 §§ 9.6–9.7, *at* http://www.ncis.gov.uk/ukta/2002/default.asp (last visited July 17, 2004).

> Most . . . paedophiles operate alone. Organised paedophile groups are relatively rare, but the extent of networking by paedophiles is significant. . . . [T]he purpose of networking is to exchange . . . pornography and fantasies, and to support those involved in justifying their actions. For example, paedophile networks provide positive reinforcement that child pornography is acceptable. . . . Online guides to all aspects of paedophilia are available. Some have hyper-links to paedophile bulletin boards, information about paedophile chat rooms, where IT expertise and access or grooming techniques are shared, and passwords or pass-phrases given to access pornography. . . .
>
> Most online paedophile networks are hierarchical in structure and secretive, with access by invitation only. Paedophiles may be approached in chat rooms and invited to join a network. Often, there is a vetting process, with status and trust

While not widespread, "child love" websites have been growing in popularity. These sites use terms such as child lovers, boy lovers and girl lovers to describe the activity they promote. While these sites make it clear they do not host child pornography, they offer message boards, chat rooms and other methods for communicating that can be used to establish a community for those interested in child love and related topics.[103] It is not clear how many of those who frequent these sites are interested in child pornography, but the sites give those who are interested an opportunity to share knowledge and ideas, including ideas about how to avoid law enforcement. The North American Man/Boy Love Association, for example, includes an entrapment warning on its website.[104] Other similar sites provide information about anonymity, encryption and evidence elimination.[105]

The increasing cohesiveness of child pornography collectors, coupled with the availability of the Trojan horse defense, means interrogation can be especially important in a child pornography case. One useful technique in interrogating those suspected of being involved with child pornography is rationalization. Rationalization is a one-sided discussion that offers excuses or reasons that minimize the seriousness of the crime and make it easier for the suspect to confess by allowing him to save face.[106] It also allows an interrogator to overcome fears the suspect has about confessing.[107] Two common fears that are especially prevalent in child pornography cases: fear of embarrassment and fear of arrest and prosecution. The fear of embarrassment stems from the stigma society attaches to the crime.

> being gained by evidence of illegal activity. Protecting themselves against law enforcement is a key concern, and some online paedophiles openly discuss methods for keeping their activities from the police. There is also evidence that online networks undertake counter-intelligence activity, researching techniques used by the police and internet watch groups by debriefing people who have been arrested.

Id.; *see also* JENKINS, *supra* note 99, at 88–96.

103. *See, e.g.*, GL Garden, *at* http://www.glgarden.org (last visited July 17, 2004).

104. *See Entrapment Alert*, North American Man/Boy Love Association, *at* http://216.220.97.17/entrapment.htm (last visited Aug. 1, 2004).

105. *See, e.g.*, *Resources: Privacy & Security*, BoyLinks.net, *at* http://www.boylinks.net/resources_privacyandsecurity.html (last visited July 17, 2004); *Security and Privacy*, Girl Chat, *at* http://www.annabelleigh.net/securityx.htm (last visited July 17, 2004).

106. *See, e.g.*, Michael R. Napier & Susan H. Adams, Ph.D., *Criminal Confessions: Overcoming the Challenges*, 71 FBI L. ENFORCEMENT BULL. 9, 13 (November 2002), *available at* http://www.fbi.gov/publications/leb/2002/nov02leb.pdf.

107. *Id.* at 203.

The community aspects of child love websites, such as message boards, may contribute to the fear of arrest and prosecution.

In addition to questions that are designed to elicit a suspect's admission that he did commit the crime, such as possession of child pornography, he should be asked a series of other questions that are designed to rebut a Trojan horse or related defense. Questions such as "Who else has access to this computer?" and "Have you ever been the victim of a Trojan horse? Do you know what a Trojan horse is?" can help bolster the prosecution's case while foreclosing the defendant's use of such a defense.

Surveillance is another important investigatory tool, but it loses much of its effectiveness when a defendant raises a Trojan horse defense. Surveillance can be used to place a suspect at the computer when it was used for unlawful purposes, allowing officers to determine who had access to the target computer and when each person had access.[108] Surveillance is especially useful, therefore, in defeating a "real-world" SODDI defense (i.e., a claim that someone else was using the computer when child pornography was downloaded or other types of unlawful activity occurred).[109] Generally, however, surveillance is not effective against a Trojan horse defense because the defendant admits to using the computer in question but attributes the unlawful activity to the malware.[110]

To rebut a defendant's claim that malware carried out unlawful activity without his or her knowledge, the prosecution can utilize traditional approaches to establishing motive, intent, and culpable conduct. One approach is to show the extent to which the computer in question was utilized for unlawful purposes; if it was predominantly used, say, to collect child pornography, this evidence of a pattern of consistent behavior can be used to rebut the defendant's contention that he had no idea illegal material was on his

108. *See* Astrowsky & Kreston, *supra* note 86.

> Surveillance is one way to put the perpetrator behind the computer. Meeting the untrue SODDI defense may require that the perpetrator's home/business be surveilled to determine who has access to the computer and at what times of the day. It is crucial that information be gained at the investigatory stage to defeat this claim.

Id. For an explanation of the SODDI defense, *see supra* Part I.

109. *See* Astrowsky & Kreston, *supra* note 86. *See, e.g.,* United States v. Gallo, 53 M.J. 556, 559, 567-568 (A.F. Ct. Crim. App. 2000). *See generally* Burnett v. State, 848 So. 2d 1170, 1172-1173 (Fla. Dist. Ct. App. 2003) (applying the SODDI defense in child pornography case).

110. *See supra* Part I.

computer.[111] Another tactic is to focus on how the evidence relating to the crime is stored on the defendant's computer. This tactic is particularly useful when dealing with child pornography cases, since those who collect child pornography tend to store their images in well-organized, hierarchical file structures.[112] In a child pornography case, if the images in question are carefully organized into directories and sub-directories, the prosecution can use this evidence of planning and attention to rebut the defendant's claim that he had no idea child pornography was on his computer.[113] The same is true if the files

111. *See, e.g.*, NEIL BARRETT, TRACES OF GUILT 148 (Bantam Press 2004). In his book, Barrett describes the analysis he undertook for British prosecutors who had charged "Gary Glitter," a British rock and roll star, with possessing child pornography; computer repair technicians had found child pornography on Glitter's laptop when he took it in for servicing. *See id.* at 139-140. *See also Gary Glitter*, Wikipedia, *at* http://en.wikipedia.org/wiki/Gary_Glitter (last visited July 17, 2004). Barrett's initial analysis of the data on the laptop showed that

> [i]t was in many ways a typical laptop structure, representing a non-computer expert's use for predominantly pornographic browsing. The laptop seemed to have been used 90 per cent of the time for access to paedophile-interest websites and only 10 per cent of the time as a tool to support the 'Gary Glitter' business.

