International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 5 –NOVEMBER 2014.

TRACKING THE HACKER WITH CYBER FORENSICS

R.P.S.P.Veerraju[#1] and B.V.S.T.Sai[*2]

[1]*Associate Professor, Department of IT, UshaRama College of Engg & Tech, Telaprolu, Vijayawada, A.P., India*

[2]*Professor, Department of CSE, St. Mary's College of Engg for Women, Budampadu, Guntur, A.P., India*

Abstract— With the increased use of Internet and information technology all over the world, there is an increased amount of criminal activities that involve computing and digital data. These digital crimes (e-crimes) impose new challenges on prevention, detection, investigation, and prosecution of the corresponding offences. Computer forensics (also known as cyber forensics) is an emerging research area that applies computer investigation and analysis techniques to help detection of these crimes and gathering of digital evidence suitable for presentation in courts. This new area combines the knowledge of information technology, forensics science, and law and gives rise to a number of interesting and challenging problems related to computer security and cryptography that are yet to be solved

Index Terms— Computer Forensics, Preserving digital evidence, computer forensics tools, Keystroke Logger

I. INTRODUCTION

Computer systems today provide the foundation of data storage for many businesses and a must have convenience for individuals. Customer records, account data, transaction records, personal identifying information, and other data rich information are available for use or to be protected from use or loss. In any case, an event that leads to the loss, theft, access (authorized or not), transmission or other use may be called into question to answer who, what, when, where, why, and how.

In the mentioned situations, computer forensics comes to the light in order to search, find, and protect system logs or application logs. This is because information regarding the location of the actual data or information relating to the actual data is very valuable in various instances.

Computer Forensics, thanks to the ever increasing use and dependence on computers, is becoming a growing and valuable field. Computer Forensics refers to "the use of analytical and investigative techniques to identify, collect, examine and preserve evidence/information which is magnetically stored or encoded" [1]. There are many instances of where crimes involving a computer need to be investigated. These crimes range from child exploitation to a network breach resulting in the theft of personal data or the destruction of digital information. In today's digital world, it is important to put a real person behind the keyboard of any type of cyber event, primarily in instances of cybercrime. Computer Forensics attempts to do exactly that. "The core goals of computer forensics are fairly straightforward: the preservation, identification, extraction, documentation, and interpretation of computer data [2]." In order to do this, there are generally two types of data that are collected in computer forensics. Persistent data, which is data stored on a local hard drive or another medium. This type of data is preserved when the computer is powered off. There is also volatile data, which is any data stored in memory, or exists in transit. This refers to data that is lost when the computer loses power or is turned off. This type of data resides in cache and RAM [3]. Depending on the nature of the crime, skill or knowledge the cybercriminal has relating to computers or origin of the cyber event, the digital evidence remaining as proof of the event may be limited. Also, what little evidence that is recovered, or could be recovered, becomes a vital part of the legal proceedings that could follow.

II. POTENTIAL EVIDENCE

First, let's focus on the idea of identifying what is potential evidence in a cyber-related crime. With computer related crimes, there are various locations evidence can be. "Computer evidence [can be] represented by physical items such as chips, boards, central processing units, storage media, monitors, and printers" [10]. It can be found on site in the form of hard drives in computer or laptops, flash drives, CD's or diskettes at the scene or at another location, it can be stored on PDA's, IPods, cell phones, smartcards and other electronic devices. Computer Forensic Specialists could find useful information stored in the Cookies folder, temporary Internet Files folder, examining stored Bookmarks, or other folders on the computer. One of the treasure troves of information can be found in a little known temp area known as file slack. File slack consists of "raw memory dumps that occur during the work session as files are closed. The data dumped from memory ends up being stored at the end of allocated files, beyond the reach or the view of the computer user” [21]. There is also valuable information that can be found on computer hardware equipment in a totally different location like the equipment of an ISP or within equipment at another business or home. Once potential evidence has been found, it must be collected. Even your favorite search engine companies like Google or Yahoo, have some method of tracking who runs searches and what they search for and since IP Addresses are unique identifiers, tracing crime related searches is not a far-fetched idea

