Golden G. Richard, III

Title: Digital Investigation and the Trojan Defense, Revisited

Abstract:

Over the past 15 years, digital forensics has been radically transformed by the introduction of new tools and techniques that support very detailed investigation of a wide variety of digital crime scenes, spanning unauthorized data exfiltration, fraud, employee misconduct, kidnapping, child pornography, and murder. Modern digital forensics tools can be used to deeply examine not only computer systems, but smartphones, voice recorders, printers, cars, and much more. A common defense used by those accused of wrongdoing in crimes involving digital evidence is the so-called Trojan defense, which essentially means "I didn't do that--a computer virus did it." This defense has traditionally been quickly dismissed by investigators after a cursory examination of digital devices for the presence of malware. Often, this sweep for malware consists of simply running an antivirus program, noting a negative result, and using this as a basis for proceeding with the charge of wrongdoing. In all likelihood, this process was historically fairly accurate, because it was pretty unlikely that a virus did "do it". Now, in the face of increasingly sophisticated cyber attacks and malware infections, it's frequently very possible that someone or something (e.g., malware) other than the "obvious" party may be guilty. The solution to unraveling the accuracy of Trojan defenses and pointing the finger of blame in the right direction is increased technical sophistication for investigators. This talk surveys a number of recent high tech cyber attacks and discusses the implications for surety in digital investigations while simultaneously underlining the importance of combatting cyber attackers with their own weapon: deep technical knowledge.