BARRETT, *supra,* at 148. *See, e.g.*, People v. Timberlake, No. B163233, 2004 WL 928188, at *2 (Cal. Ct. App. April 30, 2004).

> The computers' hard drives were examined by Los Angeles Police Detective Alexander Moreno, a computer expert. One of the hard drives, a Hewlett Packard, contained 30,943 JPG images . . . . The "vast majority" were pornographic or sexual. Of the 30,943 images, 1640 involved juveniles or persons who appeared to be juveniles. Of those, approximately 1440 showed children or young adults 'striking various poses in various modes of dress and undress, some of them innocent looking, most of them seductive in nature.' The other 200 images depicted young children involved in sexual activity either with other children or with adults, including penetration and the child performing sex acts, such as oral copulation, on the adult.

Id. The court of appeals held that

> [t]he fact over 30,000 sexual images were discovered on the computer was highly relevant to prove Timberlake knew the images were on the computer**,** and had not been placed there by someone else, or by accident. . . . Evidence of the large number of sexual images was strong proof that Timberlake, rather than some other individual, was responsible for the child pornography found on the computer. The large number of images proved that only an individual with unfettered access to the computer, such as Timberlake, would have had time to place the material there. The evidence was also critical to demonstrate that the images did not appear on the computer by accident, i.e, by the computer user's mistyping a website address or a remote computer's surreptitious download of the material.

Id. at *4.

112. *See, e.g.*, BARRETT, *supra* note 111, at 15.

113. A defendant might try to claim that the lack of such organization is evidence supporting his claim that he did not knowingly acquire child pornography. *Cf.* BARRETT, *supra*

containing evidence of criminal activity are encrypted; the prosecution can cite the defendant's use of encryption to conceal the contents of the files as demonstrating clear consciousness of guilt.

4. Alibi Defense

Another response the prosecution can make to the assertion of a Trojan horse defense is to argue that it is, in effect, an alibi defense.[114] While this is not a response on the merits, it can ensure that the prosecution has an opportunity to prepare a rebuttal to the assertion of the defense, as the federal system and "more than forty states" require a defendant to give advance notice of his intention to raise an alibi defense.[115] Arguing that the Trojan horse defense is an alibi defense can also limit or preclude its assertion, at least in some jurisdictions, if the defendant has not provided timely notice as required by statute or court rule.[116]

But is the Trojan horse defense really an "alibi" defense? Traditionally, an alibi defense has been "based on the physical impossibility of a defendant's guilt by placing the defendant in a

note 111, at 147 (discussing child pornography in folders that were not well-organized or encrypted).

114. *See infra* note 116 and accompanying text.

115. LAFAVE ET AL., *supra* note 38, § 20.5(b).

> Most alibi provisions are similar . . . to Federal Rule 12.1. . . . [T]he government must issue a demand for notification, stating therein the time, date, and place of the alleged offense. If the defendant intends to raise the defense, he is required to respond within a specified number of days. His response must state the specific place . . . where he claims to have been at the time of the alleged offense and the names and addresses of the witnesses upon whom he intends to rely to establish his alibi.

Id. (notes omitted); *see also infra* note 116 & accompanying text.

116. *See, e.g.*, FED. R. CRIM. P. 12.1(e) ("If a party fails to comply with this rule, the court may exclude the testimony of any undisclosed witness regarding the defendant's alibi. This rule does not limit the defendant's right to testify."); *see also* COLO. REV. STAT. § 16-7-102 (2003):

> If the defendant intends to introduce evidence that the defendant was at a place other than the location of the offense, the defendant shall serve upon the prosecuting attorney as soon as practicable, but not later than thirty days before trial, a statement . . . specifying the place where the defendant claims to have been and the names and addresses of the witnesses the defendant will call to support the defense of alibi. . . . If the defendant fails to make the specification required by this section, the court shall exclude evidence offered in support of the defense of alibi unless the court finds upon good cause shown that such evidence should be admitted in the interest of justice.

Id. *See generally* Taylor v. Illinois, 484 U.S. 400, 412–23 (1988); Wardius v. Oregon, 412 U.S. 470, 473–74 (1973).

location other than the scene of the crime at the relevant time."[117] As was noted earlier, the Trojan horse defense is a variant of the real-world SODDI defense, in which the defendant claims that someone else committed the crime.[118] In raising a SODDI defense, defendants generally claim that they were "in a location other than the scene of the crime" when the "other dude" committed the offense.[119] This is consistent with the foundation of the defense—that someone quite unknown to the defendant committed the crime.[120] When a defendant admits to having been present at the crime scene, he or she can usually identify the perpetrator, by description if not by name.

Like the alibi defense, the Trojan horse defense shifts blame for the crime from the accused to another perpetrator which in this context can be either another individual (direct perpetration) or an automated process (*e.g.*, a program) that was created and released by another individual (indirect perpetration).[121] Unlike the alibi defense, the Trojan horse defense does not necessarily include a claim that the accused was not physically present at the crime "scene" when the offense was committed. This, however, is a distinction more of form than of substance because both defenses are based on the proposition that the accused *could not* have committed the crime because of certain circumstances beyond his or her control. In the alibi defense, the critical circumstance is his or her absence from the crime scene; in the Trojan horse defense, it is the accused's ignorance that malware has been installed on his or her computer and is causing it to engage in activities that are illegal.[122]

The functional parallels between the alibi defense and the Trojan horse defense suggest it is not unreasonable to apply the notice

117. BLACK'S LAW DICTIONARY 72 (7th ed. 1999); *see also* United States v. Chambers, 922 F.2d 228, 240 (5th Cir. 1991); People v. Muritok, No. CRA02-001, 2003 WL 23019178, at *7 (Guam Dec. 24, 2003).

118. *See supra* Part I.

119. *See, e.g.*, People v. Frize, No. E032988, slip op., 2004 WL 161498, at *2 (Cal. Ct. App. Jan. 28, 2004) ("Frize's now-proposed instruction was inconsistent with his defense, which was that he was not at the house while the crimes were being committed, in other words, a straight 'some other dude did it' defense."); s*ee also* United States v. Lively, 817 F. Supp. 453, 462-63 (D. Del. 1993).

120. *See, e.g.*, Gomez v. Duncan, No. 02 Civ. 0846 LAP AJP, slip op., 2004 WL 119360, at *34 (S.D.N.Y. Jan. 27, 2004) (describing "the 'some other dude did it' defense - last name unknown who was not seen by any witness").

121. *See supra* Part I.

