Available online at http://www.journalijdr.com

International Journal of
DEVELOPMENT RESEARCH

IJDR

ISSN: 2230-9926

International Journal of Development Research
Vol. 06, Issue, 01, pp. 6539-6546, January, 2016

Full Length Research Article

PERFORMING INFORMATION GOVERNANCE: GOLDEN TRIANGLE COMPONENTS FOR APTS COUNTERMEASURES

[*]Da-Yu Kao

Department of Information Management, Central Police University, TaoYuan City, Taiwan 33304

ARTICLE INFO

Article History:
Received 16th October, 2015
Received in revised form
12th November, 2015
Accepted 20th December, 2015
Published online 31st January, 2016

Key Words:
Advanced Persistent Threats,
Computer Hacking,
Digital Evidence,
Security Policy.

ABSTRACT

Advanced Persistent Threats (APTs) use multiple processes to break into a system, avoid detection, harvest valuable information, and inflict serious harm to an organization. It may help us perform information governance to implement security policies, identify risk assessment, and block computer packets. There is still a lack of standards in the APTs investigation processes. In order to obtain the required evidences in the court for prosecution, the golden triangle components (People, Process and Technology) for APTs counter measures have been carried out in this study. Since information security is vital for developing and running an efficient business, this study constitutes a strategic approach to improve the information security. The result of this study is also expected to improve the APTs investigation process and place emphasis on potential possibilities of gathered evidence. The golden triangle components of this proposed methodology is illustrated by applying to some APTs incidents in Taiwan.

INTRODUCTION

Thousands of organizations rely on the internet services. As the dependence on information systems grows, the internet security becomes ever more essential to any individuals. The increasing rate of cyber-attack crimes is a fact (Petrescu *et al.*, 2011). The cyber-attack process is usually focused on a particular system or set of similar systems. Throughout the attack process, offenders seek to cover or obfuscate their activities. Offenders may want to appear to be attacking from a different location than where they are physically located and wish to remove any traces of their activities on the system (Andress *et al.*, 2014). Several researches have been carried out in the domain of cyber-attack investigation. Each investigation is based on a set of activities that should be performed in or der to obtain the necessary evidences in the court (Roger and Achille, 2012). When an offender is detected and analyzed, systems administrators in MIS department should exercise a suitable response to the attack. They should be able to detect computer hacking activities and to initiate full-packet capture devices with some other preventive techniques once offenders pass the defensive technologies, such as Anti-virus, Firewall, Intrusion Detection System or Intrusion Prevention System. The response of various options should be available, and be accordant with the threat. It is possible to block or redirect any offensive packets (Vacca, 2014). Preventive measures are necessary and help reduce the risk of cyber offense, but it is practically impossible to prevent all attacks. Advanced Persistent Threats (APTs) are mostly a concern of governments, financial companies, and large organizations. APTs use multiple phases to break into a system, avoid detection, and harvest valuable information. They can inflict serious harm to an organization before an organization knows that it has been hit (Andress, 2014). APTs target specific system vulnerabilities and key people over the long term. Their sophisticated intrusions typically target specific users within organizations to gain access to intellectual property, commercial secrets, and any other valuable information available (http://www.mcafee.com/ us/resources/ white-papers/ wp-combat-advanced-persist-threats.pdf). While APTs use many of the same techniques as traditional attacks, they differ from common botnets and malware because they target strategic users to gain undetected access to key assets. The remainder of the paper is organized as follows. Section 2 reviews previous works on cyber-attack process in APTs attempt, and auditing components in prosecuting cyber offenders. Section 3 describes cross-strait computer hacking cases and performing information governance. The proposed golden triangle components for APTs countermeasures are further discussed and analyzed in Section 4. The conclusion is drawn in Section 5.

[*]Corresponding author: Da-Yu Kao,
Department of Information Management, Central Police University, TaoYuan City, Taiwan 33304.

Review

Cyber-Attack Process in APTsAttempt

The cyber-attack process in APTs attempt includes information reconnaissance, system access, privilege escalation, data exfiltration, and attack systems (Andress *et al.*, 2014; Luttgens and Pepe, 2014; Moore, 2010; Vacca, 2014) (see Fig. 1).

