2015 International Conference on Computational Science and Computational Intelligence

Incident Response through Behavioral Science: An Industrial approach

Arvinder Pal Singh Gagneja
Dept. of Psychiatry
ASANTE
Medford, USA
Arvinder.gagneja@asante.org

Kanwalinderjit Kaur Gagneja
Dept. of Computer Science
Southern Oregon University
Ashland, USA
gagnejak@sou.edu

***Abstract*— We can apply psychological methods and behavioral science to understand the practices, techniques, processes, and skillset cyber-criminals are using nowadays for cyberattacks. We can setup honeypots to observe the techniques and methods used for attacks through logs and security settings. However, setting up a honeypot is very expensive and time consuming. So we have to work with our running systems and need to go through the logs and security settings. This way we can build a description of mind set of the cybercriminals behind the cyberattack. This description could be used as a new vector in finding infiltration method. The specific infiltration could signify a tenacious threat or just one time incident. This vector, if applied correctly, could lead to finding threats and risks relatively easily. This vector could also reduce the time required to investigate the incident. Security incident response is centered on detection, response, and resolution of the incident. Once you know the intent behind the incident, incident response becomes much easier.**

Keywords—Security; response; prevention; detection; breach;

I. Introduction

Incident response is an attack management technique to some security breach or cyber-attack so as to minimize the loss. Once an event or an attack is detected, to comprehend the compromise a sequence of events is reconstructed. Hence the outcome is considered as a weakness in the system and based on that the vulnerability is recognized [4]. All incident management techniques support different technical methods for investigating, understanding and to protect the organizational systems.

In this paper we are trying to construct categories of hackers based on the behavioral science. Through literature we have found out that among hacker community, there also exist stereotype categories. In the given process, initially we established the technical threats to understand the motive of the hackers. To do this we applied the psychological model to construct the factors those may have motivated the hacker's mind. If construction of factors is done appropriately, then motivation factors are applied to the approaches of hacking techniques. Then statistical tools discover what type of hackers is involved in the attack [11].

There are numerous attacks against institutional computers, applications and their networks. These attacks are so prevalent that they are pushing corporations and organizations to pay attention on upgrading their security systems and improving their response management and incident response.

Any significant network or security breach can lead to loss of personal data or intellectual property. It can also lead to customer and shareholder lawsuits. Sometimes these breaches could lead to compliance audits and even sanctions. Usually these breaches are not made public for the good will and security of the organization. However, the records show that 783 data breaches occurred in 2014. Identity Theft Resource Center [1] tracked and reported that it has increased by 30 percent in comparison to 2013.

It is really difficult to compute the total damage in figures. However, the calculated loss to the organizations because of these breaches is in billions of dollars annually. One hacking gang known as Carbanak alone has used advanced persistent threat (APT) technique against over one hundred banks (any size) and they have cheated these banks for over $1 billion dollars in the past two years [2]. The retail store –Target's security was breached in 2013 during thanks giving season. The analysts predicted that this breach could cost the retail store-Target over $1 billion, since it lost records for 110 million customers' payment card transactions.

The paper is organized as follows: Section II elaborates on what is the need to study the behavioral science behind incident response. Section III describes the categorization of hackers based on their behavior, motivation and techniques that they use to hack. Section IV discusses the motives behind hacking Section V generates the description of hacker during incident response when some system is compromised. Section VI gives our proposed Incident Response based on hackers' behavioral description. Section VII concludes the paper.

II. Need

What is the need to study the behavioral science behind incident responding! The behavioral science refers to unconcealed actions; to fundamental psychological progressions for instance temperament, emotion, cognition, and motivation. The incident responders should be trained about

978-1-4673-9795-7/15 $31.00 © 2015 IEEE
DOI 10.1109/CSCI.2015.170

the behavioral science back ground of hackers or attackers, while handling such incidents, so that they can determine the incident effect and the motive behind such an incident. The computer systems at organizations should be hardened enough so that whenever some attack occurs, incident response could determine the motive, reason, and mindset behind such an attack [3].