122. These claims often incorporate a related proposition, namely that the accused's technological unsophistication not only prevented him or her from detecting the malware, but also meant that he or she would not have been able to remove or disable it if it had been detected.

requirements imposed upon the former to the Trojan horse defense. This conclusion is also supported by the applicability of at least some of the justifications advanced for requiring notice of an alibi defense:

> (1) alibi is a "hip pocket" defense, easily prepared for introduction in the final hours of trial and therefore more likely to catch the prosecutor by surprise; (2) a false alibi defense will be based on perjured testimony of third parties, which can be readily discouraged by affording the prosecution an opportunity to prepare for their testimony; (3) alibi requires an independent investigation by the prosecutor, and the failure to facilitate that investigation before trial will often necessitate a continuance during trial; and (4) alibi is the type of defense which will lead the prosecution to dismiss the charges if it determines from its pretrial investigation that the alibi witnesses are not lying.[123]

While all four justifications can apply to the assertion of a Trojan horse defense, the last two provide the most compelling support for extrapolating the notice requirement to this new defense. As explained elsewhere in this article,[124] rebutting a Trojan horse defense requires a great deal of investigation and preparation, much of which will have to be carried out by individuals who have technological expertise in computer forensics and related areas. Since many prosecutors are not knowledgeable in these areas and do not have ready access to the experts whose assistance they need, advance notice of the intent to raise a Trojan horse defense is essential if the prosecution is to have a fair opportunity to rebut it. Furthermore, if a prosecutor concludes, after being given a fair opportunity to investigate a Trojan horse defense, that the defense is valid, he or she will certainly dismiss the charges against the accused.[125]

Conceptually, then, advance notice should be required for the Trojan horse defense for the same reasons as, and to the same extent as, such notice is required for the assertion of an alibi defense. It should be noted, however, that because one can plausibly argue that the court rules and statutes which currently impose such notice requirements do not encompass the Trojan horse defense; because it is not included in the relevant provisions, prosecutors will be forced to rely on the argument analyzed above, i.e., that the Trojan horse defense is merely an alibi defense. Therefore, since extant statutes and court rules do not explicitly reference this new defense, a

123. LAFAVE ET AL., *supra* note 38 § 20.5(b).

124. *See supra* Part II.B.1–3; *see also infra* Part III.

125. *See supra* Part I.

defendant could still argue that (a) no advance notice is required or (b) even if advance notice is required, this requirement is not evident from the text of the statute or court rule; thus, it cannot be enforced to the defense's detriment. Therefore, to avoid unfairness to the defense or prosecution, jurisdictions should either amend their existing provisions to encompass notice of the Trojan horse defense or adopt new provisions that impose such a requirement.[126]

C. Summary

There are several tactics the prosecution can use to combat a defendant's invocation of the Trojan horse defense. One is to present evidence establishing the defendant's computer expertise. The prosecution can ask the jury to infer that one with his expertise would not have been the unknowing victim of malware. The prosecution may also use the defendant's technical expertise to suggest that the defense is a sham, that he is using it "to escape justice."[127] The defense may try to prevent the prosecution from introducing evidence concerning a defendant's computer expertise, along with efforts he took to protect his system from malware, by claiming the prosecution is attempting to utilize "character" evidence in violation of Federal Rule of Evidence 404(a) and comparable state provisions. The prosecution can respond by arguing that the evidence is admissible under the "other acts" provisions of Federal Rule of Evidence 404(b) and comparable state provisions.

As a general matter, the best way to attack a Trojan horse defense is to negate the factual foundation of the defense. Prosecutors can do this in two non-exclusive ways: one is to have the computer alleged to have been used in the commission of the offense subjected to a thorough forensic examination. If the examination finds no trace of malware, prosecutors can use this to rebut the defendant's

126. Interestingly, at least one state has adopted a statute which requires that notice be given of certain "defenses in offenses involving computes." *See* N.Y. CRIM. PROC. LAW § 250.30 (McKinney 2003).

127. J.D. Abolins, *Two Risks of the Trojan Horse Defense*, ZD Net, *at* http://reviews-zdnet.com.com/5208-6118-0.html?forumID=1&threadID=125&messageID=2529&start=-1 (Nov. 17, 2003).

> Good to keep torjan [sic] horses and other problem software off one's computer. But there are people who DO want to have Trojan Horses, worms, and viruses on their systems to rig a Trojan Horse defense. This leads to the two risks:
> 1. Innocent people implicated by action done by Trojan horses or by remote manipulation by others.
> 2. Guilty people using the claim of #1 to escape justice.

Id.

contention that a Trojan horse is responsible for the conduct at issue in the prosecution; if the examination finds malware, prosecutors should have their computer experts subject it to a thorough examination and analysis in an attempt to show that it could not have been responsible for the crime charged. The other way to negate the factual foundation of a Trojan horse defense is to use traditional investigative tactics, such as suspect interrogation, to obtain evidence that refutes the defendant's claim that he did not commit the crime(s) charged. Finally, prosecutors can argue that the defense qualifies as an alibi defense under Federal Rule of Criminal Procedure 12 and similar state rules and statutes. While this does not go to the merits of the case, by insisting that defendants give advance notice of their intention to invoke a Trojan horse defense, prosecutors can gain time to prepare an adequate rebuttal.

III. TECHNICAL ISSUES

In addition to the legal issues that arise from the Trojan horse defense, there are technical issues, which must be considered. For the most part, these technical issues are the result of investigators' needing to collect more evidence than they may have had to collect in other cases. This section will examine, with regard to these technical issues, (a) what the Trojan horse defense is, (b) what steps an investigator should take to counter a Trojan horse defense, (c) what should be done when malware is or is not found, and (d) what new skills and technologies are needed.

A. Defined

Before we discuss the technical issues associated with the Trojan horse defense, we will consider what the Trojan horse defense is from a technical perspective. We define *malware* as "a set of instructions that run on your computer and make your system do something that an attacker wants it to do."[128] The Trojan horse defense is the claim that an attacker ran instructions on the defendant's computer without his or her consent.

1. Malware

Malware can take on many forms. For instance, a Trojan horse is "a program that appears to have some useful or benign purpose, but

128. SKOUDIS & ZELTSER, *supra* note 2.

really masks some hidden malicious functionality."[129] A Trojan horse program may be named in such a way that the user thinks it is a normal program or it may be a simple game that a friend has e-mailed to the user. When the user executes it, the trojan performs actions that the user did not intend.

In some cases, malware will perform a limited set of tasks and will not have any interaction with the attacker after the infection. In other cases, the malware will contain a "back door" which is "a program that allows attackers to bypass normal security controls on a system, gaining access on the attacker's own terms."[130] Trojan horse and backdoor applications are sometimes referred to as being equal, but this is not correct.[131] While it is possible for a malware application to be both a Trojan horse and a back door, not all applications have both features. Some backdoor applications can allow an attacker to connect to an infected computer from over the Internet and control the infected computer. The attacker can delete files, download files, and do anything that a local user sitting at the keyboard could. When an attacker breaks into a series of computers, he or she will use some type of backdoor application to gain complete control of it. For example, in order to administer computers, companies use commercial programs that give a remote user full control of a computer.

