HIGH TECH CRIME INSTITUTE INC RESEARCH PAPER

6/21/2015

Protecting Forensic Production Exams from Media Viruses

Recently computers deployed to forward regions have become susceptible to computer viruses. The viruses are a result of conducting Media Forensic Exams. This paper will propose a methodology to protect the forensic computer, as well as be able to reset the computer to a preset configuration ready to conduct a forensic exam.

Report Prepared By: Stephen Pearson

INTRODUCTION

Recent reports from the field indicate an issue with the deployed forensic computers. Personnel that are conducting forensic examinations are using tools on the computer to open media files. When using these programs the computer maybe exposed to computer viruses. Computer viruses take advantage of flaws in computer programs. When an application opens an infected file the virus is able to launch its payload infecting the computer. Once the computer has been compromised the infected system can no longer be reliably used for the collection or processing of media. This paper proposes a strategy that is used commonly in Law Enforcement Media Forensics to address this issue or problem. The paper is focused on attacking the problem with tools currently available in the operational toolkits.

PREVENTION

Anti-Virus Protection

The use of Anti-Virus (AV) programs is a method to help prevent systems from becoming compromised by known viruses. Several papers address the use of AV in computer forensics. The issue with using AV applications is that they can attempt to corrupt or remove the malicious software. If the malicious software is being used to protect the file or files being examined the removal of the virus may also lead to the infected file being removed. This file may have data that is useful in the forensic examination. Files located in image files such as an E01 file or DD file may be protected from this erasure by the AV tool. The downside of this is that the AV tool may block the use of that E01 or DD file. If this happens then the image file is no longer able to be used by the investigator.

A method of using the AV tool that will allow the operator to make a decision as to the disposition of a file is to run the AV program with the sandbox option. This will quarantine the malicious files without removing the files. The investigator can make a decision to not delete the file.

Alternate applications. Some malicious software is designed to work with a specific program such as Microsoft Paint. If a file is opened with that application and it has malware designed to exploit a flaw in the Microsoft Paint program then the computer will most likely be infected. Replacing the Microsoft Paint program with another default application would prevent this from happening as the alternative application would not have the security flaw. There are two recommended programs for viewing images and videos:

IRFAN VIEW – CAN OPEN JUST ABOUT ANY GRAPHIC IMAGE. IT IS DESIGNED TO ALLOW QUALITY PHOTO EDITING. THIS APPLICATION IS IN USE IN JUST ABOUT EVERY LAB IN THE WORLD AS IT IS ONE OF THE BEST TOOLS TO WORK WITH GRAPHIC IMAGES. THE PROGRAM IS OPEN-SOURCE AND CAN BE DOWNLOADED FROM WWW.IRFANVIEW.ORG

VLC - THIS PROGRAM CAN OPEN JUST ABOUT ANY VIDEO FORMAT. IT IS DESIGNED TO SUPPORT MOST CODECS TO INCLUDE CELLPHONE SPECIFIC CODECS LIKE THE ONES BEING USED BY NOKIA ETC. THIS APPLICATION IS IN USE IN JUST ABOUT EVERY LAB IN THE WORLD AS IT IS ONE OF THE BEST TOOLS TO WORK WITH VIDEO FILES. THE PROGRAM IS OPEN-SOURCE AND CAN BE DOWNLOADED FROM WWW.VIDEOLAN.ORG

Anti-Virus Updates

Operators need to ensure to dedicate time to update and refresh computers being used for collection purposes. This means that the computer being used will need to be connected to a network to either download new virus signatures from the internet or from a local repository setup for enterprise updates. The later would be the safest method available for the operators.

QUICK SYSTEM RESTORE

Creating a Backup Strategy

The backup media strategy is based on having 3 identical or close to identical hard drives (Size and speed are the most important factors to ensure this strategy works).

1. The Forensic Collection Computer (FCC) should start out as a fresh computer. The computer's hard drive should be wiped and prepared using tools in the operator's kit such as the TD-2 Wiping utility.
2. Once the computer is wiped and prepared the operating system and all tools should be loaded from clean install media. After all the programs are installed the computer should be connected to the internet to gather all updates for the OS and installed programs. Ensure that you are running and AV tool before connecting the system to the internet.
3. Once the operating system and all programs are updated disconnect the computer from the internet.
4. Follow the steps below in the Using the Tableau TD-2 Imager to create the two production drives.

Using the Tableau TD-2 Imager

Prepare the forensic system with all programs and updates needed for operation. Make sure to do all windows updates and driver updates to the system. Once this is done the system is ready to be used to collect evidence. To update your system put the master drive back in and update the master drive. Never use the master drive to collect evidence. Reimage the production drives from the master drive.	
Place the laptop back cover side up	

Remove the retainer screws from the cover that covers the additional hard drive and DVD RW access	
Remove the single retainer screw holding the DVD RW in place. This screw is at the back of the DVD RW. Carefully remove the DVD RW sliding it to the left away from the laptop main body.	
This will expose the primary hard drive located under the DVD RW	
Remove the 4 retainer screws holding the hard drive in place. Slide the hard drive to the left away from the body of the laptop. You will see the gold in color connectors be displayed. Lift the hard drive up and out of the laptop. Make sure not to bind or damage the drive as you remove it.	

The drive is now removed. Take the hard drive out of the drive carrier tray by removing the side retainer screws.	
When the hard drive has been removed it should resemble the picture	
Gather your two production drives that you are going to make a duplicate images too and the master drive that you just removed. (The kits may not come with these additional 2.5 inch drives. The drives can be purchased from any computer outlet or online. Try to match the drives up as much as possible. They must be the same size 500gb = 500gb	
Using the Tableau TD-2 in your kit you will create 2 duplicate or production drives from the master drive. Connect the TD-2 to a power outlet. Turn the TD-2 ON. Let the TD-2 boot up until the Main Menu is accessible. Place the master drive on the left side of the TD-2 and attach it to the TD-2 using the supplied SATA cable. Connect the two production drives to the right side of the TD-2 to Destination 1 and 2 using the supplied cables.	

From the TD-2 main menu select option 1 "Duplicate Disk"	
Select option 1 Disk to Disk	
The TD-2 will identify the drives connected and show you the source drive Src which is the master drive and destination 1 D-1 and destination 2 D-2. If any of these fails to show check the cables and connections replace the destination drives as needed. If the Src drive is not shown stop and correct any issues as the Src is required for the duplication. Once all the Note fields have been bypassed select Start to begin the process.	
A summary of the collection will be shown on the screen, estimating the completion time.	

Once you are done you will have two production drives and a master drive. Place one of the production drives into the laptop. Place the master drive and second production drive in a safe location for use later.	

5. Now that the hard drives have been created the operator has a hot swap drive that can be switched quickly into the FCC. All the operator has to do is remove the other drive and put in the other production drive.
6. The hard drive that is corrupted is connected to the TD-2 and reimaged using the master drive. The operator can continue on, and if there is another incident can quickly switch the next drive in to the computer. With this method the mission can continue. It is very important that the next drive be reimaged immediately to prevent downtime for the operator. If this backup rotation is followed operator collection should be optimized.

CONCLUSION

The methods talked about in this paper are based on the current toolkits available. As new tools are implemented or added to the kits, new methods would need to be created. This document is a brief overview of a suggested methodology that will allow an operator to have as much uptime as possible when working with the deployed kits.

References:

Stephen Pearson

Sebastiano Pepenella

Steven Wood