Information Reconnaissance

Offenders leverage information from various factors to understand their target (Luttgens and Pepe, 2014). They will likely identify individuals, get their email addresses conduct reconnaissance and discover information from the system. The target of privilege escalation is often root or administrator level access, giving us relative rights on the system (Andress *et al*., 2014).

System Access

Offenders can also modify interpreted scripts or shell scripts that are not secured properly, in order to pass operating system commands or gain direct access to an operating system shell. It can be accomplished through a different set of exploit methods (Andress *et al*., 2014; Moore, 2010). It all typically starts with spear-phishing emails, which include malicious links or malicious document attachments. Through social engineering offenders may find account names through searching the physical surroundings, or any similar tactics. Gaining access to a system can take place when offenders use various tools or methods.

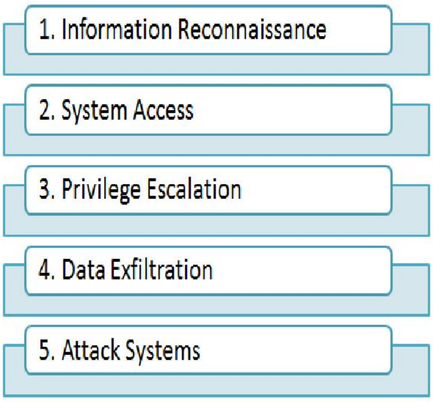

Fig. 1.Cyber-Attack Process in APTs Attempt

Privilege Escalation

Once offenders have gained some kinds of access rights to a compromised computer, they may need to gain additional or upgraded privileges (Vacca, 2014). Offenders may utilize the privileges of application programs that are operating with heightened permissions. For example, various daemons, or other running application processes may require higher privileges and can be often vulnerable to the flaw attacks of buffer overflows or race conditions. That is commonly known as privilege escalation.

- **Vertical privilege escalation:** Offenders attempt to gain access to a higher level of privilege accounts.
- **Horizontal privilege escalation:** Offenders attempt to gain access to a same level of different accounts.

Data Exfiltration

Offenders typically try to get domain administrative credentials and install malware via process injection, registry modification, or scheduled services (Vacca, 2014). Once offenders have gained the necessary access to the computer, offenders may find some particular transfer protocols to piggyback information across the network (Andress *et al*., 2014). There are a very wide variety of tools that offenders can use to exfiltrate data, or move data around. File transfers can be accomplished with FTP, TFTP, or any of a number of other common protocols.

Attack Systems

Running processes can be interrupted, and digital files can be deleted or manipulated (Andress *et al*., 2014). Although system attack can cause panic, causing disruption in any online systems is often a relatively easy proposition.

Auditing Components in Offense Prosecution

There is a lack of standards in the cyber-attack investigation processes. In order to obtain the required evidences that are needed in the court for prosecution, several works have been carried out in the domain of cyber-attack investigation. The identity or location of the offender is a critical issue in an offense (Marcella, 2008; Pande *et al*., 2014; Vacca, 2014). An initial interview of the suspect is an important chance of fact finding if he or she is a cooperative suspect. By using a variety of investigative skills, a suspect may reveal passwords and confess the offense (Marcella, 2008). Even though the discovery of an offender on the internet has encountered some obstacles, Fig. 2 explores the four auditing components in prosecuting cyber offenders.

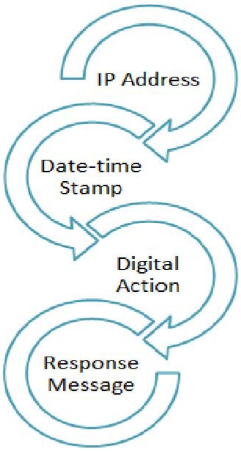

Fig. 2. Auditing Components in Offense Prosecution

IP Address: Offenders can use a series of intermediary hosts (called stepping stones or zombie computers) to carry out their attacks. IP address can be easily spoofed or forged. The offender may control innocent computers which are taken over by an exploit or malware. In practice, it might be possible to trace an offense back to the recorded IP address, but it does not mean that computer is the real offender of an offense.