One type of backdoor application involves the use of Instant Messaging ("IM"). When a user of instant messaging receives a malware executable file and runs it, they can become infected with a virus that will wait for commands.[132] The infected computer will join a chat room in an IM network, such as IRC and AOL Instant Messenger, and announce its presence. An attacker can wait for infected computers to join the chat room and send them messages to download or delete files.

Malware can also infect a computer from a web browser. When a web page is viewed, the server sends data to the local browser. The data could include code that the browser executes. Malicious code can add a website to the list of bookmarks and it can set a website as the default home page.[133] Such code could add a website with

129. *Id.* at 251.

130. *Id.* at 188.

131. *Id.*

132. Christopher Saunders, *Viruses Learn How to IM*, InstantMessagingPlanet.com, *at* http://www.instantmessagingplanet.com/security/article.php/2208441 (May 16, 2003).

133. SKOUDIS & ZELTSER, *supra* note 2, at 125.

pornographic material into the bookmarks of a computer and it would appear that the user intentionally bookmarked the site.

Finally, malware can cause a web browser to download files that are contraband. For example, a website, popup ad, or e-mail could have a photograph containing child pornography.[134] This will cause a web browser to download the picture and save a temporary copy of it to the local computer's cache. The user may not have intentionally downloaded the picture, but a copy of it exists on his or her system. In this example, a user may notice what happened and take steps to delete the temporary file, however, it is possible for the malware to display the full-sized picture in a scaled down size that the user does not see. In this case, a temporary copy of the file will exist, but the user will never have seen it.

2. The Bot defense

The Bot defense is not a separate defense; it is a version of the Trojan horse defense, one that is likely to appear in child pornography prosecutions.[135] Technically, it is a variation on the scenario noted at the end of the previous section, in which a website or a popup ad causes a web browser to download a picture and save a copy of it.

There is some difference between the Trojan horse defense and the Bot defense. One who invokes the Trojan horse defense claims to have been unaware that (a) a Trojan horse had installed itself on his computer and was using it for unlawful purposes and (b) he engaged in activity which led to the installation of the Trojan horse program. Those who invoke the Bot defense can claim (a) but have more difficulty with (b). They can claim that a bot downloaded illegal material, such as child pornography, to their computer without their knowledge but have to concede they knew they were engaging in activity that could result in a bot's doing so.[136] Therefore, someone who is charged with possessing child pornography can use a Bot

134. *See infra* Part II.A.2.

135. A bot (from "robot") is generally defined as

> [a]ny type of autonomous software that operates as an agent for a user or a program or simulates a human activity. On the Internet, the most popular bots are programs (called spiders or crawlers) used for searching. They access web sites, retrieve documents and follow all the hyperlinks in them . . . .
>
> A chatbot converses with humans (or other bots). A shopbot searches the Web to find the best price for a product.

"Bot," Hyperdictionary, *at* http://www.hyperdictionary.com/dictionary/bot (last visited July 17, 2004); s*ee, e.g.*, BotSpot, *at* http://www.botspot.com/ (last visited July 17, 2004).

136. For a definition of "bot," see *supra* note 135.

defense when he denies knowingly acquiring the child pornography but does not deny visiting chat rooms where child pornography is distributed.[137]

The defendant will claim that while visiting such a chat room, he accidentally and unknowingly triggered a file-bot that sent him the images.[138] To understand the factual basis of this claim, it is necessary to understand how these chat rooms operate. One or more participants will run bots that interface with the chat rooms.[139] When one of these individuals presses a button, the bot sends a message to the chat room announcing that child porn files will soon be sent out via email;[140] if those who are participating want to be added to the

137. *See, e.g.*, Commonwealth v. Robertson-Dewar, 829 A.2d 1207, 1209-1210 (Pa. Super. Ct. 2003) (concerning prosecution of individual who ran a file server program that offered child pornography on ten Internet Relay Chat (IRC) channels). These chat rooms are usually named in a code word, such as YG, which stands for young girls. It is unlikely that there will be a chat room entitled, "Free Child Pornography." This can lend further support to the defendant's claims because he can argue that it is not readily apparent that chat room YG contains illegal activity. *See, e.g.*, State v. Evers, 815 A.2d 432, 457 (N.J. 2003), *appeal after new sentencing hearing,* 845 A.2d 674 (N.J. Super. Ct. App. Div. 2004) (mentioning that defendant claimed to have "accidentally" collected child pornography). *See generally* United States v. Greathouse, 297 F. Supp. 2d 1264, 1267 (D. Or. 2003) (discussing a situation where a user known as cyotee "offered to exchange [child] pornographic images with an entire Internet Relay Channel.").

138. *See generally* James E. Farnan, Testimony Before the House Committee on Government Reform (May 15, 2003), *at* http://www.fbi.gov/congress/congress03/farnan051503.htm (May 15, 2003) (noting that the FBI has seen an increase in cases in which bots have been inadvertently installed on someone's computer).

139. *See, e.g.*, Jerry Ropelato, Cyberporn and Internet Safety, Presentation at Cyber Secrets Conference on Pornography at Brigham Young University (Feb. 18, 2003), *at* http://byubroadcasting.org/secrets/transcript/ropelato_transcript_2003.htm (last visited July 17, 2004).

> Chat is where you can have real time conversations in between 2 to 20 people all online at the same time. There's over 100 million people daily who use chat . . . . Now let's talk about what are the risks with chat . . . . Chat is just a playground for pedophiles . . . . Here's another chat risk – they're called bots, or robots. Bots are little programs that just run out there, and they'll actually communicate with people in a chat room, and here's a list here of about 20 chat bots, but there are literally hundreds of them. They're not all bad – some are more of an artificial intelligence. Here's an actual AOL instant messenger session, okay, an actual chat session going on here. Can you tell me by looking at these who are the humans and who are the bots? It's very difficult.

Id.

140. *See, e.g.*, Orin S. Kerr, *The Problem of Perspective in Internet Law,* 91 GEO. L. J. 357, 398 (2003) (describing how while undercover officer was logged into AOL chatroom devoted to child pornography "another chatroom visitor named 'Charbyq' sent an e-mail to everyone else in the chat room that included an attachment containing child pornography").

mailing list they must type a specific trigger.[141] Users in the chat room will usually see one or two lines that give the name and version of the bot and its author; the next line may say something like "child pornography server" or "really good images,"[142] while the fourth line will say "type '123' to get on" or "type 'I love good images' to get listed." When someone types the trigger, the bot sends the user a message letting him know he has been listed. After a certain period, the bot sends out the images, usually in one email at a time;[143] within minutes, every user who signed up will have an e-mailbox full of child pornography. They download these images to their hard drive, where they may be found and result in prosecutions for possessing child pornography.

