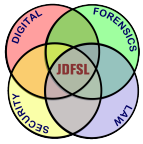

THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 9 | Number 4

Article 4

2014

Technical Soddi Defenses: The Trojan Horse Defense Revisited

Chad M. Steel
Steel George Mason University

TECHNICAL SODDI DEFENSES: THE TROJAN HORSE DEFENSE REVISITED

Chad M. S. Steel
George Mason University
MS 2B5
Fairfax, VA 22030
csteel@gmu.edu

ABSTRACT

In 2004, the Trojan horse defense was at a crossroads, having been successfully employed in two child pornography cases in the United Kingdom, resulting in acquittals. Despite the early successes, the Trojan horse defense has failed to become a regularly employed strategy. The original Trojan horse defense has now become part of the more general technical SODDI (Some Other Dude Did It) defense, which includes the possibility of unknown actors using unsecured Wi-Fi connections or having physical access to a computer to perform criminal acts. In the past ten years, it has not been effective in the United States for criminal cases, with no published acquittals in cases where it was the primary defense. Where the technical SODDI defense has been successfully used as leverage in plea negotiations, there has been either poor forensics performed by the prosecution or political pressure to resolve a matter. On the civil side, however, the defense has been wildly successful, effectively shutting down large John Doe copyright infringement litigation against non-commercial violators.

Keywords: SODDI defense, Trojan horse, copyright infringement

1. INTRODUCTION

In 2004, Brenner et al visited the use of the Trojan horse defense in court, citing two recent cases in the United Kingdom where reasonable doubt was successfully established. In their seminal review, they speculated that:

> 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 (Brenner, Carrier, & Henninger, 2004).

In the decade that followed, the defense has evolved and, consistent with the prediction above, has failed to become a successful, mainstream strategy in criminal matters. Despite increases in computer literacy for judges and juries and an increased prosecutorial and investigative awareness of the defense, it is still occasionally employed, although it has not become a commonplace strategy.

The Trojan horse defense and the more general technology-driven SODDI (Some Other Dude Did It) defense are raised most frequently in child pornography cases, though variants have been successfully employed in civil litigation related to copyright infringement. On the criminal side, the defense has been largely unsuccessful, though on the civil side, specifically in cases of copyright infringement, it has been employed more fruitfully.

This paper examines the current state of the Trojan horse defense, and the related,

more frequent employed, technical SODDI defense, which can include blaming an unknown actor for using anything from a single computer with multiple accounts to an open wireless access point. It examines United States case law for the past ten years, and provides an analysis of the current and future state of the technical SODDI defense.

2. TYPOLOGY OF TECHNICAL SODDI DEFENSES

Trojan horses are a form of malware named after the legendary Greek ploy to enter the city of Troy. The term refers to a particular type of malware that masquerades as innocent software but contains malicious code inside that entices a victim to install it on their system (Landwehr, Bull, McDermott, & Choi, 1994). For the purposes of the Trojan horse defense, the malware involved does not necessarily meet the strict definition of a Trojan horse, but may be a virus, worm, spyware, or even legitimate software that facilitates an unauthorized remote or local access.

At its heart, the Trojan horse defense is simply a variant of the age-old SODDI strategy. The strategy is to blame the digital activities under investigation on another actor, either known or unknown (Lubet, 1992). The Trojan horse defense is the most common form of the technical SODDI defense, but other forms of the defense exist. The actor in question in the technical SODDI defense may be a person, malware, or a combination of both.

In general, the technical SODDI defense can be broken into a taxonomy based on the type activity that is being put forth as evidence. While the base defense is the same, the strategy relies on different actors and motivations (if motive can be indirectly ascribed to malware) based on the type of offense. Case law can be broken up into two separate areas of offense–traditional Trojan horse defenses, which blame the actions on software, and the more general technical SODDI defenses, which blame the actions on an unknown actor that may be either a person or malware.

3. TRADITIONAL TROJAN HORSE CASES

Traditional Trojan horse cases generally rely on forensic evidence to cast doubt that the actions ascribed to a defendant's machine were performed by the defendant. They sidestep the issue of "putting the defendant at the keyboard" by blaming malicious code running on the machine for the observed actions. The two common defense approaches are to forensically identify malware currently on the machine (or previously present on the machine), or to find that sufficient malware protection was not in place at the time of the events of interest.

Traditional Trojan horse cases can be broken up into two categories–content-related cases, where the malware is blamed for the presence of contraband on a system, and illegal access/system interference cases where the malware is blamed for some activity associated with a system. In cases where both claims are made, the claim associated with the primary activity being charged is used to classify the case.

3.1 Content-Related Cases

Content-related cases are those where the presence of material on an individual's digital media form the basis of the criminality. The primary crime involved in these cases is child pornography possession.