III. CATEGORIES OF HACKERS

The paper presents a categorization of hackers based on their behavior, motivation and techniques that they use to hack. Once such elements are known the humans at the other end guarding their vicinities could have another tool to hamper or prevent such attempts from occurring [12].

During incident response at some point behavioral science is applied to establish different reasons or factors.

How did they found where to find the information? Did they use some insider to reveal the information? How effective was the search methodology? Was the information gathering process a complete download or just partial records were collected?

What steps they followed after they got the information? Did they remove some items or records? If yes, how do they affect the existing system or who could benefit from that? What steps were taken to cover the attack?

A number of such questions could be asked to reveal the information about the attack. However, coming up with the right questions during incident handing is the key to close the case successfully otherwise usual incident response could miss a lot of it. If you know what, why, and how you have won half the battle. Then applying behavioral description to these factors, you could win the complete battle.

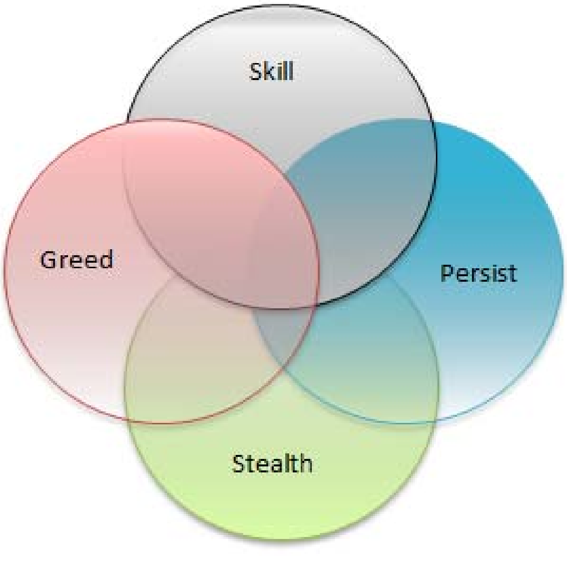

Figure 1: Assessment of hacker

There are various types of hackers based on several characteristics such as motive, action, understanding and depth of applying numerous techniques to achieve their motive. These characteristics are used to build behavioral description of hackers. However, this description may change depending on the earth boundaries (countries) or the skillsets possessed by the hackers [9]. The following table I present various categories of the hackers in a simplified manner based on intentions, activities, and expertise. Only the mentioned categories are referenced further in this paper.

Table I: Hacker Categories

Hacker Type	Activities	Intention	Examples
Beginner level	-no particular objective -a lot of missed tries	Inquisitiveness	Newbies, tinkerer, and fiddlers
Insider	-working or ex-employee	Retribution	Trying to break or steal from internal system
Secret Agent	-country -state	Surveillance, reconnaissance, spying	National security, knowing the enemy or friend
Terrorist	-Intrusion, infiltration, stealing, destroying records	wreaking havoc	Sony systems hacking
Well thought-out crime	-making money	Stealing money	Hacked celebrity photos

The following are the metrics those are used for description building for various types of above mentioned hackers. Figure 1 represents how these factors contribute together for some hacker to perform malicious activity:

- Skill sets: This metric is to determine that how good is hacker with his technical skills, as well as with social engineering skills. Technical skills further could be characterized into computer programming, computer security, and computer system management etc. Better the skills more damaging the hacker.
- Persistence: This metric is to determine that how much time and effort is invested into understanding the compromised system. How much meticulousness is used? What different tools and resources are used to attack the given target?
- Greed: This metric is to determine that what the basic necessity behind such an attack was on the part of hacker. This

metric explains the hacker's greed in terms of money, satisfaction, ego, and superiority etc.

