Detecting Computer Crimes with Modern Tools

David C. Shields

Submitted to Dr. Clint P. Garrison

In Partial Fulfillment of CSEC650

University of Maryland University College

Table of Contents

Detecting Computer Crimes with Modern Tools

Introduction

Computer crimes are defining the criminal landscape of the digital age. In this new world, computer crimes such as network intrusion, malware downloads and insider threats can costs companies millions or even billions of dollars. It is not enough to simply monitor books or papers that an employee takes out of the building anymore, now a company must monitor all egress points on their network including the internet, USB thumb drives, and even email traffic. Companies now hire teams of compliance and legal professionals with the primary purpose of preventing digital theft and monitoring employee activity on the network. Despite the large number of challenges the digital world may bring, there are many ways to use modern tools to detect these computer crimes. Almost all computer systems have some sort of system logs or records that can illustrate what is occurring on the computers. Also, most modern companies with any sizable technology footprint have access to network intrusion systems which can also generate logs. It is also a common practice for a company with a large enough data footprint to implement some sort of Data Loss Prevention mechanism which may lead to the detection of other strange behaviors. Last but not least, a company can always interview the users who are in the environment to gain useful insight into some of these situations. The use of items such as system logs, network security logs, data loss prevention software (DLP) and user feedback can greatly enhance a company’s ability to detect network intrusion, malware installation, and insider file deletion.

Detecting Network Intrusion

One of the most common yet also most complex attacks a company may face in their lifetime is a network intrusion. This is one of the crimes that are covered under the Computer Fraud and Abuse Act as a punishable offense (Brenner, 2011, p. 86). Often a network intrusion is carried out after an attacker has performed an extensive analysis of the network and has found the weakest points. Prior to an actual network intrusion, it is highly likely that an attacker will have performed some investigation of the network and a well-trained security engineer may be able to detect some common signs of a potential intrusion (Street, Nabors, & Fritz, 2010, p. 178).

The system event logs of a Windows server or the Linux system logs are constantly collecting data of various operations on the computer system. Any time there is a change to the state of the system or the security controls of any system are activated, there will be some sort of logs generated. In the event of the network being analyzed by a potential attacker, it is possible that the system logs will show a pattern of unusual behavior (Casey, Applying Forensic Science to Networks, 2011, p. 664). By knowing what to look for in a particular system log and understanding symptoms of a potential attack, the security engineer can use these logs to predict or detect various techniques. The logs generated in a single system may not be sufficient to detect an attack but when this data is coupled with a network log analyzer, the picture may become clearer.

A network intrusion by its name is indicative of events that occur on the network as a whole rather than on a single system. Many modern firewalls and network appliances, much like their desktop or server counterparts, also have some sort of log files that may provide useful evidence in tracking the hallmarks of a network intrusion (Cobb, Cobb, & Kabay, 2009, pp. 15.23-25).

When an attacker makes any number of actions on the network, a skilled engineer can use the network logs and the logs from any Network Intrusion Detection/Prevention System (NIDPS) in place to help reconstruct what has occurred and hopefully catch the criminal before any actual data loss has occurred. Many modern IT Security infrastructures have some sort of alarm system in place that will watch for certain behaviors and either perform automated tasks if detected or will notify the security team depending on the event and the triggers (Nelson, Phillips, & Steuart, 2010, p. 434).

When investigating a network intrusion, the data collected by these network logging tools and automated alarm systems can be great sources of information. If the victim of the network intrusion has additional tools such as Data Loss Prevention (DLP) in place, the data these items produce could also be used to detect a network intrusion. One of the greatest strengths of DLP tools is their ability to detect internal threats before they happen or as they are happening (Brussin & Opatrny, 2009, p. 26.3). Although DLP tools are certainly not the primary source for useful information in a network intrusion, they will be able to help provide a more complete picture of the intrusion if internal data was modified or compromised.