Collecting information/evidence from computer media is similar and different, at the same time, as other physical evidence collection. First, it must be collected and handled in a manner not to damage it. Secondly, it is important to document every aspect of the evaluation and processing of the computer. Not only do you document the evidence found, but you document all of the software and versions used in the extraction of the evidence. The more documentation you have on the processes and methods used that leads up to the evidence that is found makes it creditable in court. This process is known as chain of custody, and it is a vital part of computer forensics and the legal system [13] . Many times, a computer forensic investigator has to make a difficult decision. Do they risk losing vital evidence by pulling the plug on a computer, or risk damaging it by attempting to collect data on a live computer? If they chose to work with the live system, it is important that the system activity and contents are captured. This means checking CPU activity and system memory, evaluate the active processes that are running at the time, documenting network connections, and evaluating open files. On the other hand, if the system is analyzed while the power is off, a more representative backup can be made, because the normal boot process changes to drive media, makes changes to files or temporary file information. This forensic backup differs from a normal backup, because this will image the entire drive[14]. There are many computer forensic tools on the market which will assist in collecting digital evidence. Tools like EnCase, Forensic Toolkit, and SleuthKit. EnCase can search a pc for Word documents that are password encrypted, extract Windows registry information, or recognize file types by their internal structures rather than by the file type extension [17]. Forensic Toolkit is one of the more powerful tools available. Not only can it analyze registry entries, decrypt files, and crack passwords using dictionary attacks. One of the more promising features is the ability to identify steganography [18]. The main concern with this powerful product is the potential use in negative ways, by hackers or other attackers. After all, this is a powerful decryption/password cracker tool. SleuthKit is an open source tool that focuses more on Unix computers, but it can show files, examine disk layouts and locate and extract partitions; even deleted ones [19]. After the task of collecting information/information, the real challenge is preserving it. One of the more promising freeware software options that can recover deleted files or partions is called Recover My Files. It is free to try and $69.99 to buy. It can even recover files lost in a computer format [20]. I was skeptical of this claim, but I was able to verify this after running it on my own computer. The software was able to find several virtual machines that I had created and deleted to test various Desktop and Server Operating Systems for other classes. Furthermore the software was able to recover the whole deleted virtual machines, as well as other files dating back eight months. This surprised me, considering when you delete a virtual machine file; the file is too large for the recycle bin and is lost beyond recovery. I assumed those files too large for the recycle bin were not kept in a temporary location, like other deleted files

III. PRESERVE THE INFORMATION

Preserving the information in the original state is the most important aspect of Computer Forensics. Some of the steps to preserving digital information as evidence include the following items: Evaluate the risk of turning off the computer system. There is potential useful information that is stored in memory (RAM) and will be lost. Disconnect the system from the network, because if it stays connected, an individual could cover his/her tracks by deleting log files and other data that could be used as evidence. This could cause issues if the computer is a vital part of day-to-day operations, like a server for example. Do not use the system in question to do anything. You could inadvertently overwrite valuable data. In some cases, the cyber-criminal might have planted a program that will erase data when triggered by some event (such as opening or closing a program). The issue is further clouded because digital information is easily manipulated. For instance, just opening a file changes the date and time stamp of a file. This can be exploited by a trained law professional to raise doubts about the validity of the evidence collecting process or the evidence itself [15]. It is my opinion that if trials for which computer related evidence was admitted, it would be easy to raise doubt in a jurors mind about the authenticity of the evidence, because the average person is weak at understanding technology and may be easily convinced to doubt the evidence

IV. TRACKING THE HACKER

After examining the logs and a reasonable interpretation of the hacker.s activities has been reached, a next possible step is to trace down the hacker himself. Unfortunately, this is rarely an easy task. The system logs are the only key to find out who is responsible for the attack. When an attacker invades a system, they often modify or delete logs that can be used to trace him, so it is good practice to set up your system so that logs are written to an offline file system as to prevent the hacker from accessing them. A similar practice should be adopted for the cryptographic checksums of system executables and system configurations. This will ensure that the system can be recovered successfully and perhaps even catch the person responsible. Network router logs can also be useful in finding a hacker as they record information about packets that pass through. If a general time frame for the attack can be determined, then it will be much easier to find relevant information on network logs. Once an IP address is determined to be the source of the attacks, a simple traceroute can find the system.

However, this system is likely to be simply another victimized system that the hacker has used, so this entire process must be repeated for that system and any other systems along the way until the hacker is ultimately found. Unfortunately, this is difficult because there are many barriers that prevent us from finding the perpetrator. If any compromised system along the way did not keep adequate logs, then the trail grows cold very fast. If the ISP of the hacker is uncooperative then tracing becomes difficult as well. Most difficult of all, if one of the compromised systems lies across international borders then things get a lot more complicated. It is because of these and other complications that can bring the hunt to a screeching halt. The best that can be done is to do the best we can to restore the services, learn from past mistakes, consistently update system security patches and to stay vigilant.

V. KEYSTROKE LOGGERS TO FIND THE SPY

Keystroke loggers run primarily in the background of a computer and many run in .stealth. mode, meaning they are not listed in process lists and hide the registry modifications it makes to system settings. Once each key is intercepted, the information may be stored somewhere on the computer (or a remote computer) to be accessed later or streamed, in real-time, over the network to the person who started the logging program. Keystroke loggers have become more advanced and now are capable of features such as notification for the logger.s initiator when specific behavior or content is encountered and can even record screenshots of anything that is displayed on the monitor at any particular event or at regular time intervals, allowing key loggers to become even more intrusive.