Date-time Stamp: Date-time stamps are an important part of the computer forensic process.

Digital Action: Routers seldom keep digital action records of forwarded packets by design. More messages can be found from the relevant logs, such as system, event or security logs in Windows.

Response Message: If an offense occurs, investigators can query the relevant logs to examine whether this is a successful action or not. The kind of auditing logs is temporary instead of permanent so that log files will not run out of memory.

Sample Case

Cross-Strait Computer Hacking Case

Since 1996, Taiwan Criminal Investigation Bureau (under National Police Agency) has investigated cyber security breaches at hundreds of organizations in Taiwan. Cross-strait computer hacking cases in China and Taiwan usually aimed at cyber data theft. The data theft attempts have expanded from military and political data to technological and corporate data. For example, the information engineers of Taiwan Coast Guard Administration in June 2012 received system warnings which showed malware lurking in the servers, and attempted to attack its firewall. The engineers immediately blocked its network to prevent the outflow of secrets (http://www.wantchinatimes.com/news-subclass-cnt.aspx?cid=1101&MainCatID=11&id=20130321000109; http://www.wantchinatimes.com/news-subclass-cnt.aspx?id= 2012070 80 00008&cid=1101. 2012-07-08). A cyber-attack incident was apparently not an isolated incident. The securities of Taiwan government departments are also at risk. The majority of these security breaches are attributed to Advanced Persistent Threats (APTs). Some government or organizations might authorize this activity, but there's difficult to determine the extent of their involvement. The Chinese government is believed to employ nearly 100,000 hackers and their cyber army works around the clock to infiltrate companies and governments all over the world (http://www.wantchinatimes.com/news-subclass-cnt.aspx?id=20120708000008&cid=1101. 2012-07-08).

Performing Information Governance

The following threetraditional processes have beenhighlighted for performing information governance based on a cyber-attack situation (http://www.mcafee.com/us/resources/white-papers/wp-combat-advanced-persist-threats.pdf; Petrescu *et al.*, 2011; Vacca, 2014).

Implement Security Policies

The goals of security policies are to allow access for authenticated users, and to deny access to unauthenticated users (Vacca, 2014). The user community would prefer open access, whereas the network administrator insists on restricted and monitored access to the network. There is always the unauthorized user who perceives the potential flaw in the system (http://www.mcafee.com/us/resources/white-papers/wp-combat-advanced-persist-threats.pdf). It would be almost unrealistic to expect a built and secured network at all times.

Identify Risk Assessment

Proper risk assessment identifies the risks throughout an organization, and specifies the external and internal sources that an organization may face (Petrescu *et al.*, 2011). An organization should have a thorough understanding of critical business processes to enable the evaluation of risk mitigation plans.

Block Computer Packets

It is an appropriate response to prevent an infected computer from contaminating other computers in the context of malware (Vacca, 2014). Infectious malware requires connectivity between an infected computer and an offending source, so it is essential to interrupt that kind of data transfer. System administrators can utilize firewalls or routers with ACLs (Access Control Lists) to block computer traffic packets or can allow routers to selectively drop traffic. However, it will become almost difficult to trace back offenders once system administrators have blocked their hacking activities.

Golden Triangle Components for APTs Counter measures

Nowadays cyberattacks are deploying persistent and stealthy ways to evade the traditional security measures. Enhanced security measures are actually needed to sneak past those conventional security controls (http://www.mcafee.com/us/resources/white-papers/wp-combat- advanced-persist-threats.pdf).