The hypothetical defendant noted in the previous paragraph will respond by raising the Bot defense, to which the prosecution must respond in kind. The defendant will concede that he visited a chat-room in which the participants discussed child pornography but will contend that he did not intentionally download the images of child pornography that were eventually found on this computer and that gave rise to the prosecution. He may concede that he inadvertently triggered the bot which sent the child pornography to him, or he may claim that he was blameless, that the bot automatically sent the images to him. This is a variation of the Trojan horse defense because, like that defense, the defendant is asserting (a) that he did not engage in the conduct which constitutes the crime(s) with which he is charged or (b) that while he may have engaged in conduct which "technically" constitutes the crime charged, he did so without the *mens rea* required for the commission of the offense. The Bot defense is analogous to the Trojan horse defense in that the defendant claims automated processes acting without his knowledge or control

141. *See generally* Da Chronic, *AOHell v3.0 Rage Against The Machine*, Part II, *at* http://www.aolwatch.org/chronic2.htm (last visited July 17,2004).

> This feature is used to send messages to the chat room when certain 'events' happen in it. For instance, you can set it so that when a person enters the room, they are greeted with a message. You can also set it so AOHell automatically sends a certain message when someone says certain key words.

Id.; *see also* United States v. Gunderson, 345 F.3d 471, 472 (7th Cir. 2003) (describing how police used password to obtain child pornography via an Internet chat room); State v. Zabrinas, 24 P.3d 77, 80 (Kan. 2001) (describing how defendant requested to be on list for distribution of child pornography images).

142. *See, e.g.*, United States v. Pabon-Cruz, 255 F. Supp.2d 200, 212 (S.D.N.Y. 2003) ("Pabon posted an advertisement noting: 'Fine stuff here like: Preteen (black/asian/redheads/cumshots).' . . . Another ad in a similar chat room ('preteen666') stated that Pabon was 'Offering: Preteen (black/asian/redheads/cumshots)' . . . .").

143. *See, e.g.*, *Evers*, 815 A.2d at 437.

are actually responsible for the criminal conduct attributed to him. It differs from the Trojan horse defense in that (a) a different type of automated process forms the predicate for the defense and (b) the defendant must concede that he put himself at risk by frequenting a chat-room in which illegal activity was at least discussed. The first distinction is of little import with regard to the invocation and success of the defense; the second can undermine a defendant's ability to successfully invoke the Bot defense, especially when he uses it to negate *mens rea*, as the trier of fact may not be convinced that he did not intentionally acquire the images in question.

The best way for the prosecution to overcome the Bot defense—and any Trojan horse defense for that matter—is to have solid evidence of the defendant's knowledge and intent before filing charges against him.[144] The importance of being able to establish intent explains why many prosecutors will not file possession of child pornography charges against someone who had only a few images, the premise being that the possession could have been inadvertent.[145] In many cases, intent is readily apparent; many defendants will have vast collections of images that are stored in a variety of formats, with some printed out and organized in a photo album.[146] Absent such a collection, the prosecutor should insist that the investigator perform a forensic evaluation of the defendant's computer and any related media in an effort to find evidence showing defendant intended to possess child pornography. For example, if the investigator finds a CD-ROM containing images of child pornography and then finds the same images in unallocated space on the computer's hard drive, this shows defendant burned images that were originally on the hard drive

144. *See, e.g.*, Schwartz, *supra* note 17. One Department of Justice official noted that in child pornography cases, investigators could rebut the defense by finding "other corroborating evidence, like Internet communications with known pedophiles, or a stack of child pornography in the suspect's home." *Id*.

145. When a vast number of legal images are found, prosecutors realize that when a person "casts a wide net" they are bound to accidentally pull in "some" images which may not be legal.

146. *See, e.g.*, *Evers*, 815 A.2d at 457.

> The [trial court's] finding that defendant "apparently entered the particular chat room for child pornography by accident" is difficult to reconcile with defendant's confession that he knew of "hundreds" of child pornography web sites and interacted with many of them, including "under 15, 10, 11, 12 year old triple X [sic]." The sheer scope of defendant's knowledge of child pornography Internet sources and his affirmative acts of visiting those sites on a daily basis for a period of six weeks while requesting and disseminating such pornography belie the notion that defendant's descent into the world of child pornography was "accidental."

Id.

on the CD-ROM and deleted them from the hard drive.[147] Such conduct inferentially establishes that a defendant knew he possessed child pornography, and may have been trying to delete evidence.[148] Another prosecutorial tactic is to determine if the defendant subscribed to newsgroups related to child pornography (or to any other illegal activity with which he is charged). If he did, then the investigator may find that he saved chats in which the topic was child pornography. This evidence establishes the defendant's interest in child pornography, and his frequenting chat rooms where child pornography is freely traded indicates his interest in acquiring such material.[149]

While child pornography is a useful way to illustrate the use of a Bot defense because child pornography cases currently represent the majority of computer crime cases, the defense can be invoked for other types of computer crime as well. In other contexts, the invocation of the defense will likely be predicated on a defendant's accidentally triggering a file bot or mistakenly triggering a worm that was meant to test the security of his home network. If the prosecutor believes the conduct was not inadvertent, he or she may be able to use

147. In *Traces of Guilt,* Neil Barrett describes examining the hard drive of a laptop belonging to a man charged with possessing child pornography:

> There was a large group of . . . pictures, quite clearly illustrating sexual acts between adults and children, and between children. There was little doubt but that the vast majority of the picture collection . . . was indeed illegal. Moreover, the gallery showed multiple copies of a large number of the picture files. I could see that the pictures appeared in the Temporary Internet Files location – showing that they had been viewed as part of a web page – before then appearing in a second temporary file location, showing them downloaded from the Internet, and finally appearing in the folder collections that had first been detected by the PC World staff. After having made notes of around a dozen pictures that had followed that same programme of collection I was confident that I had reasonable proof of Internet paedophile behaviour.

BARRETT, *supra* note 111, at 149.

148. *See, e.g.*, State v. Anderson, No. 03CA3, 2004 WL 413273, at *4–*6 (Ohio Ct. App. Mar. 2, 2004).

149. In *Commonwealth v. Simone,* No. CRIM. 03-0986, 2003 WL 22994245 (Va. Cir. Ct. Nov. 12, 2003), the court held that evidence in the defendant's possession was sufficient to rebut his contention that pop-ups from a website were responsible for child pornography found on his computer. *See id*. at *4–*7 (Simone's possession "of stories involving graphic sexual activity of juveniles" in combination with the Internet search terms he used and the child pornography image he used as computer wallpaper refuted his contention.).