A key logger normally consists of two parts: a Dynamic-Link Library (DLL) file that performs the logging, and an executable (EXE) file that loads the DLL and sets the hook onto the keyboard28. A hook is defined as any mechanism that uses a function to intercept events before they can reach an application. The function can then change, manipulate, or discard (keyboard) events in any way before allowing them through to the destination application. Hooks come in two flavors: system-wide and thread-specific; key loggers use system-wide hooks. DLLs are files that contain functions (as well as other information) that can be linked to any application at run-time. When this is done, the functions in a DLL are attached to processes themselves and are mapped into the process’s address space, allowing them to be called from the process. DLLs are used for keyboard hooks because any application can then call the keystroke logging function in the DLL and enables recording of all keystrokes from all applications

Keystroke logging programs can be installed either in person who has physical access to the target computer, or remotely, either by a .Trojan horse. Application or by a hacker who has gained root access to a system. Once loaded, the keystroke logging software is virtually undetectable by the user. Key loggers normally use little memory and do not affect a computer.s performance, making it more difficult to detect. However, there are anti-snooping products available that claim to be able to find such key loggers by probing the resident memory and recognize the programs that exhibit devious behavior. Products, like one called KeyPatrol30, use behavior-detecting and patternmatching algorithms. Once a particular application has .hooked. the keyboard, the application can be easily found by detecting a procedure call to the keystroke logging function. Products also can search through resident memory and match applications against numerous known key logging programs; much like anti-virus software searches a computer for programs matching known viruses.

VI. CONCLUSION

With technology overtaking the face of businesses or personal life, it is time IT Professionals understand the importance of the data they contain. In the event of any cyber related crime, or potential crime, it is important to understand who, what, when, where, why, and how of the situation. Once that happens, we must begin to realize that all those answers could be contained in a digital format located within the hardware and software of a computer system or network. If we are a part of a business and suspect some cyber-crime has been committed against our organization, there needs to be a plan that has been tested and is in place. It needs to have procedures on who we should contact, how we should proceed until a trained forensic examiner can arrive, how our consumers must be notified and what we should or should not do regarding the affected system or device, keeping in mind that these systems or devices contain the evidence of the wrongdoing. This evidence is very sensitive and exploitable, so it must be handled with the same care and precision needed to preserve the frailest object. The first instinct may be to pull the plug or something else, but that might destroy all the evidence. Furthermore, as we become more and more we dependent upon computers, the stakes become higher for cyber criminals to free themselves of the tell-tell information left behind during their crimes or acts of illegal activity

VII. REFERENCES

[1] Computer Forensics World. “Computer Forensics Basics: Frequently Asked Questions”. (Online) Retrieved April 3rd, 2009,

[2] Dixon, Phillip D. “An overview of computer forensics”. 2005 Potentials, IEEE. Volume 24 Issue 5. IEEE International.

[3] United States Computer Emergency Readiness Team. “Computer Forensics”. (Online) Retrieved April 3rd, 2009

[4] United States Department of Justice. “Crime Scene Investigation: A Guide for First Responders”. (Online) Retrieved April 2nd, 2009,

[5] CNN News. “Caylee Blog”. (Online) Retrieved April 2nd, 2009,

[6] Marcella Jr., Albert J. “Cyber Forensics: A Field Manual for Collecting, Examining and Preserving Evidence of Computer Crimes". 2008. Taylor & Francis Group, LLC. Auerbach Publications.

[7] How Stuff Works. “How Computer Forensics Work”. (Online) Retrieved April 5th, 2009,

[8] Vacca, John. “Computer Crime Scene Investigation: Second Edition". 2005. Cengage Learning. Charles River Media, Inc.

[9] Information Week. “Data Breaches: Getting Worse Or Better?” (Online) Retrieved April 4th, 2009,

[10] Federal Bureau of Investigation. “Forensic Science Communications”. Volume 2 Number 4. (Online) Retrieved April 3rd, 2009,

[11] US Department of Justice. “Stored Wire and Electronic Communication Transactional Records Access” (Online) Retrieved April 4th, 2009

[12] CNN News. “Bill proposes ISPs, Wi-Fi keep logs for police”. (Online) Retrieved April 5th, 2009,

[13] McQuade, Samuel C. “Understanding and Managing Cybercrime”. (2006). Pearson Education, Inc.

[14] Bragg, Roberta Rhodes-Ousley, Mark and Strassberg, Keith. “Network Security: The Complete Reference”. (2004). McGraw-Hill.

[15] TechGenix. “Bill P reserving Digital Evidence to Bring Hackers and Attackers to Justice”. (Online) Retrieved April 12th, 2009,

[16] Hayes, Darren R and Qureshi, Shareq. “A Framework for Computer Forensics Investigations Involving Microsoft Vista”. 2008. Systems, Applications and Technology Conference, 2008 IEEE Long Island.

[17] Allen, William H. “Computer Forensics”. 2005. Security & Privacy, IEEE. Volume 3, Issue 4.

[18] Access Data. “Forensic Toolkit”. (Online) Retrieved April 13th, 2009,

[19] Sleuthkit.orf. “The Sleuth Kit”. (Online) Retrieved April 13th, 2009,

[20] Get Data Software. “Recover My Files”. (Online) Retrieved April 13th, 2009,

[21] New Technologies, Inc. “Computer Evidence Processing Steps”. (Online) Retrieved April 13th, 2009,