Lastly, user feedback in a network intrusion case could be useful or further complicate the issue. It is highly unlikely that the standard user in a company will have any idea that a network intrusion has occurred unless the intrusion causes some sort of service disruption for the user. It is also possible that if a user population is informed of a network intrusion and asked to provide feedback, it may prompt them to associate unrelated issues to the network intrusion and skew the potential usefulness of data.

In a worst case scenario, users who are informed about a network intrusion may discuss it more openly than technical staff including discussing it in open forums such as social networks. If the network intrusion information is published on a social network then it is likely to make catching the culprit much more challenging.

Malware Combat

The spread of malware across corporate devices is a staggering figure. It seems that malware is becoming one of the biggest challenges in the corporate security landscape. Much like the antivirus challenges of the late 90’s and early 2000’s, more money and effort has been spent to combat this menace than many other security threats (Goodrich & Tamassia, 2011, pp. 174-176). Because of the wide variety of potential forms in which malware can manifest, the security engineer and digital investigator will need to access every resource available to them if they hope to build a case. On a positive note, the installation of malware is also a punishable offense under the Computer Fraud and Abuse Act which means that if a case can be built against a person who knowingly released this software, they can be prosecuted (Brenner, 2011, p. 88)

When malware is installed on a computer, it is a change to the system state and therefore should generate some system logs. Unfortunately, the creators of malware are also aware that logs will be generated and will go to great lengths to disguise the changes being made to a system (Anderson, 2008, pp. 645-646). Another side effect of the manner in which malware works is that it often will disrupt other system processes as it is executing its own code. As a result, the system logs may show odd behavior and process crashes that may be linked to a malware infection.

If a forensics analyst or security engineer has already found some records in the network logs or system logs that indicate when a possible malware was installed elsewhere, the events in any other computer's system logs can be correlated by time and date to determine if similar activity is witnessed elsewhere.

A common consistency in malware infections is the fact that the malware is likely to transmit some data from the local system to a remote system as either a payload or as a data mining task (Moser, Kruegel, & Kirda, 2007). This particular transmission is likely to appear unusual in the standard traffic logs across a network as the IP and host are likely in another country or at least sending unusual patterns. If the patterns appear to be consistent with a particular host or with a particular range of addresses, the network engineer can use this data to formulate an idea of the source of the malware. In this way, the network logs can produce a great amount of useful data for the company or forensics investigator to build a case against the attacker. Unfortunately, the many subversion techniques on the Internet such as The Onion Router (TOR) make the legitimate tracing of an external transmission source somewhat difficult (The Tor Project, 2013).

It is highly unlikely that a DLP tool will offer much usefulness in detecting a malware installation as this is beyond its standard purpose. There is a possibility of data being transmitted from the infected host to an external web site as mentioned recently. In this case, the data transmission records may offer some hints as to what host(s) is/are infected and may lead to detecting some sort of upload pattern. A unique way that DLP may help, however, is if a malware has been programmed to copy itself to any external device attached to a computer. In these cases, the DLP tool should be able to register that data is being transferred and the original host from which it was transferred.

The single most helpful source of information in the event of a malware installation is the user. As malware is often installed on individual host machines as opposed to a large scale install across many systems, the individual user experience on a compromised machine is likely to suffer. If a user notices a sluggish performance from their computer system – especially if the performance seems sudden – this may be an important sign that malware has found its way on to the machine (Cobb, Cobb, & Kabay, 2009). The caveat to seeking user feedback regarding a potential malware installation on their machine is that it must be done in a way that is seemingly random to the user. It is common for users who hear about a potential malware infection or other performance-reducing events to attempt and identify that they, too, are suffering from this performance issue. While it may be true that their machine is infected, it may also be true that the machine has other issues besides malware that are slowing it down but find it easy to identify with a group epidemic rather than to attribute something to its root cause (Sophos AG, 2012). Regardless of the situation in which a user reports a performance issue, there is no reason not to analyze the issue as due diligence against potential threats.

