The Trojan Defense:

A Brief History and Use of the Program

[redacted]

Indiana University of Pennsylvania

The Trojan Defense

This research paper talks about the history of a Trojan defense and the Trojan programs them. Throughout the growth of computers many people have started to use malicious malware on others peoples program to hack or hold information that could be used against them. When people have certain items on their computers for example like child pornography, the accused will used the so called “Trojan defense” and blame it on a virus that attacked their computer. This leads to trouble with the lawyers who accuse the people and try and fight the case.

The Trojan Defense

Introduction

Through the growth of computers throughout the last 20 years, we have seen the growth do wonders in the world of communications, information, and connectedness. Though all these things have good intent behind them, sometimes the people behind the screens do not. Since the dawn of computers there have been people who try and use them for the bad. They create malware or virus that do damage to certain information and wipe out information or access information that they might not be able to before. So if someone is caught with either malicious information on their computer like a launched hack or content that is illegal, they are sent to court to be tried and see what the consequences will be. Since the start of the computer age, these attacks the defense have used the so called “Trojan defense” to save them from jail time whether innocent or not.

Background/ Topic

Once people are arrested for the malware found on computers they have to put up a defense to fight the case guilt or not. “A Trojan horse program, a variety of malware, is a program that appears to have some useful or benign purpose, but really masks some hidden malicious functionality. Malicious functionality could include anything from downloading contraband files to attacking other computers” (Brenner, 2004). Once police and investigators started to find crimes like this they had a strong defense counter them with the Trojan defense. The Trojan defense is an “online version of the SODDI defense. Instead of blaming "some other dude," the defendant blames malware for the unlawful conduct that is being attributed to him or her” (Brenner, 2004). Basically the defense will say, “I did not put that information on my computer, some other dude put a Trojan virus on my computer and put it there.” This raises extreme

problems for the prosecution when trying to convict these people. One reason for difficultly is the jury. The jury might have little to no knowledge on computer jargon, computer science, or computer forensics. This helps the defense with them not knowing anything but them saying yeah it's possible that a guy put it there and I don't have any trace of a Trojan virus on my computer. In most cases a computer forensic expert will check the computer for a Trojan virus, but most of the time they will find one. So a defense with I did not put it there and a virus to back that up provides difficulty to prosecute that. The prosecution has had difficult times then determining the guilt of the defendant when they use the Trojan defense. Over time as Wi-Fi has been used many cases involve the use of hacking a wifi network and using that as putting malicious content on someones computer instead of a Trojan virus. "Ardolf used a WEP cracker and hijacked their WiFi 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" (Steel, 2014). This is a famous case is United States v Ardolf, where he got on a WiFi connection when he was mad at his neighbor and posed under his Wifi as the neighbor doing malicious things. This is one example of how difficult and complex this whole system. This has changed the way that the Trojan defense has been presented since the early 2000s. "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" (Steel, 2014).

The "Trojan defense" has been used throughout the cybercrime history as a way for the defense to claim. "I did not commit this crime; someone else infiltrated my computer and did it." This

leads the prosecution to have troubles convicting them of the crime and providing proof of guilt. Many cases lead the defendant to get off free, because they have proof of a Trojan virus on the computer but no proof they were at the computer when it happen. It raises many questions in the world of computer forensics and computer crime on how to catch who is doing and who is guilt or not guilty. The defense has to support their case by having proof that the Trojan virus was put there and someone else did it. The prosecution might have trouble also because the accused may have more knowledge on the subject over them and have a way to deny knowledge of how it happens. These cases of the Trojan Defense favor the defense in many ways and cause problems for the prosecution to get a conviction against them.

The Trojan Defense

References

Susan W. Brenner, Brian Carrier, and Jef Henninger, *The Trojan Horse Defense in Cybercrime Cases*, 21 Santa Clara High Tech. L.J. 1 (2004).

Chad M. Steel, *Technical SODDI Defenses: The Trojan Horse Defense Revisited,* 9 George Mason University