The general standard for possession of contraband was set by *United States v. Kuchinski* (*US v. Kuchinski*, 2006), a child pornography possession case. In the case, Kuchinski was found to have approximately 19,000 images of child pornography in his Temporary Internet Files directory, both active and deleted, and was charged with

possession and receipt of child pornography. On appeal, the court held that Kuchinski could not be charged with possession of the temporary files, finding:

> Where a defendant lacks knowledge about the cache files, and concomitantly lacks access to and control over those files, it is not proper to charge him with possession and control of the child pornography images located in those files, without some other indication of dominion and control over the images.

Post-Kuchinski, possession of contraband requires that the prosecution show the defendant had knowledge about the existence of content on a device and access to a mechanism to affect that content. This case would at first appearance tend to support a technical SODDI defense, requiring the prosecution to show that the defendant had knowledge of the presence of child pornography on a computer. The courts have narrowly applied Kuchinski in relation to technical SODDI defenses, however.

In *Wise v. State of Texas* (*Wise v. State*, 2012), Wise was convicted of the possession of child pornography based on deleted images found in free space on his computer. The conviction was overturned on appeal, based on Wise's double defense that (1) there were viruses found on his computer, and the viruses could have downloaded the child pornography, and (2) the computer was purchased at a flea market and the previous owner could have downloaded the child pornography. The appellate court's decision was similarly overturned and the trial court's decision held. The court found neither count credible, opining that "placement of a pornographic image on the free space of a computer would be inconsistent with the purpose for placing a virus on a computer", and that the testimony about previous owner came from the defendant's brother and lacked specificity, leading to a reasonable possibility of bias. The court further held that finding an extensive collection of child erotica and browser activity related to child pornography were sufficient grounds to overcome the Trojan horse defense and to uphold the original conviction.

In several content-related cases, the technical SODDI defense has been made before proceeding to trial. In at least one case, a defense forensics team conducted an analysis and made use of the press prior to trial, potentially facilitating a plea agreement. In *State of Arizona v. Bandy* (*State of Arizona v. Matthew Bandy*, 2005), the defendant, the then 16-year-old Matthew Bandy, was charged with uploading child pornography to a Yahoo! group and with possessing the child pornography that was found on both his computer and on a CD in his home. The defense hired Tami Loehrs to perform a forensic analysis. Loehrs identified what she believed to be Trojan horse software on Bandy's computer, and concluded that it "is common for a person that views child pornography to store the images on an innocent person's computer". A subsequent forensic analysis found that, while there was malware present, it was installed after the dates of the child pornography offense and did not contain the functionality to surreptitiously download child pornography. The examination further identified web searches consistent with child pornography activity and registration information linking Bandy and the online Yahoo! account. Bandy ultimately pleaded guilty to three counts of distributing pornography to a minor. The prosecutor's office ultimately concluded:

> In light of the circumstances surrounding this case–such as the age of the juvenile and his lack of prior criminal conduct–we felt 90 years was disproportionately harsh and offered a plea bargain allowing Bandy to plead guilty to the lesser

charge of distributing pornography to minors. Bandy accepted this agreement (Alexander, 2007).

In *United States v. Kerr* (*US v. Kerr*, 2006), Kerr was identified by the FBI when he offered child pornography through Internet Relay Chat (IRC). Kerr provided the address of a server he hosted in the chat room, offering to allow anyone who first uploaded a contraband image to download child pornography. An FBI special agent was able to download an image depicting sexual activity between pre-teen minors, and an analysis of Kerr's computer found child pornographic images present. In a twist on the Trojan horse defense, Kerr claimed that he was actually *writing* a virus, for which he would use the child pornography as a distribution vector. The planned virus would allegedly infect and damage the machines of pedophiles. The forensic analysis of Kerr's machine found, however, no evidence that he was writing any such virus and Kerr's conviction was upheld.

Although there have yet to be any malware defenses brought forth in court that have identified specific malware associated with child pornography, at least one virus made claims of *finding* child pornography already present on a computer. The Reveton ransomware virus would infect a machine and claim to be from the FBI, "identify" child pornography on the machine, and then request the user pay a fine online. While the virus did not place any actual child pornography on machines, one user, Jay Riley, went to his local police department asking if he was wanted on child pornography charges after being infected with the virus. After Riley allowed police to view his machine, they found child pornography on it and he was arrested (Matyszczyk, 2013).

3.2 Illegal Access/System Interference Cases

In illegal access/system interference cases, the Trojan horse claim is that malware was installed on the computer of a defendant or used to take over the account of a defendant. That computer or account was then used as a launch pad to conduct illegal activities. The activities may have been the direct result of the malware, with the malicious code automatically retrieving content, or indirectly the result of the malware, with the malicious code facilitating remote access for a human attacker.

