

The Trojan Horse Defence

By Marty Musters CISSP, CFE

No, this is not an article on chess. This is an article on the latest defense strategies now being used by criminals in their attempts to conceal their crimes. Why is it that at every turn we find new ways to say, “It Wasn’t Me”. In fact, some criminals are planting Trojans on their computers with the idea that if caught, they will pull out their “defense” card.

As computer forensic investigators we are asked to take an image of a hard drive, preserve it for evidentiary integrity and then perform a detailed analysis on what we found. Sometimes the obvious isn’t so obvious anymore. When the guilt or innocence of a person, their reputation, their standing in the community, their jobs, their livelihood, civil action (which translates to money) and possibly jail time hang in the balance it is important to perform a detailed and accurate assessment that looks at all possible scenarios.

There is the common scenario where the bad guys are using zombies or bots (small computer programs residing on a computer and controlled by someone else) to extort money from others. According to Symantec, the city of Winsford in Cheshire is the world’s second biggest hotspot for zombies, followed by Seoul in Korea. The anti-virus company estimates that nearly a third of between one and two million computers worldwide infected with the bot software are now located in the UK. In a Sept 19 2005 article in TechWorld entitled “Zombies take hold of London”, the article details how zombie computers have become a weapon of choice for spammers and phishers as well as attackers looking to swamp a victim’s server with a distributed denial of service attack.

Take BetCBSports.com. In an Information Week article they tell of how they received an email one day which said, “You have 3 choices. You can make a deal with us now before the attacks start. You can make a deal with us when you are under attack. You can ignore us and plan on losing your Internet business”. This type of distributed denial of service attack (DDos) is becoming increasingly popular against businesses that rely completely on the internet for their source of revenue. Typically the amount of money asked for is relatively small in comparison with the lost revenues the company could expect as a result of being down. More times than not the extortion fee is paid. For those that don’t pay, it is an endless battle of bandwidth. The more bots the extortionist control, the more bandwidth they can pump into the DDos attack. The more bandwidth they throw at the site, the more bandwidth you need to combat them. For an interesting article on how a whiz kid and a bookmaker took on an extortionist and won, read the article published in CSO online.com <http://www.csoonline.com/read/050105/extortion.html?action=print>.

Which brings us to the more sophisticated type of bot or Trojan Horse. A different breed of bad guy’s are using this as a defense, more commonly known as the “Trojan Horse

Defense”. Defendants are now pleading not guilty on the basis that someone else put code on their computers that caused the illegal material to be present. Karl Schofield of Whitley England was cleared of possessing 14 images of child pornography. In another case Julian Green of Devon England was acquitted of storing 172 images of child pornography on his system.

So what can we do as forensics investigators do to combat this ever increasing problem of “It wasn’t me”. I recently came across some excellent software that every forensics investigator should have in their toolkit. Gargoyle Investigator Forensic Pro Edition made by Wetstone Technologies. Gargoyle Investigator is an invaluable software tool for digital investigations. It is fast and easy to use, it provides investigators with important information regarding the contents of a suspect’s computer along with essential information about it’s owner’s computer use. Gargoyle performs rapid searches for over 7000 known “bad or hostile” programs, their associated files and remnants of files. Once identified, Gargoyle also maps the detected files to the associated cyber weapons, and classifies them into a category of malware. With the ability to identify potentially hostile or suspicious programs based on the loaded datasets (which are regularly updated by Wetstone), it makes the forensic exam much easier. Gargoyle’s Forensic Pro should be run as a standard on all forensic examinations to prepare the prosecution or defense for the possibility that the Trojan horse defense may be used. Another useful feature of the program is that the last accessed date/time as well as the installation date/time are made available. This could provide valuable insight as to whether the Trojan/malware could have been responsible or not for the downloading of the illicit file onto the computer.

Gargoyle™

File Actions Reporting Help

Directory Drive
UNC Path Hash Drive Image

Select Drive Image Files:
Drive Mounting Software:
 Program: **Mount Image Pro**
 Status: **Installed**
 Version: **1.05**

Selected Images:
 C:\Documents and Settings\chet\I

Test Mount File Add Image File

Mount As:
 Logical Drive Single Drive

C:\Documents and Settings\chet\Desktop\Work\Instruct\Desktop Files\Seized Image.RAW mounted successfully.