Another tactic that has been used to rebut a Trojan horse defense in child pornography cases is to establish a profile of how the defendant used the computer for lawful purposes and then use that profile to analyze how it was used for unlawful purposes. *See* BARRETT, *supra* note 111, at 151–152. If the pattern of use for unlawful purposes is identical to the pattern of use for lawful purposes, this can be used to infer that it was the defendant—and not malware or some other person—who was responsible for the unlawful activity at issue. *See id*.

other crimes and acts evidence under 404(b) to rebut the claims of mistake or accident.[150]

3. Summary

Computers can become infected with Trojan horse programs and other types of malware in various ways; they can arrive via e-mail, be acquired through Instant Messaging programs, or be downloaded when one visits a website. Attackers can use Trojan horse programs and other types of malware to take control of an unwary user's computer; these programs can also be set to download files—typically pornographic images—when someone visits a website. In both instances, the computer user may be completely unaware that he/she has had an encounter with malware. Websites, popup ads, and chat-room communications that automatically send files to computer users give rise to a variant of the Trojan horse defense known as the Bot defense. Used primarily in prosecutions for possessing child pornography, the Bot defense differs from the Trojan horse defense primarily in that the defendant, in a sense, exposed himself to risk by patronizing sites where child pornography was discussed and traded.

Most forms of digital communication have the ability to transmit Trojan horses or other types of malware, which can download files or change data. Many methods of infection require some type of user intervention, although e-mail viruses have shown users can be tricked into opening unknown files. The next section discusses the technical issues involved in the Trojan horse defense.

B. The Digital Crime Scene

The Trojan horse defense does not challenge specific techniques or technical procedures. Rather, it challenges either (a) the thoroughness of the analysis that is performed or (b) the impression that a thorough analysis was performed. A comparison with a common situation in the physical world better explains this: the digital investigation of a computer is similar to the physical investigation of a house or building. [151] The "entrances" and "exits" of the computer are its input and output devices, such as keyboards, mice, floppy disks, CD-ROMs, and the local area network or Internet. Each folder in a computer contains files, just as the rooms in a

150. *See supra* Part II.B.2.

151. *See* Brian Carrier & Eugene H. Spafford, *Getting Physical With the Digital Investigation Process*, 2 INT'L J. DIGITAL EVIDENCE 1, Fall 2003, at 1, *available at* http://www.cerias.purdue.edu/homes/carrier/forensics/docs/ijde_physical.pdf.

building contain physical objects. When digital files are deleted, they are placed in the equivalent to the dumpster. Files are added and removed from directories by programs, just like objects are added and removed from rooms by people.

Now consider a murder in which the victim is shot on a city street. The crime scene reconstruction shows that the shot was likely fired from a house across the street. The police look into the open window of the house and see the gun that meets the general requirements of one that was used to commit the crime. With only that knowledge, the owner of the house is arrested and charged with the murder.

There are obvious questions that would be asked in such a situation. Were the suspect's fingerprints found on the gun? Does the suspect have an alibi? Does the suspect have a motive? Is there evidence that the suspect shot the victim? Who owned the gun? Is there evidence that the suspect could shoot a gun? Is there evidence that the suspect was in his house at the time of the shooting? Is there evidence that other people were in the house at the time of the shooting? Is there evidence of forced entry into the house? Were the house doors and windows locked when the police searched the crime scene? These are basic and intuitive questions, the answers to which will determine whether the investigating officers conclude that the owner of the house is the one who shot the gun and that someone did not walk in from off the street and commit the murder.

Compare this with a virtual crime scenario where instead of bullets being used to attack someone, network packets are used, and the officers track the attack to a computer or Internet access account instead of to a building.[152] The computer is searched and evidence of network attack tools or contraband files is found. The owner of the computer is arrested. We should now ask the same questions as in the physical crime. Does the owner have a motive or alibi? Does the owner have the knowledge to commit the crime? Is there evidence

152. Neil Barrett, a British computer forensic expert, calls this the "scene-of-habitation" analysis:

> I realized that . . . there might be a way of adapting techniques used in other types of crime-scene analysis.
>
> Every scene of crime is also a place that has been occupied and lived in . . . . A murder room, for example, might be untidy. Did it become untidy as a result of the murderer's actions . . . . Is the arrangement of furniture, books and things intentional and therefore representative of the murderer? Or was it untidy before, in which case no interpretation of the murderer's actions and mentality can be made on the basis of the room?

BARRETT, *supra* note 111, at 141.

that the owner committed the crime? Was the computer secured? Is there evidence of forced entry into the computer? Is there evidence of other users accessing the computer? The recent cases described in Part I represent instances where the defense has convinced a jury that the investigators have not sufficiently answered these types of questions.

C. Standard Operating Procedure

These challenges require that investigators perform a comprehensive investigation and evidence search at the crime scene. In the past, a computer search focused on the existence of specific items and not on how they got there. Consider the National Institute of Justice's *Electronic Crime Scene Investigation: A Guide for First Responders,*[153] which lists expected types of electronic evidence based on the particular type of crime being investigated.[154] Only the list for computer intrusion crimes includes configuration files as an expected type of evidence,[155] yet it is configuration files that will show if there are malware programs on the system that run when it is started. Therefore, it was expected that, for example, a contraband image investigation would be interested in images and image software and not the configuration of the system, which may show if a backdoor existed that could have been used to plant the images.

In the physical crime scene investigation previously described, before a law enforcement officer concludes that the owner of the house is the person who shot the gun, the officer would want to check the entry and exit points to find evidence of forced entry and evidence showing who had entered and left the building. The same should be done for a computer. Examples of entry and exit points for a computer are the devices that are used when someone physically sits in front of it. An investigator should check what mechanisms exist to prevent people from sitting in front of the computer and using it. Was there a password and was it difficult to guess? Are there any keystroke loggers that may have recorded what was typed? Are there any logs that show what was typed from a keyboard instead of from a remote host? The perpetrator can stage a digital crime scene, so the

153. NATIONAL INSTITUTE OF JUSTICE, ELECTRONIC CRIME SCENE INVESTIGATION: A GUIDE FOR FIRST RESPONDERS (2001), *at* http://www.ncjrs.org/pdffiles1/nij/187736.pdf.

154. *See id*. at 37–41 (listing auction fraud, child exploitation, computer intrusion, death investigation, domestic violence, economic fraud, e-mail threats/harassment/stalking, extortion, gambling, identity theft, narcotics, prostitution, software piracy and telecommunications fraud as among the types of evidence to be expected).