In *United States v. Miller* (*US v. Miller*, 2008), Miller was found to be in possession of a Zip disk containing approximately 1,200 images of pornography, of which 20 were child pornography. Miller claimed to have no knowledge of the images, and presented a two-part Trojan horse defense. In the first part, Miller claimed that he previously had a virus on his machine that may have downloaded the images on his behalf (a stored content claim). In the second portion of the claim, Miller stated that he had been the victim of credit card fraud and that the accesses to websites may have been because "someone may have gotten access to his 'log ons' and credit card numbers". The court rejected both arguments. The digital forensics report showed multiple accesses to the Zip disk to copy child pornography. Additionally, the defendant admitted to acquiring the adult pornography on the disk, which the forensics showed was copied concurrent with the child pornography.

In *United States v. Gardner* (*US v. Gardner*, 2012), Gardner was charged with both possession and distribution of child pornography. Part of the defense strategy was to claim that either the defendant's brother was responsible (he had access to the computer and the defendant had bookmarked his online account to allow automatic logins) or a virus found on the computer was responsible. The court reviewed the report of the computer forensics expert presented by the defense, and denied the inclusion of the portions related to a possible Trojan horse defense, stating:

> Absent any evidence (other than the speculation offered by the Defendant) that a third party hacked into the Gardner family computer to download the offending images, [the defense expert's] conclusion is, at best, not relevant, and would confuse the jury.

One of the most reported illegal access/system interference cases employing a technical SODDI defense never made it to trial. Michael Fiola, a then-employee of the Massachusetts Department of Industrial Accidents, was charged with possession of child pornography on his State-issued laptop in August 2007. The charges were based, in part, on an examination of the laptop by State IT staff following unusually high Internet activity associated with the machine. The examination purported to find child pornography and web activity associated with child pornography. The charges were dropped in 2008, but Fiola was still terminated (Sweet, 2008).

The only publicly available examination of Fiola's computer was performed on behalf of the defense, and while it concludes there was malware present on the system, the malware cited is not known to be associated with child pornography. Statements in the report such as "Since BBS's have not been active in almost 20 years, the use of this term as a current search term makes no sense and seems suspicious" regarding the term "sun Lolita bbs" exhibit a poor understanding of the terms used by child pornographers (Steel, 2009), and far reaching conclusions such as "I can say with 100% certainty that the Laptop was compromised by numerous viruses and Trojans and may have been hacked by outside sources" are beyond those that can be drawn from the information available in the forensic report (Loehrs, 2009). On the other hand, the IT examination done by the State is not available, and the administrative investigation was not performed by forensic specialists, so no definitive conclusions can be drawn regarding the state of compromise in the case.

In *State of Connecticut v. Amero* (*State of Connecticut v. Amero*, 2007), a substitute teacher, Julie Amero, was initially convicted on four counts of endangering the welfare of a child for allowing her seventh grade class to see pop-up ads containing adult pornography. The prosecution claimed that Amero visited pornographic websites on the classroom computer that was visible to her students. During the initial trial, the defense was prevented from putting forth a theory that malware caused the pop-ups (Green, 2008).

A review of the court transcripts and a forensic examination of a logical drive image (the original drive was never forensically imaged and had been accessed after the incident) were conducted by an independent group of forensics experts. They concluded that the testimony provided by the prosecution's expert witness was in error, and that their forensic analysis was not performed in accordance with industry best practices. The group further concluded that the machine was infected with adware, and that it would pop up ads related to search terms entered and sites visited by the user. Further, a site visit by Amero to what could reasonably have been mistaken for a site on hairstyles was found to have pornographic material present. Additionally, the close proximity of the load times for the pornographic material was consistent with an automated retrieval (Eckelberry et al., 2007). In 2007, the appellate court vacated the conviction based on false facts presented during the trial and Amero ultimately pleaded to a single court of disorderly conduct (Green, 2008).

In *United States v. Solon* (*US v. Solon*, 2013), Solon was convicted of possession and attempted receipt of child pornography in 2008. Solon was initially identified by the Wyoming Internet Crimes Against Children (ICAC) taskforce after he used Limewire to

download five movies containing child pornography. Solon's computer was seized, and a forensic analysis confirmed the presence of the child pornography movies on his computer. The defendant admitted to installing Limewire and using it to download "Grand Theft Auto", but not to downloading the child pornography. The defense asserted Solon's computer was compromised by malware, leading to the downloads (Associated Press, 2009). A jury found Solon guilty, and the conviction was upheld on appeal.