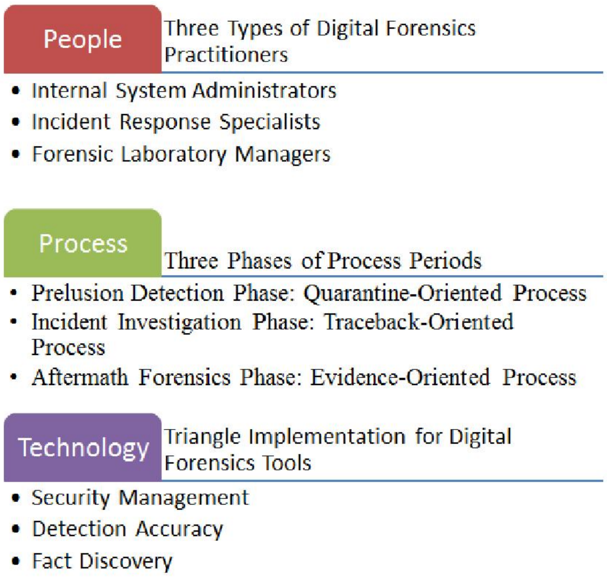
People
Three Types of Digital Forensics Practitioners
• Internal System Administrators
• Incident Response Specialists
• Forensic Laboratory Managers
Process
Three Phases of Process Periods
• Prelusion Detection Phase: Quarantine-Oriented Process
• Incident Investigation Phase: Traceback-Oriented Process
• Aftermath Forensics Phase: Evidence-Oriented Process
Technology
Triangle Implementation for Digital Forensics Tools
• Security Management
• Detection Accuracy
• Fact Discovery

Fig. 3. Tree-Component Discussions on Digital Forensics Tools

In Table 1, the golden triangle components of people, process and technology need to be rebalanced to fight against APTs in favor of organization policy.

Table 1. Golden Triangle Components for APTs Countermeasures

Phase Component	Prelusion Detection	Incident Investigation	Aftermath Forensics
People	Internal System Administrators	Incident Response Specialists	Forensic Laboratory Managers
Process	Quarantine-Oriented	Traceback-Oriented	Evidence-Oriented
Technology	Security Management	Detection Accuracy	Fact Discovery

Each incident response team had to evolve the truth from a mass of confused evidence. People, process and technology are all important components of APTs investigations and forensics (see Fig. 3). Many of the challenges need solutions in all three areas. Prosecuting the offender cannot be implemented successfully until the challenges practitioners face in each of these three components are addressed.

People: Three Types of Digital Forensics Practitioners

Not every organization has the potential of funding its own forensic laboratory. Organizations should have a potential capability to (Ligh *et al*., 2014; Malin *et al*., 2008; Marcella, 2008): (1) analyze volatile data and non-volatile data, (2) perform live acquisition and dead acquisition, and (3) process digital evidence. Without these capabilities, people will have difficulty in determining what the evidence shows, what kinds of events have occurred, how it happens and which data can be collected within it systems and networks. In a cyber-attack event, there are three types of digital forensic practitioners: internal system administrators, incident response specialists and forensic laboratory managers (see Table 1). ICT devices that contain potential digital evidence may be removed from their original location by internal system administrators or incident response specialists to a laboratory environment for later acquisition and analysis by digital forensic laboratory managers (ISO, 2012). Due diligence of examining digital evidence is an important factor to avoid accidents and error. Three types of digital practitioners including the following: internal system administrators, incident response specialists and forensic laboratory managers. They perform cyber-attack investigation or digital forensics at times. Some work directly for agency while others are part of private investigation company.

Internal System Administrators

Every cyber-attack investigation begins with a complaint. Whether a criminal, civil, or administrative investigation is undertaken, internal system administrators may receive an initial complaint from a number of sources by telephone, by walk-in or by someone's request for services (Stephenson, 2014). It is critical to begin the process of evidence preservation. The internal system administrators should focus on the human artifacts of unusual data after an incident had been detected and confirmed.

Ensure the Computer Security

Internal system administrators are individuals who are responsible for the reliable operation and security maintenance of computer systems. They seek to ensure that the performance, resources and security of the computers without exceeding the budget and to quickly recover form a security incident.

Perform an Initial Analysis

Every organization should have a basic capability in performing IT security functions or live response analysis. Live response handles network connection issues on a live system rather than on a forensic image. During the data analysis of live response, internal system administrators or incident response specialists may try to find more leads, and explain what happened. The results of live response analysis should help practitioners understand the unauthorized access to the compromised system.

Document All Steps

Every operation may change the computer status and can impede the forensic analysis. Documentation of a scene creates a record in the type, location, and position of computers and their peripheral equipment for the investigation (Johnson, 2013). The initial considerations use video, photography, notes or sketches to help reconstruct the details of the scene later (Moore, 2010). Changing the system as little as possible is standard practice. If the incident results in criminal proceedings, practitioners should document all the steps and hash the acquired data to vouch for the validity of the collected data.