Insider Threat Detections

Among all the potential security threats discussed in this document, none are as potentially damaging as the crimes performed by an insider. It is commonplace for companies to do considerable research before making a hiring decision on any employee but even a person with a clean history (or at least an undocumented one) has the potential to do major damage to their company (Post, 2009, pp. 13.4-5). These crimes are usually severe enough that they not only carry potential charges under the Computer Fraud and Abuse Act (Brenner, 2011) but may also carry charges such as Damage to Intellectual Property or even federal criminal charges.

Unfortunately, these crimes may be much harder to detect with available tools than the crimes mentioned elsewhere in this document.

When an insider chooses to delete a file (be the intent malicious or accidental) there is little evidence that the standard computer system logs can provide. Most logs will be able to reflect the user name logged into the machine at the time the event is reported to occur and may illustrate other activity the user has performed during that session but this may not always be useful. If the file is a critical system file that is necessary for the operating system or program to run, it is certainly likely that the logs would reflect the missing file or at least the degraded performance being experienced as a result. Certainly, this information may be useful in some ways but it is also unlikely that the insider who is knowingly committing a crime would choose to delete system files unless they held some sort of administrative role and were intending to disrupt service for the other users (Goodrich & Tamassia, 2011, pp. 175-177). Once a file has been deleted, however, many modern forensic tools are able to find and restore deleted files based off records within the hard drive’s file allocation table as these deletions are logged but not easily accessible in live systems (Nelson, Phillips, & Steuart, 2010, pp. 227-228).

Network logs may also prove relatively unhelpful in detecting an insider file deletion or other insider attack unless a network vector is involved. Common practice in small business and enterprises alike is the use of network shares to store critical files. This practice is suggested and used as it keeps these critical files in a location that is safe from local system failure and is usually backed up frequently (Stallings, 2009). If the file being deleted is stored on network shares, it may be possible to use the network logs to determine the user responsible and may even be possible to restore it from a backup.

If an investigator seeks to track down data about user shares, it would be a beneficial idea to seek out those within the company's IT department who control network shares and determine what information is collected as well as what is necessary to be provided access to this information (Casey & Schatz, 2011, p. 211).

In the case of insider file deletions, none of the various sources examined in this document are as useful as Data Loss Prevention tools. The protection of critical company data and managing who has access to the aforementioned data is one of the primary purposes of a DLP tool. If properly configured, DLP tools are likely to log any access, modification, or deletion of important files that may be targeted by an insider. Real-time DLP tools are generally designed to monitor file activity across the network and on individual machines and will often generate logs or alarms to an administrator when undesirable actions are performed (Deepa, Priyadarsini, Sathiyaseelan, & Kumar, 2012). To this end, an investigator seeking to build a case for insider foul-play should be able to reference the DLP logs, cross-reference the logs with other case data, and identify the user(s) and the data that was impacted. In fact, if the DLP solution is somehow linked into a Security Event and Incident Management (SEIM) system, all the data needed to locate the potential suspects may be combined in a single system.

Due to the nature of an insider file deletion and the suggested amount of secrecy involved, it is not highly likely that user feedback will offer much assistance. If the file(s) were critical and accessed by several different people – say in a network share – it is certainly possible that the users will notice if the file is missing or deleted. In fact, these users are likely the first ones to contact security about such a situation. Regrettably, users will have little to offer if the file deletion occurred on a local machine and may be completely oblivious to any such action.

User feedback may be solicited regarding a particular employee’s actions after the other security precautions (release of the offender, forensic copy of hard drives, etc.) have been completed but should certainly not be requested otherwise. Sensitive matters such as negative actions of employees must be tightly controlled by HR and Legal teams or risk potential lawsuits by those impacted (Kabay & Robertson, 2009, pp. 45.10-11). Instead, a quality security awareness training course should be implemented in such a way that if a user witnesses a potential crime such as insider file deletion, they will be aware of the proper personnel to contact and avoid confrontation with the suspect.