155. *Compare id*. at 38 *with id*. at 37, 39–41.

investigator must also look for evidence that the logs or other digital data were tampered with; such evidence can take the form of inconsistencies in missing files, missing or incorrect log entries, or file times. An investigator should also look for physical evidence around the computer that is related to the crime. Evidence from these sources may help to show that the perpetrator had physical access to the computer, even if malware is found.

Another entry and exit point in a computer is access to a network, which can be a corporate network or a home Internet connection. To examine these entry and exit points, the investigator must identify which applications can connect to other computers on the network and which applications can accept connections from other networked computers. A search for applications that can initiate connections to remote systems may show which ones had the ability to create a suspect file. A search for applications that can receive connections from remote systems may show those that allowed an attacker to gain access and control of the computer. These applications are similar to the doors and windows of a building and each will have varying amounts of security to prevent an attacker form gaining access.

For malware to operate, it needs to be started. Some malware works by looking like another application so that the user starts it by accident. Another method is adding itself to the list of applications that are started every time the computer is booted. This is common for malware applications that can receive network connections and allow an attacker remote control of a computer. The investigator should examine the startup configuration files for the computers to identify unknown programs.

Anti-virus scanning software can also be used to detect known malware. The software will scan the system being analyzed just like it does to a desktop system and look for signatures of malware that has been seen before. Previously, this was difficult during a forensic analysis because the anti-virus software expects to scan the hard disks on the local system. Many investigations occur with special software that reads a file that corresponds to a hard disk, but there does not have to be an actual hard disk mounted in the system. New Microsoft Windows-based products such as the EnCase Virtual File System module[156] and Mount Image Pro[157] allow investigators to use existing

156. *EnCase Virtual File System*, Guidance Software, *at* http://encase.com/products/modules/EnCaseVFS.shtm (last visited July 17, 2004).

Windows anti-virus software,[158] while anti-virus software for the Linux operating system[159] also provides another method for detecting malware. However, some corporations use commercial backdoor[160] software to monitor employees or to gain remote access to fix computers, causing those types of software to possibly go undetected by some anti-virus software.

Because any crime scene can be staged to thwart an investigation, the crime scene must be processed in such a way that the inconsistencies from the staging can be detected. This requires extensive knowledge about the behavior of applications to know what evidence should exist after an event. Unfortunately, this is difficult with many software applications because the behavior can change with every new version of software and the expected behavior is not well documented. Much of the focus has been on the existence of inculpatory evidence of an event, but these cases have shown that all exculpatory evidence that may show that an event did not occur must also be identified.

Ultimately, while the burden should be placed on the defense to show where the malware is and how it could have been used in the crime, a thorough initial investigation by the prosecution can help to ensure that the correct person is identified. If standard operating procedures are thorough and include steps to detect malware, then an investigator can testify that he or she performed the steps. This may decrease the impact of a Trojan horse defense unless the defense can produce evidence.

157. *Mount Image Pro*, Get Data Pty. Ltd., *at* http://www.mountimage.com/ (last visited July 17, 2004).

158. *See, e.g.*, Central Command, *at* http://www.centralcommand.com/windows_products.html (last visited July 17, 2004); Computer Associates, *at* http://www.my-etrust.com/ (last visited July 17, 2004); FRISK Software International, *at* http://www.f-prot.com/ (last visited July 17, 2004); F-Secure, *at* http://www.f-secure.com/ (last visited July 17, 2004); McAfee, *at* http://www.mcafee.com/ (last visited July 17, 2004); SOFTWIN, BitDefender, *at* http://www.bitdefender.com/ (last visited July 17, 2004); Sophos, *at* http://www.sophos.com/ (last visited July 17, 2004); Symantec, *at* http://www.symantec.com/index.htm (last visited July 17, 2004); Trend Micro, *at* http://www.trendmicro.com/ (last visited July 17, 2004).

159. *See, e.g.,* Central Command, *at* http://www.centralcommand.com/linux_products.html (last visited July 17, 2004); FRISK Software International, *at* http://www.f-prot.com/ (last visited July 17, 2004); F-Secure, *at* http://www.f-secure.com/ (last visited July 17, 2004); SOFTWIN, BitDefender, *at* http://www.bitdefender.com/ (last visited July 17, 2004).

160. *See supra* Part III.A.1.

D. What To Do When Malware Is Found

When an investigator finds an application she suspects is malware, the investigator must try to identify the capabilities of the application. It is a difficult task to analyze an application since it requires extensive programming knowledge, which many law enforcement investigators may not have. Fortunately, the anti-virus vendors have examined many of the known malware applications and provided the information on their websites. The investigator should use all available resources to determine if a remote person could have used the application to commit the crime or to install additional software that could have committed the crime. Furthermore, the investigator should identify how the malware was installed on the system, when it was installed, and if it was ever run.

The nature and design of computer systems may prevent an investigator from being able to testify that a backdoor or Trojan program did not install a contraband file. Instead, it is better to find evidence to show that a specific user downloaded the file. This evidence may come from logs from the Internet service provider that show the network traffic that downloads the contraband files but does not show network traffic to a malware application. The evidence may also come from physical access evidence, such as passwords or web sites that are on notes around the computer.

E. What To Do When Malware Is Not Found

It is technically possible that a malware program was installed but has been removed and no evidence of it exists. Normally, when a file is deleted, the data associated with it will still exist on the computer until it is overwritten by normal system usage.[161] The data associated with the malware could have been deleted and overwritten by the time that the investigation occurs. This is not unlike physical evidence at a crime scene being lost because of weather or normal activity.

To prevent deleted data from being recovered, special "wiping" tools exist that will manually overwrite the data in a file before the file is deleted.[162] When these tools are used, the data that will

161. *See, e.g.*, United States v. Sanchez, 59 M.J. 566, 570 (A.F. Ct. Crim. App. 2003) (describing how investigators used a program called "Carve This" to uncover remnants of files that were deleted and overwritten on defendant's hard drive).

162. *See, e.g.*, BCWipe, *at* http://www.jetico.com/ (last visited July 17, 2004); Eraser, *at* http://www.heidi.ie/eraser/ (last visited July 17, 2004); R-wipe & Clean, *at* http://www.r-wipe.com/ (last visited July 17, 2004); Sdelete, *at*

eventually be overwritten by the computer is not related to the original file content. The Caffrey defense claimed that these types of tools were used to remove the Trojan files from his computer.

Although some operating systems will wipe files by default, most currently do not. A special application would be needed to wipe other files. If an attacker is going to remove all traces of their attack, they will also need to delete the files associated with the wiping tool. Because the wiping tool cannot delete itself, the normal delete functionality will need to be used and the wiping tool may still be recovered if the computer has not overwritten it when the investigation occurs.