Incident Response Specialists

Perform a Live Analysis

Incident response specialists are individuals who are authorized, trained and qualified to act first at an incident scene in performing digital evidence collection and acquisition with the responsibility for handling that evidence (ISO, 2012). A live response toolkit can collect relevant data from the target computer to confirm whether an incident has occurred (Casey, 2011). The live response data can be collected by running a series of commands. Each command produces data in an easily readable format.

Implement a Trusted Toolkit

If an offender has broken in and achieved administrator rights, practitioners must prepare some trusted tools to quickly analyze the compromised machine. When practitioners conduct live response forensics it is essential to implement trusted toolkits and linked libraries to acquire data from the examined system (Malin, 2008). Practitioners should never trust the compromised computer. Because the examined system has been potentially compromised, the native programs may be modified.

Use an Incident Response Toolkit

Using an incident response toolkit can quickly collect evidence at the incident scene. Practitioners can perform a whole analysis of a compromised computer and bring evidence to court.

Forensic Laboratory Managers

The easiest way to secure data to a forensic lab is by making an exact copy of a data storage drive onto a portable device.

Change Something in Destructive DNA Analysis

Traditional forensic disciplines such as DNA analysis show that measure of forensic soundness does not require the original to be left unaltered. Forensic analysis of the evidential sample further alters the sample because DNA tests are destructive (Casey, 2011). Despite the changes during processing, these methods are considered forensically sound and DNA evidence is regularly admitted as evidence.

Change Nothing in Digital Image Analysis

Some practitioners of digital forensics think that a method of preserving or examining digital evidence is only forensically sound if it does not alter the original evidence source in any way (Casey, 2011; Stephenson, 2014). However, setting an absolute standard that dictates "preserve everything but change nothing" is only possible in forensic laboratory. It is almost impossible to conform to such a standard at the incident scene. In some circumstances, the main reasons are (Bashir and Khan, 2013; Casey, 2010; ISO, 2012; Marcella, 2008):

- Many cases are handled at the same period;
- Many computers appear at the incident scene;
- There are time consuming jobs;
- There is limited man-power in digital forensic lab;
- That is inconsistent with other forensic disciplines (i.e., fingerprint process or DNA analysis);
- There is the loss of volatile data;
- It is dangerous in a legal context.

However, postulating the above ‘Change Nothing in Digital Image Analysis ‘standard as a best practice still opens digital evidence to criticisms.

Process: Three Phases of Process Periods

This handling process of potential digital evidence is divided into the following (Marcella, 2008).

Prelusion Detection Phase: Quarantine-Oriented Process

Prelusion detection phase includes identifying where the commencement of the incident is. If a full investigation is required, the initial information will lead the follow-up incident digital investigation and aftermath digital forensics.

Risk Assessments by Network Security Tools

Offenders often look for known weaknesses or exploits in the OS (Operating System) or any applications. There are the signs which indicate a potential area of concern, and which needs immediate attention. Some network security tools can be valuable in helping people conduct risk assessments of network’s vulnerability, monitor the time intervals between activities, build a database of suspicious signatures, and distinguish between legitimate and suspicious activity over a given period (Vacca, 2014). Sufficient preparation facilitates smooth execution and includes (Johnson, 2013):

- Detect intruder and collect the related information;
- Develop criteria on when to report an incident to the authority;
- Ensure needed services are available;
- Establish an information security policy;
- Maintain an approach to handle an incident.

Identify the Incident at the Commencement

Unsuccessful login attempts are a good indicator that a computer system has been targeted. When users enter a mistyped response, they usually correct the error on the next try. However, numerous mistyped commands or incorrect login responses can be a sign of brute-force intrusion attempt. At the start of any investigation, several questions must be answered by the responders and system managers immediately. Are there any file deletion activities? If so, incident response specialists must pull the plug cable out of the wall. This will freeze the computer and its network (Casey, 2011; Johnson, 2013). Let the forensic laboratory managers to obtain potential evidence later.