- Stealth: This metric is to determine the hackers' talent to operate and break into the existing systems without being identified. The hacker has the capability to remotely attack the system and modify system logs or steal important information such as drug formula or trade secret without getting detected.

IV. MOTIVES BEHIND HACKING

a) Community vs individual

Hackers live in society so they socialize and are part of a community. However, they also have online associations, a platform for the hackers to do their malicious activities [1]. The following equation (I) presents cost vs benefit for the motivation for some malicious activity.

$$CM = (\beta * \alpha) - (\lambda * \gamma) \qquad (I)$$

The CM stands for Criminal Motive. An, α represents the attained probability, that is what they achieved by doing this malicious activity. The β represents the benefit, how much they gained with this malicious activity. The γ represents realization probability, means what are the chances that they were successful executing their plan. Finally the λ represents the projected disadvantage, means doing this activity how much they will have to pay in terms of social justice [8].

Since hackers may be operating in group, so the criminal motive (CM) is dependent on what the principles are of the group, what is the motivation behind the hack, such as newbies or insiders or spies or terrorists or organized criminals? Knowing the motive to hack and the category involved in hacking the values of parameters in eq. (I) will change. In some circumstances, we will find that criminal motive could be low; however the benefits could exceed the projected disadvantages.

Any group is comprised of individuals, and the individual live in society and community. Therefore, within that group some members could be resistant or afraid to perform the malicious activity. On the other hand some members with lower conscience could be willing to perform such acts for the benefits.

b) Social Learning Theory

In society people interact with each other and learn from each other. Hence this interaction is a tool to build good behavior and personal characteristics [5]. However, the cyber world is not connected as the societies or communities are. Given the fact that cyber world is faceless people don't mind performing malicious activities.

c) No sense of personal identity

Internet does not reveal your personal identity, so the level of societal constraints is low. This factor gives the hacker the ability to perform malicious activities without being recognized in the society [14].

d) Moral detachment

The hacker performing malicious activity thinks that it is the owner's responsibility to protect their systems. If the system has a security hole or lacks specific protection level then it is the systems' weakness and he has every right to exploit that weakness [2]. Due to moral detachment the hacker believes that it is the responsibility of system owner to protect his assets in a manner that any malicious activity could be stopped.

V. DESCRIPTION OF HACKERS

Realization of the hacker's intention and skill set used in the cyberattack are mandatory for the incident response. The system security is enhancing gradually, but man made attacks are also increasing. Generating behavioral science hypothesis could help formulate one more level of security for such malicious activities [7].

The description of hacker is created during incident response when some system is compromised. The description of hacker is prepared using figure 1 with respect to table I.

a) Beginner level

There are number of tools and scripts those could be used by such hackers. These tools are enough good that these can penetrate through IDS (Intrusion Detection Systems) and firewalls without even being detected. However, good log analysis in terms of physical layer traffic can show the attempts made to break the system. These logs can provide evidences of multiple failed tries or use of resources after normal working hours above and beyond the usual usage scale.

b) Insiders

It is really difficult to find someone that is an insider. He has all the rights to perform his/her duties as an insider. It becomes difficult to find someone at the security analyst or system admin levels. One example of the insider attack was on the public owned oil enterprise Saudi Aramco. This attack deleted records on almost 30,000 computers owned by the enterprise by means of a virus known as Shamoon. The forensic experts analyzed the logs and other events and discovered that some insider was engaged in performing this attack, which had access to Aramco's infrastructure and networks. Shamoon virus may have been bring in at the work place on a thumb drive that may have been inserted into a networked computer system controlling many computers. In such situations developing behavioral description of all the employees controlling enterprise systems is really a good idea. This is particularly important when we know that specific employee has the intention of leaving the enterprise. Such employee will demonstrate aggressive or pessimistic behavior and would not be contributing much in the business success.