Operating systems create various copies of data in the form of temporary files and in memory. The data stored in memory is lost when a computer is powered off, so it is not frequently used in an investigation. However, when the memory is full of data, some of the data is saved to the swap space on a hard disk so that new data can be saved to memory. The data in the swap space will exist after the computer is powered off, so it can be used to find evidence that was in memory. If the operating system does not wipe data by default, the temporary files and swap space may contain evidence of malware or the secure wiping tool.

Finally, wiping tools can leave signatures behind. For example, the low-level file system structures may show signs that a wiping tool was used because one of the entries is all zeros or has invalid data. Consider a table where each entry is made in an increasing numerical order. If entry 20 is all zeros and entries 1 to 19 and 21 to 294 have valid data in them, then entry 20 may have been wiped. The signatures of file wiping will be overwritten by normal system activity,[163] so the time between the incident and the investigation will be important when determining what data existed on the system at the time of the incident.

Even if no malware has been found and signatures of wiping tools have been found, we cannot immediately conclude that malware, which wipes itself from the computer, was responsible. Those concerned about their privacy or corporate secrets will use wiping tools to remove sensitive data from their computer in case it is stolen. Those involved in illegal activity, such as downloading

http://www.sysinternals.com/ntw2k/source/sdelete.shtml (last visited July 17, 2004); Wipe Disk, *at* http://www.birdcomputer.ca/Software/SoftwareToC.html (last visited July 17, 2004).

163. If we consider the previous table example, entry 20 could be reused by normal activity and the signature would be erased.

contraband, will use wiping tools to remove traces of their activity. In both of these cases, the signatures of wiping tools could be the result of the user wiping non-malware data, and malware may not have existed on the system.

F. New Skills and Technologies

To determine how digital evidence was created, an event reconstruction process must occur. This process will try to determine if evidence was created by a user sitting in front of the computer or by an attacker using a backdoor. Unfortunately, little attention has been paid to digital crime scene event reconstruction. Although research has begun, it is not yet practical since the comprehensive analysis of systems to detect and analyze malware requires skills that many investigators do not possess and requires technology that does not exist in an easy to use fashion. [164]

Computer forensic labs will be necessary to identify the capabilities of an unknown application. In the physical world, an investigator can look at an unknown physical object and get a rough idea about what it does. However, an unknown application is like an unknown gas or liquid; scientific techniques are needed to identify what it is and what it can do. The process of identifying the capabilities of an application is known as "reverse engineering," and books have only recently begun appearing on the topic.[165] While not all investigators will have to possess these skills, all must have access to someone who does.

To understand the process, imagine that you buy a kit to build a car. Every screw, wire, hose, and piece of metal is separated. You have an instruction manual that is hundreds or thousands of pages long. The manual has steps such as "Use bolt 13284 to fasten plate 482b-9 to widget 1320-a" and the only pictures are those in an index that show which bolt is number 13284. There is no final picture and no intermediate picture—only thousands of instructions.

The reverse engineering process of an application is equivalent to an investigator's receiving only the inside pages of the instruction

164. See, e.g., Megan Carney & Marc Rogers, *The Trojan Made Me Do It: A First Step in Statistical Based Computer Forensics Event Reconstruction*, 2 INT'L J. DIGITAL EVIDENCE, Spring 2004, at 1, *available at* http://www.ijde.org/current_home.html; Brian D. Carrier & Eugene H. Spafford, *Defining Event Reconstruction of Digital Crime Scenes*, 49 J. OF FORENSIC SCI. (forthcoming November 2004); Pavel Gladyshev & Ahmed Patel, *Finite State Machine Approach to Digital Event Reconstruction*, 1 DIGITAL INVESTIGATION 130 (2004).

165. *See, e.g.*, SKOUDIS & ZELTSER, *supra* note 2, at 125; *see also* CYRUS PEIKARI & ANTON CHUVAKIN, SECURITY WARRIOR (2004).

manual for the car kit and having to determine what the manual is for because the front cover is missing. Using the pictures of the individual parts in the index and the instructions, the investigator may realize that there are wheels and an engine so that it is probably some type of land-based vehicle, but maybe some of the pieces of metal will be formed into something that can also fly or float. All of the instructions must be examined to determine if this is the case. With reverse engineering, an investigator can identify the basic properties of an application, but a detailed examination of the computer instructions are needed to identify all capabilities.

New technologies are also needed to make the reverse engineering process easier. Now, it is largely a manual process of reading each instruction; new technologies could help to produce a higher-level view of the application. To return to our car kit example, a higher-level view of the process could reduce the 150 steps needed to build a steering wheel into a single "build steering wheel" action. This technology will make reverse engineering more accessible to investigators.

IV. CONCLUSION

Our experience with the Trojan horse is in its infancy, but it is, after all, merely a new incarnation of the SODDI defense. It may well be, as was suggested earlier, that the success the defense has so far enjoyed will be a transient phenomenon, a product of the general public's current unfamiliarity with computer technology and online activity.[166] The verdicts in the Caffrey and Pitts cases suggest this is the case since the results in both completely defy the common sense reasoning jurors are presumed to bring to their deliberations.

If this is true, the Trojan horse defense is a variant on a phenomenon we have seen before: the defense's use of complex, arcane technology to unsettle jurors and lead them to find reasonable doubt where there is none. One way prosecutors can respond to this tactic is by de-mystifying the technology at issue, thereby helping the jury understand that the mere possibility that something *could* have happened is not, in and of itself, enough to establish reasonable doubt

166. In the United Kingdom, the success of the Trojan horse defense led some to call for a debate on "'[T]he need for specialist judging panels or juries that would allow for a more complete understanding of the evidence brought forth in technology-based trials.'" Daniel Thomas, *Call for Specialist Technical Judges after Teenager Is Cleared of Attack,* ComputerWeekly.com, *at* http://www.computerweekly.com/Article125951.htm (Oct. 28, 2003) (quoting Richard Starnes, Director of Incident Response for the Managed Security Operations at Cable & Wireless).

in a criminal trial.[167] Another way is to anticipate the possibility that such a defense may be raised and have the computer(s) in question thoroughly examined by forensic experts to ascertain if there is any evidence of malware on them and, if there is, to determine if the malware could have done what it is claimed to have done.

167. Such a possibility is not sufficient to establish reasonable doubt in prosecutions based solely on real-world activity. *See, e.g.*, Brimmer v. State, 29 S.W.3d 497, 513 (Tenn. Crim. App. 1998) (stating that in closing, prosecutor argued that "[t]here is . . . the Soddi defense . . . . Some other dude did it. Who? . . . It's easy though to fantasize. One could fantasize anything. One could fantasize Martians coming down and doing it. But that's not what the proof in this case is. I trust you to use your common sense").