Initial Response Activities

Initial response is an activity that performs the initial collection and response steps on stolen data, network indicators, or potential subjects that can lead to the security incident (Andress *et al*., 2014). The goal of initial response is to gather enough initial information to determine the appropriate response. The initial response reviews network-based available data, determines the type of incident, and assesses the potential impact. Few organizations can fully prepare for data security incidents. Incident response is a coordinated approach and may include activities that (Bashir and Khan, 2013; ISO, 2012):

- Confirm whether or not an incident occurred;
- Document all the relevant information of the incident;
- Educate senior management;
- Implement a remediation plan against future incidents;
- Interview the person(s) who reported the incident;
- Keep that incident under control;
- Minimize the damage to network operations;
- Photograph scene, computer, monitor and screen;
- Provide rapid detection;
- Restore normal operations from the investigation;
- Review application, network and security logs to identify why an incident has occurred.

Incident Investigation Phase: Traceback-Oriented Process
This incident investigation phase is designed to be taken as soon as an incident occurs.

To generate a quick assessment of the event, collecting the first pieces of non-volatile/volatile data is critical. An incident means a threatening computer security breach. An incident response is the action which is taken to respond to a situation. Practitioners should ascertain the nature of the incident, the offender, the seriousness, scope, and potential consequences (Ligh *et al*., 2014; Roger and Achille, 2012; Shahabi *et al*., 2014; Vacca, 2014).

Electronic Equipment Identification

Practitioners seldom have time to methodically perform a comprehensive examination or analysis. Practitioners should identify all the electronic equipment used by the suspect. Additional imperative sub-procedure will be identifying fragile or volatile evidence.

Live Acquisition Process

Practitioners may collect evidence from the running system in incident investigation phase, and take the system down for imaging in aftermath forensics phase (Ligh *et al*., 2014). Live acquisition process can be set up to retrieve the date-time stamp, registry content, swap files, and memory details (Roger and Achille, 2012). Some fragile evidence will change or will be lost as the time goes by. The practitioners must try to obtain the necessary information at the incident scene. The collection of initial clues is a critical step in any investigation. In the incident period of digital investigation, law enforcement agents often ask help from computer experts to be the first incident responder. The evidential phase of identification and collection on a live system is crucial to analyze any suspicious activities. The memory artifacts on the examined computer are also essential to find some past clues to support or refute the offender (Bashir and Khan, 2013). Once systems have active indicators of compromise, collecting some artifacts becomes crucial for latter analysis.

Volatile Evidence Collection

Because the digital file contents can be changed, the volatile evidence may be lost soon. To obtain better results, it is suitable to use proper tools in collect evidence. The network evidence includes capturing, recording, or analyzing network audit trails in order to discover the source of incident problems. Not all the recorded information can be useful for later prosecution. Network connection status is based on audit trails, but it often encounters the integrity problem. This stage involves proper documentation of the crime scene along with photographing, sketching and crime-scene mapping. Components under the incident period are defined as follows (Davidoff and Ham, 2012; Johnson, 2013; Ligh *et al*., 2014; Roger and Achille, 2012):

- Analyze the activities of suspicious malware or activities;
- Assess the attack damage;
- Determine the initial attack vector;
- Establish the time frame of the incident;
- Explore how the systems were affected;
- Interview management staffs who may provide a context for the incident;
- Interview MIS staffs who might have insight into the technical details of an incident;
- Observe the ongoing incident.

Evidence Documentation Preservation

Any changes to a system must be documented when practitioners access the original drive. Screen snapshots in time can provide a clue with valuable information when practitioners get access to the system (Andress *et al*., 2014). It is important to decide what type of evidence to collect at the incident scene (Roger and Achille, 2012).

Aftermath Forensics Phase: Evidence-Oriented Process

The goals of aftermath digital forensics are to successfully report an incident which is followed by determining the root-cause of the incident, identifying the perpetrator, and linking accomplices to the incident (Andress *et al*., 2014; Johnson, 2013).