In one of the more audacious illegal access/system interference cases, David Goldstein was charged with felony possession of child pornography following an attempt to frame two other individuals for the same offense. Goldstein, a mental health patient, allegedly posted links to child pornographic images in online forums using the names of Timothy Jerman, a Vermont state representative, and Dr. Stuart Graves, a mental health professional. Graves was associated with a facility that Goldstein had previously been admitted to, and Jerman's wife worked as a nurse at the same facility. The "distribution" was reported to the Internet Crimes Against Children taskforce by Goldstein. Goldstein never obtained physical or virtual access to the devices owned by Jerman or Graves, so there were no forensic ties to their machines and the police quickly cleared them and identified Goldstein, who used his own email to register fake profiles he used to post the images (Moats, 2010).

4. TECHNICAL SODDI CASES

The more general technical SODDI cases are similar to illegal access/system interference cases, but the defendant claims that an unnamed individual used their Wi-Fi connection (which is generally unsecured) or their computer to commit the charged offenses. The technical SODDI defense has only been used occasionally in criminal cases, but it has been used extensively in civil litigation related to copyright infringement and intellectual property theft.

4.1 Illegal Access/System Interference Cases

Individuals who have their connections hijacked or their computers used by another individual for illegal purposes rarely end up in court, with the confusion generally resolved prior to indictment. They have, however, been subject to erroneous and invasive searches and seizures in several cases. While many of the cases involve content-related offenses, the defenses put forth are based on illegal access.

In *United States v. Smith* (*US v. Smith*, 2014), Smith's laptop was identified as having downloaded 26 child pornography movies to his local hard drive using the peer-to-peer client Frostwire. The defense presented the case that one of Smith's roommates, who also had access to the laptop, had downloaded the child pornography. The jury convicted Smith, but the district court entered an acquittal based on insufficient evidence of guilt being presented. The jury's conviction was upheld on appeal, with the appellate court ruling that the jury was allowed to determine Smith's guilt based on their assessment of the testimony of the roommates.

In other cases, individuals used their roommate's computer to commit offenses. In *United States v. Moriarity* (*US v. Moriarty*, 2005), Moriarity admitted to using his roommate's computer to access child pornography, which he later attempted to distribute in return for money. In *Commonwealth v. Robertson-Dewar* (*Com. v. Robertson-Dewar*, 2003), the defendant admitted to using both his roommate's computer and his roommate's Penn State account to download child pornography. In *United States v. Holness* (*US v. Holness*, 2013), Holness used his roommate's computer to obtain a $500,000 life insurance policy on his wife, who he was subsequently

convicted of murdering. None of these cases resulted in any charges against the computer owners, however, indicating that investigators and prosecutors were able to recognize that the owner was not likely the perpetrator of the criminal acts prior to indictment.

A confession to being the "mysterious stranger" in a technical SODDI defense is not sufficient, however, to assign guilt. In one of the more unusual technical SODDI defenses, *People v. Lindstrom* (*People v. Lindstrom*, 2009), Steven Lyle Lindstrom wrote a letter taking responsibility for downloading child pornography using his roommate's computer. Lindstrom later admitted his "roommate generally told him what to write, and he had confessed to something he did not do. He made the false confession because his roommate and the roommate's girlfriend helped defendant [sic] when he was homeless." Because of his false testimony, Lindstrom was convicted of perjury and the creation of false documentation.

While an unnamed individual having direct access to a defendant's computer is usually an easy claim to prove or disprove, technical SODDI defenses based on the use of wireless networks are generally more fungible. The widespread use of Wi-Fi has increased the number of technical SODDI issues that have arisen, primarily due to open wireless access points. In *United States v. Heiland* (*US v. Heiland*, 2014), the government obtained a warrant to search the home of Heiland's neighbors after tracing child pornography downloads to an IP address associated with their home. After executing the warrant and finding no child pornography in their forensic examination, the investigators found that the home had an open wireless access point that had been setup by Heiland. Several thousand child pornography images and videos were found in a subsequent search of Heiland's computer, and he is currently awaiting trial (Pulkkinen, 2014).

Similarly, in *United States v. Stanley* (*US v. Stanley*, 2014), Stanley was identified when police used a tool called MoocherHunter to track a connection from his computer to his neighbor's Wi-Fi. Stanley's neighbors were targeted when their IP address was associated with distributing child pornography. Following a forensic review of their computers, police identified no child pornography but did find that they had an unsecured Wi-Fi connection. Police tracked a connection to their access point to Stanley's home and obtained a warrant to search his computer. Stanley was convicted for child pornography offenses, but challenged the use of MoocherHunter in an appellate court. The conviction was upheld, with the appellate court determining that Stanley had "opened his window and extended an invisible, virtual arm across the street to the Neighbor's router so that he could exploit his Internet connection"(Lord, 2014).