c) Secret Agents

Secret Agents groups are usually run by national organizations. Britain, China, South Korea, and US has such hacking groups. These groups basically function to gather intelligence as directed by government agencies. Very current and new threat is Advanced Persistent Threats (APT). These groups poses extremely skilled hackers are usually very well-funded and they work on particular motive; generally established by a national organizations and execute APT. If we talk of nation China alone, it poses six "technical reconnaissance bureaus". They execute APT attacks on enterprises or countries selected by the Chinese government.

d) Terrorist

Cyberterrorism is terrorism through Internet. Terrorist do it deliberately to gain some motive. It could be at large scale or it could be at small scale by using some tools such as viruses, worms, crawlers, or spiders etc. In 2014 they compromised the website of Sony. They were having some issues with the movie 'The Interview' made by Sony. The terrorists also issued a threat that there will be violence against this movie watcher. The behavioral science behind such attacks is to achieve their motive and it could be any [6].

e) Well thought-out crime

In this category the hackers' main motive is to make money. During the malicious activity they keep monitoring every change in the compromised system. However they hide themselves in a manner that they should not be detected, so that they can keep making money [10]. These attacks are generally conducted through phishing or spam or online theft or by using destructive code for identity theft.

The hackers with good social engineering skills get successful in performing such attacks. Such hackings are difficult to detect. Moreover, it is also difficult to train the staff against such social engineered attacked. Usually the staff deals with day today stuff and it does not occur to them that it is a plot for an attack. Therefore, response to phishing or spam varies from person to person. One person may give away all information to a request for information other may not. Again one individual may click on a link to phishing website without reviewing it and other may not. To stop such situations from happening the staff should be trained not to give away personal information without knowing that they are giving the information to authorized personnel. The system admins should keep reviewing the fake URLs and should submit them as malicious websites.

Cyber laws vary from country to country. These hackers could use these boundaries to their favor, because enquiries, investigations, court hearings and trial etc. become enormously hard.

VI. PROPOSED INCIDENT RESPONSES

A. Point of Sale Intrusion

i) **Symptoms**: The data is compromised at Point of Sale in the form of Payment Card Industry (PCI), because the systems of some businesses are configured poorly, so are vulnerable. The law enforcement or banks or other fraud detection agencies detect these compromises.

ii) **Current Response**: The hackers attack small business groups, with small infrastructure and low security. Once the attack occurs, it could take a week or over 10 days to detect 90% of such cyberattacks. The organization may lose billions of dollars if such attacks are not detected immediately.

iii) **Proposed Incident Response**: To protect their businesses from such attacks they should do the following repetitive activities: Keep strong password at Point of Sale. Add routinely authentication and intrusion detection. Point of Sale command server should not be directly connected to Internet. These steps will help businesses in closing the security gaps since it will eliminate tampering of Point of Sale systems. For Payment Card Industry (PCI) data protection, businesses should setup checks around the systems storing and using customer's data. Such systems should be Payment Card Industry (PCI) and Data Security Standard (DSS) compliant.

B. Web-based Application

i) **Symptoms**: Well thought-out crime group use business website to access the customers' accounts. They install malware on the business server such as spyware or keylogger to collect the customer's credentials. The hackers can also use SQL injection and cross site scripting in such attacks.

ii) **Current Response**: About 15% of the customers purchasing online caught the attack. Given the fact that they noticed a purchase they never made or strange changes to their accounts they never made.

iii) **Proposed Incident Response**: The hacker steals the credentials and then uses them to make money. The incident response demands proper monitoring of logs and events. Once vulnerability is found don't leave that open, close it immediately to eliminate the threats. Some websites keep posting recent vulnerabilities about windows, linux, and Mac operating systems. So those sites should be checked regularly to close mentioned vulnerabilities.