Conclusion

As the digital age continues onward, so does the potential for digital crimes such as network intrusions, malware installations, and insider file deletions. The United States Legal System has made great strides in increasing the laws and punishable offenses for computer crimes but this metamorphosis is only just beginning. It seems that computer criminals and their methods continue to evolve faster than their victims’ ability to defend but this margin narrows a little more with each passing day. More and more digital tools are being made available each day for companies and investigators to react more rapidly to these crimes. This article has examined a few ways in which system logs, network logs, DLP tools and user feedback can be used as sources for investigating various cybercrimes but these are but a small sampling of the many options available. One can hope that the evolution of information security can someday reach a level in which the criminals no longer have the advantage but until that time, this field and its various disciplines will continue to evolve.

Bibliography

Anderson, R. J. (2008). *Security Engineering.* Indianapolis: WIley & Sons Publishers.

Brenner, S. W. (2011). Cybercrime and the U.S.Justice System. In H. Bidgoli, *Custom Textbook for CSEC 620* (pp. 3-15). Hoboken: John Wiley and Sons.

Brussin, D., & Opatrny, J. (2009). Gateway Security Devices. In S. Bosworth, M. E. Kabay, & E. Whyne, *Computer Security Handbook* (pp. 26.1-26.33). Hoboken: Wiley & Sons Publishing.

Casey, E. (2011). Applying Forensic Science to Networks. In E. Casey, *Digital Evidence and Computer Crime* (pp. 633-670). Waltham: Elsevier.

Casey, E., & Schatz, B. (2011). Conducting Digital Investigations. In E. Casey, *Digital Evidence and Computer Crime* (pp. 187-226). Waltham: Elsevier.

Cobb, C., Cobb, S., & Kabay, M. E. (2009). Penetrating Computer Systems and Networks. In S. Bosworth, M. E. Kabay, & D. Whyne, *Computer Security Handbook Vol. 1* (pp. 15.1-15.36). Hoboken: John Wiley and Sons Publishing, Inc.

Deepa, N., Priyadarsini, S., Sathiyaseelan, R., & Kumar, V. M. (2012, November). Image Based DLP Security for Risk Professionals - A High Impact Strategy. *International Review on Computer and Software*, *7*(6), 2831-2836.

Goodrich, M. T., & Tamassia, R. (2011). *Introduction to Computer Security.* Boston: Pearson Education.

Kabay, M. E., & Robertson, B. (2009). Employment Practices and Policies. In S. Bosworth, M. E. Kabay, & E. Whyne, *Computer Security Handbook* (pp. 45.1-45.15). Hoboken: John Wiley & Sons.

Moser, A., Kruegel, C., & Kirda, E. (2007). *Exploring Multiple Paths for Malware Analysis.* Vienna: Technical University Vienna.

Nelson, B., Phillips, A., & Steuart, C. (2010). *Guide to Computer Forensics and Investigations.* Boston: Course Technologies.

Post, J. M. (2009). The Dangerous Information Technology Insider: Psychological Characteristics and Career Patterns. In S. Bosworth, M. E. Kabay, & E. Whyne, *Computer Security Handbook* (pp. 13.1-13.9). Hoboken: John Wiley & Sons.

Sophos AG. (2012, January 1). *Security Threat Report 2012: Seeing the threats through the hype*. Retrieved October 20, 2013, from Sophos: http://www.sophos.com/en-us/medialibrary/PDFs/other/sophossecuritythreatreport2012.pdf

Stallings, W. (2009). Operating System Security. In S. Bosworth, M. E. Kabay, & E. Whyne, *Computer Security Handbook* (pp. 24.1-19). Hoboken: John Wiley & Sons.

Street, J., Nabors, K., & Fritz, D. L. (2010). *Dissecting the Hack: The F0rb1dd3n Network.* Oxford: Syngress.

The Tor Project. (2013, October 18). *Tor:Overview*. Retrieved October 19, 2013, from Tor: https://www.torproject.org/about/overview.html.en