In *United States v. Luchetti* (*US v. Luchetti*, 2013), federal agents executed a search warrant on the home of the Luchetti's neighbors for downloading child pornography. Similar to *United States v. Stanley* above, the neighbor's computers were determined to have no child pornography present, and the agents found Luchetti piggybacking on their Wi-Fi connection. After the execution of a second warrant that found child pornography on his machines, Luchetti plead guilty to receipt of child pornography (Thompson, 2011).

In another case, a home was raided by a local SWAT team in Evansville, Illinois when the owner's open Wi-Fi router was used to make anonymous Internet threats. In June 2012, a series of online threats against the local police were posted to a Topix forum from the home of Louise Milan. The police obtained a search warrant for the IP address associated with the account, and following a dynamic entry by the SWAT team were unable to link the

posting to the homeowner. A more thorough investigation of her unsecured Wi-Fi led the police to a neighbor, Derrick Murray, who was subsequently arrested for posting the threats. One of the detectives associated with the case noted that he had identified the unsecured access point as part of his surveillance of the home prior to the warrant execution, but the department failed to appropriately incorporate this information in planning their approach (Anderson, 2012; Wilson, 2014).

Not all misattribution is meant to conceal activity. In *United States v. Ardolf* (*US v. Ardolf*, 2012), Ardolf was upset with his neighbors when they filed a police complaint against him after he kissed their four-year-old on the lips. In this case, his neighbor's Wi-Fi network was secured by WEP, an easy-to-crack form of wireless security that has been largely eclipsed by the more secure WPA and WPA2. Ardolf used a WEP cracker and hijacked their Wi-Fi connection, creating a fake MySpace page, downloading child pornography, and sending threats to Vice President Joe Biden, all masquerading as his neighbors. After his neighbors installed a wireless sniffer and engaged the FBI, Ardolf was identified and arrested and convicted of identity theft, making threats against the Vice President, and receipt and distribution of child pornography (Hughes, 2011).

The above cases are a representative sample of the issues illustrating the difference between identifying an originating IP address and/or an originating device and the human committing the offense– numerous similar examples exist. For most residential connections, IP addresses are dynamically assigned to the consumer's wireless access point. Through network address translation (NAT), multiple devices may share the same externally facing IP address. Additionally, even though most providers have recently started providing access points with encryption already enabled, they frequently use default passwords or enable lesser encryption options such as WEP. Exploitation of Wi-Fi has, for criminal purposes, has led to the search and seizure of computer equipment belonging to innocent parties, and to the intrusion into their homes, but there were no acquittals identified where the defendant used a technical SODDI defense. The technical SODDI defense has, however, been widely employed in civil litigation, primarily related to copyright infringement.

4.2 Copyright Infringement Cases

Civil litigation related to activities associated with an IP address largely began with a provision of the Digital Millennium Copyright Act that allowed copyright holders to subpoena ISPs to obtain the names of the individuals responsible for accounts sharing copyrighted material (*Digital Millenium Copyright Act*, 1998). Starting in 2003, the Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA), along with several copyright aggregators, began filing lawsuits against individuals that held accounts associated with IP addresses found to be sharing allegedly infringing material online. By 2007, the RIAA alone had filed an estimated 30,000 lawsuits, achieving successful judgments of up to $9,250 per song shared (Leeds, 2007). In 2006, however, the courts began to accept the technical SODDI defense from those being sued.

In *Virgin Records v. Marson* (*Virgin Records America Inc et al v. Tammie Marson*, 2006), the Recording Industry Association of America traced copyrighted music being shared online to Marson's IP address and identified Marson as the subscriber through her ISP. After attempting unsuccessfully to get Marson to settle for $3,500, they filed suit against her. Marson claimed that, because she was a cheerleading teacher, she frequently had students over to her house and both her

students and her daughter's friends had access to her computer. Additionally, Marson's home network was configured with an open wireless access point. Marson's technical SODDI defense was successful due to an inability by the groups suing her to identify Marson as the infringer, and the lawsuit was dropped (Fisher, 2006).

In *Capitol Records v. Foster* (*Capitol Records, Inc. v. Foster*, 2007), the account "Fflygirl11" was found to have a shared folder containing copyrighted music that was made available on a peer-to-peer file sharing network. Through a subpoena, Foster was found to be the account holder associated with the IP address responsible for the sharing. Foster contended that the account was not hers, and that other individuals had access to her Internet connection. The RIAA sued Foster on the grounds that she was guilty of "contributory infringement". Ultimately, the suit was dropped when Foster requested summary judgment and the RIAA was forced to pay Foster's attorney's fees (Jones, 2007).