C. Insider

i. **Symptoms**: It is really difficult to find someone that is an insider. He has all the rights to perform his/her duties as an insider. It becomes more challenging to find someone if he is at the security analyst or system admin levels.

ii. **Current Response**: Presently companies only do background checks or they contact previous employer to see if the candidate is good for the position. Also nowadays interviews are conducted in a manner to find if the candidate is trustworthy.

iii. **Proposed Incident Response**: Security Information and Event Management (SIEM) system should be used. SIEM systems generate real-time breakdown of any security alarm whistled by the event logs or organizations hardware. The websites should be equipped with Data Loss Prevention (DLP) scheme. DLP if implemented checks that customer or internal user is not sending sensitive information outside the organizations network. Who accessed the companies 'trade secret' or 'Crown Jewels' such as Pepsi formula or Kentucky Chicken recipe should be monitored all the time and only those should be able to access such information those have the right to do so.

D. Stealing your IP orIP theft

i. **Symptoms**: Your cyber business IP is very important and it should be protected at all times. It is very difficult to detect IP theft and if the response time is in months or years your business may have lost in billions of dollars. IP theft is generally done with the assistance of an Insider.

ii. **Current Response**: The cyber businesses try to protect their IP's, nevertheless from outside intruders.

iii. **Proposed Incident Response**: To protect the business IP Security Information and Event Management system and Data Loss Prevention systems should be used in conjunction. System logs should be audited regularly. Who can access what, needs to be reviewed frequently. A person coming from a competitor or joining the competitor should be monitored carefully.

E. Mistakes

i. **Symptoms:** If someone sends a link that is a phishing link or sends a compromised file through an e-mail and one employee hit the link or opens the attachment without even aware of its consequences that a malware will be executed over all the networked computers, then it is mistake.

ii. **Current Response**: Presently, awareness training is conducted for the employees. They are informed about the procedures and policies those should be followed if some situation arises.

iii. **Proposed Incident Response**: Behavioral Science could detect if the act is performed by an Insider or someone hit the wrong button by mistake. You could defend your infrastructure by properly configuring the Security Information and Event Management system. This is really good tool to categorize the behavior of inside staff and the infrastructure of the organization.

F. Crimeware

i. **Symptoms**: A software or malware written particularly to perform cybercrime automatically to gather either customers' credentials or to collect money or to gather secret data without being detected.

ii. **Current Response**: Presently, system admins keep checking the known vulnerabilities in their web applications. Another preventive measure is system hardening to stop the entry of malware in the organizations network.

iii. **Proposed Incident Response**: Train the staff and system admins how to check for social engineering attacks and show them how to use Intrusion Prevention System (IPS). Educate them about vulnerability management as well. This for sure can prevent Crime ware.

G. Card Readers

i. **Symptoms**: The hackers install card readers at the Point of Sale terminals or ATM machines that transmit the credential information of the customers to the hackers.

ii. **Current Response**: This attack is considered unavoidable and uncontainable.

iii. **Proposed Incident Response**: Cognizant evaluation of point of sale terminals and ATM machines could focus on such strange card readers.

H. Denial of Service (DoS) attack

i. **Symptoms**: With DoS attack, the attacked system crashes since all its resources are occupied to the fullest and it fails to provide services to the incoming requests.

ii. **Current Response**: Intrusion Prevention Systems are used. To avoid the DoS attack upstream filtering is used. DoS attacks are also avoided by limiting the traffic rate.

iii. **Proposed Incident Response**: Intrusion Prevention Systems should be automated for DoS attacks. Black holing technique could be used to understand which attack dimension could be used and who could be performing DoS attacks, such as insiders or newbies or IP thieves.

I. Surveillance

i. **Symptoms**: Such attacks target the IP of the company or the business.

ii. **Current Response**: Presently, 2-factor authentication is used. For different users in the company, the privileges are set to "need to know" level.

iii. **Proposed Incident Response**: Try to find the intent or motive behind the espionage or criminal motive. Being system admins or security analyst you should know what to protect, like trade secrets or crown jewels of your business. You should also be aware of the fact that only skilled hacker will attack your business secret. You should implement access control strategies. Put in place the authentication procedures. Keep monitoring the protection mechanism and sensors internal to the network.