Forensic Imaging for Evidential Preservation

A bit-stream copy of the entire media being imaged is created to prevent contamination and maintain evidentiary status (Andress *et al*., 2014). A forensic examination performed on disk images is a time-consuming task. That forensic imaging is an accepted standard for the evidential preservation. The image can be stored on a durable medium such as a hard drive, and is used as the working copy for examination and production of evidence.

Lab Experiments on a Dead System

Aftermath digital forensics refers to collecting all the static evidence remaining, such as an image of a hard drive. Digital evidence can be collected from computers, cell phones, PDAs, hard drives, or USB memory devices. When practitioners acquire digital evidence, preservation of evidence is vital to avoid spoliation of crucial evidence. Acquisition of evidence starts by creating a forensic image. In the aftermath period of digital forensics, digital forensic practitioners can do some lab experiments on a dead system. Each file is somewhat different from others. Profiling file signature and its attributes can be useful to identify offenders or make some judgments. Special care must be taken when practitioners handle digital evidence and associated artifacts.

Restore Operations to Normal Status

Aftermath period includes identifying how to recover from the incident, and how to get back to normal business sooner. The post incident effort of ensuring the learning process is to reflect new threats, improved technology and learned lesson. These lessons can improve the incident handling and response mechanisms within response team (Johnson, 2013).

- Determine the root cause of an incident;
- Find further potential damages from the same root cause, and eradicate it;
- Get involvement of system owners to test the system;

- Improve defenses and perform vulnerability analysis;
- Restore from backups to achieve a clean state of system.

Technology: Triangle Implementation for Digital Forensics Tools

Every conclusion of APTs investigation should be presented along with all of a forensic conclusion and supporting evidence. The technical nature of cyber-attack investigation contains data discovery and retrieval (Davidoff and Ham, 2012; Vacca, 2014).

Security Management

If an organization uses some security management procedures, internal system administrators can implement effective controls. Security management consists of identifying information assets, implementing security policies for protecting these assets, assessing the controls to face those threats, determining the risks' consequence, prioritizing the type of risk, and selecting appropriate risk response.

Detection Accuracy

Detection accuracy is the critical problem for security solution. Any security solution should ideally minimize false positives (normal incidents mistaken for suspicious ones) and false negatives (malicious incidents escaping detection).

Fact Discovery

The interpretation and presentation of factual evidence should be free from bias to provide decision makers with the forensic view of the facts. A fact is based upon the evidence identification of high statistical confidence: admissibility of the evidence and degree of proof. Forensic science provides a large body of proven investigative techniques and methods for achieving the investigative ends. A characteristic of evidence should satisfy its suitability for admission.

Conclusion

Internet has become an essential component of our daily activity. As the cyber-attack increases in the modern society, there is an urgent need to set up a standard which takes into account the internet security issues. Organizations must lead a coherent response to global APTs incidents, and a strategic approach is fundamental to achieving this aim. This study proposes golden triangle components (people, process and technology) for APTs countermeasures that can be considered as a basis for standardization. Having the right balance of people, process and technology can help practitioners adopt a holistic view of the entire incident response team, to make right choices in prosecuting offenders. The proposed components are constructed by extending and unifying the existing approaches.

Acknowledgements

This research was partially supported by the Ministry of Science and Technology of the Republic of China under the Grants MOST 103-2221-E-015-003-.

REFERENCES

Andress, J., Winterfeld, S. and Ablon, L. 2014. “Cyber Warfare: Techniques, Tactics And Tools For Security Practitioners (2nd Edition),” Burlington, MA: Elsevier Inc., pp. 181-192.

Atheist, P. Feb. 23, 2013. “Mandiant Executive Summary: Exposing One of China’s Cyber Espionage Units,” http://chinadailymail.com/2013/02/23/mandiant-executive-summary-exposing-one-of-chinas-cyber-espionage-units/.

Bashir, M. S. and Khan M. N. A. 2013. “Triage in Live Digital Forensic Analysis,” The International Journal of Forensic Computer Science (IJOFCS), vol. 1, no. 1, pp. 35-44.

CAN, “China Hack Attacks A Serious Threat to Taiwan: Security Chief,” http://www.wantchinatimes.com/news-subclass-cnt.aspx?cid=1101 &MainCatID=11 &id=2013 0321000109, Mar. 21, 2013.