The RIAA is not the only group that has had difficulty combating the technical SODDI defense. The MPAA and their constituent studios have had similar difficulties. In *Elf-Man v. Cariveau* (*Elf-Man, LLC v. Cariveau*, 2014), the producers of the movie Elf-Man sued 152 individuals who owned ISP accounts associated with IP addresses sharing the movie online. The court dismissed the lawsuits, finding:

> Home wireless networks are ubiquitous, meaning that a single IP address can simultaneously support multiple computer devices throughout the home and, if not secured, additional devices operated by neighbors or passersby. Thus, the risk of false positives is very real.

Similarly, in In Re BitTorrent Adult Film Copyright Infringement Cases (*In Re BitTorrent Adult Film Copyright Infringement Cases*, 2012), a group of defendants was identified by their ISPs as owning the IP addresses that had shared adult films using the BitTorrent peer-to-peer software. The group put forth several technical SODDI defenses:

> One movant–John Doe #16–has stated that he was at work at the time of the alleged download. John Doe #2 states under oath that he closed the subject Earthlink account, which had been compromised by a hacker, before the alleged download. John Doe #29's counsel represents that his client is an octogenarian with neither the wherewithal nor the interest in using BitTorrent to download *Gang Bang Virgins*. John Doe #10 represents that downloading a copy of this film is contrary to her "religious, moral, ethical and personal views." Equally important, she notes that her wireless router was not secured and she lives near a municipal parking lot, thus providing access to countless neighbors and passersby.

The court found the various defenses compelling, and further found that the film studios were improperly avoiding court fees by aggregating offenders. Aside from John Doe #1, the actions against the other defendants were dismissed, with the court partially concluding:

> It is no more likely that the subscriber to an IP address carried out a particular computer function–here the purported illegal downloading of a single pornographic film–than to say an individual who pays the telephone bill made a specific telephone call... Indeed, due to the increasingly popularity of wireless routers, it much less likely... Unless the wireless router has been appropriately secured (and in some cases, even if it has been secured), neighbors or passersby could access the Internet using the IP address

assigned to a particular subscriber and download the plaintiff's film.

5. DISCUSSION

The technical SODDI defense has moved beyond the basic Trojan horse defense and has been used primarily in child pornography cases in the criminal courts and in copyright cases in the civil courts. The traditional Trojan horse defense has been used, albeit infrequently, when contraband is found on a machine and the defendant claims no knowledge of the material but cannot otherwise attribute the material to another person. A more general technical SODDI defense has been used more frequently when activity is associated with an IP address, or when there is a shared computer without separate accounts for each user.

Since 2004, this study was unable to identify any published cases in the United States where the technical SODDI defense resulted in an acquittal (the closest was in *Fiola*, where the charges were dropped). Additionally, there have been no court cases that have had forensics definitively show that malware placed child pornography on a subject's computer (the *Amero* case was adult pornography pop-ups). A review of the forensics reports available for many of the above cases mistake correlation with causation–the argument is essentially:

1) Malware is present on the device and,
2) It is theoretically possible for someone to write malware that causes child pornography to be present on the machine and,
3) Child pornography is present on the machine,

Therefore,

4) The child pornography is due to the malware.

In addition to the errors in logic present in this argument, it also represents an incomplete forensic analysis. To show causation to the point of a valid legal defense would require that either (a) the malware is activated and monitored to show that its behavior is consistent with the alleged activity or (b) reverse engineering the malware shows that it has the capability of performing the alleged actions. In the case of a Trojan horse that allows unfettered remote access, the defense would need to show that the infection was present and active at the time of the alleged activity and that the activity was inconsistent with other activity by the defendant (Kardasz, 2009).

The forensic analysis presented in several of the cases that resulted in reduced or dropped charges was similar and contained the logical errors noted by Kardasz above. In *Bandy*, *Solon*, and *Fiola*, the same defense technical expert, Tami Loehrs, provided the analysis that supported the Trojan horse defense. Loehrs was cited in Solon by the court for being "outrageous in her charges" related to a bill for over $10,000 for three days of services, further claiming that court had "never heard a more abrasive witness than that." The court then advised defense counsel not to use "this woman with pretty exalted ideas of her worth." Further, when the witness testified that that she had to stop her exam at the analysis of virus logs, the court provided the jury instruction:

> Members of the jury, the witness just said that she was stopped and coupled with her testimony yesterday there is the implication that the court stopped her from working. That is absolutely untrue. It is a falsity, and you are instructed to ignore it. And we will hear no more such testimony. I never did stop this witness from working. I did stop her from submitting excessive bills to the United States, and that's all I ever did (*US v. Solon*, 2013).