GARGOYLE ENTERPRISE™

Dataset Selection and Threat Legend:

Unselected	Selected	Low Threat	Medium Threat	High Threat
Evidence Altering:	File Splitters: 1	Graphic Editors:	Instant Messengers:	History Erasers:
Key Loggers:	P2P Tools:	Password Crackers:	Remote Access:	Rootkits:
Packet Sniffers:	Spyware:	Steganography: 23	Toolkits:	Trojans: 1
Wireless: 4				

Scan Location: (Drive Image File(s)) C:\Documents and Settings\chet\Desktop\Work\Instructor\Demonstration D Scan

Checking: F:\Stego Sample Programs\Wireless\Airopeek NX 2.0.1\WCAGS48C.EXE

Total Directories: 38
 Total Files: 714
 Files Checked: 652

X Abort Scan

File Name	Detected	Program	Version	Multiple	Path	Scanned Files
BSIDE.EXE	Yes	BlindSide	0.9b		F:\Stego Sample Programs	FFFF8
Copy (2) of BSIDE.EXE	Yes**	BlindSide	0.9b		F:\Stego Sample Programs	FFFF8
Copy of BSIDE.EXE	Yes**	BlindSide	0.9b		F:\Stego Sample Programs	FFFF8
EN-CID12.DOC	Yes	1900 Killer	1.2		F:\Stego Sample Programs	B46E2
BSIDE.EXE	Yes**	BlindSide	0.9b		F:\Stego Sample Programs\Blindside	FFFF8
DECODEME.BMP	Yes	BlindSide	0.9b		F:\Stego Sample Programs\Blindside	FE218
README	Yes	BlindSide	0.9b		F:\Stego Sample Programs\Blindside	7154B
hmp embed.exe	Yes	BMP Embedding	1.04		F:\Stego Sample Programs\BMP Embed	00000

Windows - Delayed Write Failed

Malware Scan Summary	
Category	Programs Found
Credit Card Fraud Programs	0
Denial of Service Programs	0
Drive Eraser Programs	0
Encryption Programs	1
Evidence Altering Programs	0
File Splitting Programs	1
Graphic Editing Programs	0
Instant Messenger Applications	0
Internet History Erasing Programs	0
Key Logging Tools	0
P2P Tools	0
Password Cracking Tools	0
Remote Access	0
Rootkits	0
Packet Sniffing Programs	0
Spyware Programs	0
Steganography Programs	23
Toolkits	0
Trojan Horse Programs	1

All of the information we gather are simply pieces to a puzzle that must be carefully put together. In the case where Trojans or malware is present, timelines and careful analysis become critical. Was the Trojan loaded onto the system AFTER the child pornography images were downloaded? What was the state of patching and anti virus protection on the machine we are examining. What was the state of patching at the time the Trojan was loaded onto the computer? If there were no known vulnerabilities at the time the Trojan was loaded how did it get on the computer? The most important question of course is to properly identify the Trojan and determine what its capabilities are. A simple bot program receives a command from it's "master" so to speak to flood traffic to a certain IP address. In this case, our little bot would not be capable of downloading child pornography. On the other hand, if there was a program on the hard drive that allowed complete remote access then clearly we have a much more complex evaluation. If someone else besides the suspect had root access then who did what when becomes the real question. How often did they use that root access. Are there clues in the logs that would identify when this malicious activity was happening and was this the time when

the child pornography was loaded. Was this an XP machine and was the personal firewall turned on. What information can we glean from the firewall logs.

It is possible that our suspect is innocent by even the most simple of means. Take for example our not very computer literate individual who sets up a wireless access point and does not secure it. Inside his home network he has a couple of p/c's and a notebook all with file and print sharing turned on. His appreciative neighbor who does not have to pay for internet services figures out one day that he can download child porn and view the images on his neighbor's p/c without ever loading the images on his own machine.

Another interesting benefit from running Gargoyle is that hiding programs, like steganography, encryption, drive erasure and evidence altering programs will also be identified. This will offer clues as to the intent of the suspect, their level of sophistication, covert behaviors, and paranoia levels can all be derived when searching for applications with a common theme. These behaviors can also assist in forensic examination.

Our world as forensic examiners is becoming more and more complex each day. Let us remember though, that the obvious is always as obvious as it looks

Marty Musters graduated with a Bachelor of Mathematics and Computer Science from the University of Waterloo. He is a CISSP and a CFE (Certified Fraud Examiner) and a member of the High Tech Crime Investigation Association (HTCIA).