Casey, E. 2010. “Handbook of Digital Forensics and Investigation,” Burlington, MA: Elsevier Inc., pp. 21-208.

Casey, E. 2011. “Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd Edition),” Waltham, MA: Elsevier Inc., pp. 187-306.

Davidoff, S. and Ham, J. 2012. “Network Forensics: Tracking Hackers through Cyberspace,” MA: Pearson Education, Inc., pp. 1-72.

ISO (International Organization for Standardization), “ISO/IEC 27037:2012 - Information Technology: Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence,” Switzerland: ISO Office, 2012.

Johnson, L. 2013. “Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response,” Burlington, MA: Elsevier Inc., pp. 97-184.

Ligh, M. H., Case, A., Levy, J. and Walters, A. 2014. “The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory,” Indianapolis. IN: John Wiley & Sons, Inc.

Luttgens, J. T. and Pepe, M. 2014. “Incident Response & Computer Forensics (3rd Edition),” New York: McGraw-Hill Education, pp. 1-50.

Malin, C. H., Casey, E. and Aquilina, J. M. 2008. “Malware forensics: Investigating and Analyzing Malicious Code,” Burlington, MA: Elsevier Inc., pp. 93-282.

Marcella, A. J. 2008. “Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes,” Auerbach Publisher.

McAfee, “Combating Advanced Persistent Threats: How to Prevent, Detect, and Remediate APTs,” http://www.mcafee.com/us/resources/ white-papers/wp-combat-advanced-persist-threats.pdf, May 4, 2012.

Moore, J. W. 2010. “From Phishing to Advanced Persistent Threats: The Application Of Cybercrime Risk To The Enterprise Risk Management Model,” Review of Business Information Systems, Fourth Quarter, vol. 14, no. 4.

Pande, P.V., Tarbani, N.M. and Ingalkar, P.V. 2014. “A Study of Web Traffic Analysis,” International Journal of Computer Science and Mobile Computing (IJCSMC), vol. 3, no. 3, pp.900 – 907.

Petrescu, M., Popescu, D. M. and Sîrbu, N. May 2011. The Challenge of Ensuring Business Security in Information Age, Review of International Comparative Management, vol. 12, no. 2, pp. 326-331.

Raghavan, S. 2014. “A Framework for Identifying Associations in Digital Evidence Using Metadata,” Brisbane: Queensland University of Technology Dissertation, pp. 73-124.

Roger, A. E. and Achille, M. M. June 2012. “Multi-Perspective Cybercrime Investigation Process Modeling,” International Journal of Applied Information Systems (IJAIS), *Foundation of Computer Science* FCS, New York, USA, vol. 2, no.2.

Shahabi, C., Kim, S. H., Nocera, L., Constantinou, G., Lu, Y., Cai, Y., Medioni, G., Nevatia, R., and Banaei-Kashani, F. Mar. 2014. "Janus - Multi Source Event Detection and Collection System for Effective Surveillance of Criminal Activity," *Journal of Information Processing Systems*, vol. 10, no.1, pp. 1 – 22.

Staff Reporter, “China hacks Taiwan's Coast Guard,” http://www.wantchinatimes.com/ news-subclass-cnt.aspx ?id=20120708000008 &cid=1101. 2012-07-08.

Smiraus, M. and Jasek, R. 2011. “Risks of Advanced Persistent Threats and Defense against Them,” Proceedings of the 22nd *International DAAAM Symposium*, vol. 22, no. 1.

Stephenson, P. 2014. “Official (ISC)2® Guide to the CCFP CBK,” Boca Raton, FL: Auerbach Publications, pp. 293-404.

Vacca, J. R. 2014. “Cyber Security and IT Infrastructure Protection,” Waltham, MA: Elsevier Inc., pp. 233-246.

Vacca, J. R. 2014. “Network and System Security (Second Edition),” Burlington, MA: Elsevier Inc., pp. 29-189.

Yadav, S. 2011. “Analysis of Digital Forensic and Investigation,” VSRD *International Journal of Computer SCI. & Information Technology*, vol. 1, no. 3, pp. 171-178.

****