Further, Loehr's objectivity was questioned related to an anti-law enforcement bias in *United States v. Elmer Guy Smith*, where she engaged in a

Facebook conversation with David Loehrs, writing:

> FBI: "our mission is to protect you from the most dangerous threats facing our nation"
>
> FBI: the most dangerous threat facing our nation
>
> David Loehrs replied "F** those guys. I'll pee on them."(*US v. Smith*, 2011)

In *Amero*, the case was brought forward based in part on poor forensics by the prosecution. The need for a thorough forensic analysis was highlighted when a proper forensic review showed basic flaws in the initial analysis, which was performed by a non-expert practitioner using a less-than-robust digital forensics tool. While the case resulted in a conviction that was overturned and an eventual plea agreement, there was sufficient doubt raised in the expert forensic analysis to have made a second prosecution unlikely to be successful.

For the general technical SODDI defense cases, multiple cases resulted in the wrong home being searched due to an unsecured or a compromised wireless access point. None of these resulted in court cases against the victims, and forensics was able to clear the individuals quickly. There was, however, a major disruption to many innocent individuals–ranging from knock-and-talks to a full SWAT response. Because of the frequency with which Wi-Fi cases have been found to be due to neighbors, law enforcement is taking a better approach to warrants, for example:

> On April 30, two FBI special agents drove past the Carmel home and noted the existence of two WiFi networks reachable from the property. One used WEP encryption, the other had the more robust WPA2, but the key point from the FBI's perspective was that neither network was unsecured. A search thus seemed much more likely to find its proper target (Anderson, 2012).

The approach noted above should be considered in all cases where criminal activity has been traced to an IP address without corroborating information that ties the activity to a specific person.

In contrast with criminal cases, civil litigation involving the technical SODDI defense has been extremely successful in recent case law. The mass lawsuits sent out by the MPAA and the RIAA have essentially been halted due to their inability to tie an IP address to a particular infringer. Part of this limitation is the inability to seize and perform forensics on devices belonging to defendants, which results in the counterintuitive situation of the defense being *more* successful in civil cases, where the burden of proof is lower, than in criminal cases (preponderance of the evidence v. reasonable doubt).

6. CONCLUSION

Despite a proliferation of botnets that use hijacked computers to launch computer attacks and hackers who attack systems after multiple hops through compromised machines, there have been no published cases in the United States where the technical SODDI defense has resulted in an acquittal, and the defense itself is rarely put forth in criminal matters outside of child pornography cases.

The Trojan horse defense has been subsumed into the broader technical SODDI defense. What originated as "the malware did it" has now morphed into a mosaic of "either the malware did it or someone else with access to my computer/network did it." More thorough forensics prior to charging is now becoming the norm, going beyond simply showing that the subject was at the keyboard at the time of the activity in question. In content-related and illegal access/system interference cases, a review and through analysis of seized devices for malware is needed to head off faulty forensic

claims made to the media or in pretrial negotiations. Similarly, prior to obtaining a search warrant for any cases involving network activity, a review of the network capabilities, specifically Wi-Fi, of the target location should be performed.

Unlike criminal cases, the technical SODDI defense has been used successfully and has largely defeated copyright infringement claims in civil litigation. It is unlikely that mass copyright infringement cases targeting individuals sharing movies or music in a non-commercial manner will continue to the extent previously seen. Even if civil imaging of computing devices were permitted, it would not likely be cost effective to pursue these actions for individual infringement actions.

REFERENCES

Alexander, R. (2007, January 28). Defense in child porn case distorts the truth. Retrieved from http://www.foxnews.com/.

Anderson, N. (2012, June 26). SWAT team throws flashbangs, raids wrong home due to open WiFi network. Retrieved from http://arstechnica.com/.

Associated Press. (2009, November 8). Computer viruses can make you an unsuspecting collector of child pornography. Retrieved from http://blog.al.com/.

Brenner, S., Carrier, B., & Henninger, J. (2004). The Trojan horse defense in cybercrime cases. *Santa Clara Computer & High Tech. LJ*, *21*(1).

Capitol Records, Inc. v. Foster, No. Civ. 04-1569-W (Dist. Court, WD Ok. 2007).

Com. v. Robertson-Dewar, No. 829 A.2d 1207 (Pa. Superior Court 2003).

Digital Millenium Copyright Act, 17 U.S. Code § 512 (1998).

Eckelberry, A., Dardick, G., Folkerts, J. A., Shipp, A., Sites, E., Stewart, J., & Stuart, R. (2007). *Technical review of the trial testimony State of Connecticut vs. Julie Amero*. Retrieved from http://dfir.com.br/.

Elf-Man, LLC v. Cariveau, No. C13-0507RSL (Dist. Court, WD Wash. 2014).