VII. Conclusions

In the US alone in last one to two years, the number of cyber-attacks and breaches has increased without measures. Some of the examples are Sony and Target. The companies running their businesses over Internet should supplement their security. Incident response handles the repercussion of any cyber-attack or breach. The incident response is performed in a way to reduce the damage and cost and shorten the recovery time. Knowing what was the intent of the hacker and to which category he belonged makes extremely easy for incident handler to put together pieces of puzzle for such an attack. If it is established that the hacker was trying to make a name for him then just close the vulnerability he used to crack the system, so that this entry point is closed for him. However, if the hacker is associated with larger group such as terrorist group or Secret agent group then view this incident as high alert incident. After closing the vulnerability keep watching your system 24X7 (twenty four X seven) or all the times for any new developments. The hacker group are generally technically strong. However, you should also be enough strong technically. First, to detect the attack; second to stop the attack immediately to minimize the damages. So generating behavioral description is an added tool to your skillsets. Therefore, being prepared for any cyber-attack with behavioral description of the attacker will permit the incident responder to make well thought out decisions.

Acknowledgment

Enormous gratitude to ETIC, and Oregon University System for supporting this research.

References

[1] Adam Bossler, George Burruss, "The general theory of crime and computer hacking: Low self- control hackers?", Idea Group Inc. (IGI), pp. 38-40, 2010.

[2] Albert Bandura, "Selective Activation and Disengagement of Moral Control", Journal of Social Issues, Vol. 46, No. 1, pp. 27-46, 1990.

[3] Bernadette Schell, "Hacker Psychology", 2013 http://www.happyhacker.org/gtmhh/bank5.shtml last accessed Aug. 2015

[4] Chad Cook, " An Introduction to Incident Handling", Symantec. http://www.symantec.com/connect/articles/introduction-incident-handling last accessed Aug. 2015

[5] Christian S. Fötinger, Wolfgang Ziegler, "Understanding a Hacker's Mind–A psychological insight into the hijacking of identities," Danube-University Krems, Austria, 2004. http://www.donau-uni.ac.at/de/department/gpa/informatik/DanubeUniversityHackersStudy.pdf Last accessed Aug. 2015.

[6] David Robb "Sony Hack: A Timeline", Deadline.com, 2014 http://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501/ last accessed Aug. 2015

[7] Deb Shinder , "Profiling and categorizing cybercriminals", Tech Republic, 2010. http://www.techrepublic.com/blog/it-security/profiling-and-categorizing-cybercriminals/ last accessed Aug. 2015

[8] Fishbein M., Icek Ajzen, Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research, Addison-Wesley, 1974.

[9] Gandhi R., Sharma A., Mahoney W., Sousan W., Qiuming Zhu., Laplante P., "Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political", Technology and Society Magazine, IEEE. Vol 30, Issue 1 pg. 28-38, 2011. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5725605&tag=1

[10] Gráinne Kirwan, Andrew Power, The Psychology of Cyber Crime: Concepts and Principles, IGI Global, 2011.

[11] Jaishankar K., Cyber criminology: exploring internet crimes and criminal behavior, CRC Press, 2011.

[12] Larisa April Long, "Profiling Hackers", 2012. http://www.sans.org/reading-room/whitepapers/hackers/profiling-hackers-33864 last accessed Aug. 2015.

[13] Michael Fitzgerald, "Behavior Analysis: New Weapon To Fight Hackers", Information Week: Dark Reading, Feb., 2014. http://www.darkreading.com/security-%20monitoring/behavior-analysis-new-weapon-to-fight-hackers/d/d-id/1113797 last accessed Aug. 2015.

[14] Seymour Bosworth, M.E. Kabay, Eric Whyne, Computer Security Handbook, 5th Edition, Wiley Inc, 2009.