Fisher, K. (2006, August 3). The RIAA, IP addresses, and evidence. Retrieved from http://arstechnica.com/.

Green, R. (2008, November 22). Misdemeanor plea ends Norwich case. Retrieved from http://articles.courant.com/.

Hughes, J. (2011, July 12). Minnesota Wi-Fi hacker gets 18 years in prison for terrorizing neighbors. *Digital Trends*. Retrieved from http://news.yahoo.com/.

In Re BitTorrent Adult Film Copyright Infringement Cases, No. 2012 U.S. Dist. LEXIS 61447 (E.D. New York 2012).

Jones, P. (2007, February 8). For the cynics, an antidote: The Order in Capitol v. Foster. Retrieved from http://www.groklaw.net/.

Kardasz, F. (2009, November 9). Highly unlikely that a virus would ever place images on your computer. Retrieved from http://kardasz.blogspot.com/.

Landwehr, C. E., Bull, A. R., McDermott, J. P., & Choi, W. S. (1994). A taxonomy of computer program security flaws. *ACM Computing Surveys*, *26*(3), 211-254.

Leeds, J. (2007, October 5). Labels win suit against song sharer. *The New York Times*. Retrieved from http://www.nytimes.com/.

Loehrs, T. (2009). Report of forensic examination. Presented at the Winning Strategies. Retrieved from http://www.fd.org/.

Lord, R. (2014, June 11). Court rejects appeal of man who piggybacked on Wi-Fi signal to access child porn. Retrieved from http://www.post-gazette.com/.

Lubet, S. (1992). Reasserting in cross-examination control. *Litigation*, *18*(4), 24-29.

Matyszczyk, C. (2013, July 27). Man gets fake FBI child porn alert, arrested for child porn. Retrieved from http://www.cnet.com/.

Moats, T. (2010, January 23). Montpelier man charged in Internet child porn scam. Retrieved from http://www.vermonttoday.com/.

People v. Lindstrom, No.60608 (Cal. Court of Appeal, 3rd Appellate Dist. 2009).

Pulkkinen, L. (2014, April 8). Feds: Neighbor's Wi-Fi a path to child porn for Bonney Lake man. Retrieved from http://www.seattlepi.com/.

State of Arizona v. Matthew Bandy, No. CR2005-014635-001 DT (Maricopa County Superior Court 2005).

State of Connecticut v. Amero, No. CR-04-93292 (Conn. Superior Court 2007).

Steel, C. M. S. (2009). Web-based child pornography: Quantification and qualification of demand. *International Journal of Digital Crime and Forensics (IJDCF)*, *1*(4), 58–69. doi:10.4018/jdcf.2009062405

Sweet, L. (2008, June 16). Probe shows kiddie porn rap was bogus. Retrieved from http://bostonherald.com/.

Thompson, C. (2011, April 24). Innocent man accused of child pornography after neighbor pirates his WiFi. Retrieved from http://www.huffingtonpost.com/.

US v. Ardolf, No. 683 F. 3d 894 (Court of Appeals, 8th Circuit 2012).

US v. Gardner, No. WL 6680395 (Dist. Court, D. Utah 2012).

US v. Heiland, No. CR14-5188BHS (Dist. Court, WD Washington 2014).

US v. Holness, 706 F. 3d 579 (Court of Appeals, 4th Circuit 2013).

US v. Kerr, 472 F. 3d 517 (Court of Appeals, 8th Circuit 2006).

US v. Kuchinski, 469 F. 3d 853 (Court of Appeals, 9th Circuit 2006).

US v. Luchetti, No. 11-CR-143 (Dist. Court, WD New York 2013).

US v. Miller, 527 F. 3d 54 (Court of Appeals, 3rd Circuit 2008).

US v. Moriarty, No. 429 F. 3d 1012 (Court of Appeals, 11th Circuit 2005).

US v. Smith, No. 4:09-CR-00441-CKJ-DTF (Dist. Court, Arizona 2011).

US v. Smith, No. 739 F. 3d 843 (Court of Appeals, 5th Circuit 2014).

US v. Solon, No. 13-8058 (Court of Appeals, 10th Circuit 2013).

US v. Stanley, No. 753 F. 3d 114 (Court of Appeals, 3rd Circuit 2014).

Virgin Records America Inc et al v. Tammie Marson, No. 2:2005cv03201 (California Central District Court 2006).

Wilson, Mark. (2014, September 13). City seeks favorable ruling in SWAT incident lawsuit; Police video shows what happened. Retrieved from http://www.courierpress.com/.

Wise v. State, 364 SW 3D 900 (Texas State Court of Criminal Appeals 2012).

