Psychology and the hacker – Psychological Incident Handling

GIAC (GCIH) Gold Certification

GIAC ID#1564414

Author: Sean Atkinson, seanwatkinson5@gmail.com

Advisor: Christopher Walker, CISSP

Accepted: June 20, 2015

Abstract

The understanding of the processes, techniques and skills of hackers or cyber-criminals can be ascertained through the practical application of forensic psychology techniques and behavioral analysis. The actions and methods used within an attack, through the monitoring of logs and forensic discovery, will contribute to a profile of the person/persons behind the intrusion. This information will be a new vector in determining infiltration techniques, if the actions leave a persistent threat (backdoor) or if it is a one-time "smash and grab". If applied correctly, the detective controls can shorten avenues of determining risk and threats, as well as the magnitude of investigation required based upon the behavioral profile. Incident handling is based on the detection, response and resolution of security incidents. Given a new understanding of the person/persons behind such an incident, the process will be a preliminary part of the incident handling process. Using the methods of behavioral analysis, it creates a new dimension of understanding to the malicious activity and network analysis of what occurred in the environment.

1. Introduction

Incident handling at its core is the response to an attack in order to minimize loss. The restoration and reconstruction of events are used to understand the compromise, thus the effect is treated as a weakness and then the vulnerability is realized (Cook, 2000). Technical methods to investigate, understand and protect are commonplace within all incident management plans. It would be rare within those plans to see any items concerning the 'person' behind the incident; it would be even rarer that the understanding of the 'person' be treated with as much rigor as the technical investigation.

This paper's premise is to build a profile of hackers; this is categorized according to the stereotypes that exist within the hacking ecosystem. The technical threats are established, what is need is the understanding of what psychological motives that is at play. When psychological theory is applied, the process to build the motivational factors that promote a hacker conscience is initiated. If applied correctly, the motivation can be applied to the methods of cracking systems and a technological response to each group of hackers is revealed (Jaishankar, 2011).

The following steps are a practical guide to apply psychological incident handling.

2. Why is there a need for 'psychological incident handling'?

To understand, prevent and define those that would attempt to penetrate cyber defenses, requires a skill known as psychological incident handling, to determine the effect or reasoning behind an incident. If systems are prepared through hardening and alerts, the incident handling process requires the ability the reason, motive and skill set that exists behind an attack or compromise. This paper has been written to show the insight that can be gained through a review of psychological motives and methods that can be used to categorize hackers. The premise is to attain a perspective into hacker's psychological reasoning to enhance the understanding of the human element for those attempting to disrupt or prevent such incidents from happening (Long, 2012).

Now imagine a plan that revolves around the human element first. What motivations were at play?

Sean Atkinson, Seanwatkinson5@gmail.com

Formulating a simple set of rules surrounding behavioral analysis will determine factors that will determine the motivations, methodology and motive at play.

Behavioral analysis utilized at specific points on the incident timeline will determine several factors:

Did they know where to go? How efficient was the search for their prize? – is internal knowledge at play or have paths to coveted data been divulged?

What did they do once they got to where they wanted to go? Was it a passive enumeration or a complete download of information? Were items deleted, and what effect, if any, was done to cover their tracks?

Through a simple matter of asking the right question at the right time, divulges information not seen through normal incident management processes. Knowing is half the battle. Knowing why, what and how and applying that to a psychological profile has just weaponized an incident response process.

As the term hacker has been defined and categorized in mass media, it is important for this paper that the term be understood from its psychological roots and how each categorized type is addressed. The terms will be defined and will be placed into a model that looks at Motivation, Motive and Methodology. These three categories will allow the full behavioral analysis of each stereotype to be addressed and adopted in a proactive manner within an organizations incident management plan (Fotinger & Ziegler, 2004).

Sun Tzu " It is said that if you know your enemies and know yourself, you will not be imperiled in a hundred battles; if you do not know your enemies but do know yourself, you will win one and lose one; if you do not know your enemies nor yourself, you will be imperiled in every single battle." (Griffith, 1971)

3. Categorizing hackers as threats

The review of the stereotypes and the types of black hat hackers has been formalized in a list based on ability, motive and methodology. Each characterization has its own pros and cons in enabling a behavioral profile, as the stereotypes are altered dependent upon the country,

socioeconomic status and overall skill that the hacker possesses (Schinder, 2010). To simplify the category of a hacker, the following table has been created. Throughout the paper, reference to these stereotypes and the attributes that each possesses is made.

Black Hat Actor	**Example**	**Motive**	**Actions**
Script Kiddie	Newbies and tinkerers	Curiosity	Very loud, no specific target and lots of attempts
Malicious Insider	Work force or ex-employee	Revenge	Stealing information or wreaking havoc with internal systems
Activist	Snowden	Revelation	Revealing trade secrets or bringing light to a cause
Spy	Nation States	Espionage	Better understand your enemy or ally
Terrorist	Sony Hack	Destruction	Infiltrate, discredit or destroy data/ systems
Organized crime	Russian Mob	Making money	Making money but maintaining the computer infrastructure

Table 1: Categorizing hackers by stereotype

To introduce the profiles of these threat "actors", defined metrics are as follows:

- **Persistence:** The time and effort taken to compromise or understand the system(s) that a target utilizes within its infrastructure. The attention to detail and resources utilized to enumerate the target and how long it takes to gather such information.
- **Skill:** The technical skills or social engineering skills that a hacker possesses. Skills can be based on the particular 'actor' and the ends to which each requires in order to perform their malicious/criminal activities. Skills can be generalized into sub categories such as programming, networking and system administration etc.
- **Greed:** The amount or need to acquire information or compromise numerous systems define the greed that a hacker possesses in order to get the most out of their ill-gotten gains.
- **Stealth:** The ability to manipulate and exfiltrate data without being detected. The ability to compromise a system and alter system logs without raising alarms makes for an invisible advisory. This is exemplified in the clandestine or mission objective examples of corporate espionage and competitive intelligence gathering.

3.1 The kid or script kiddie:

A person whom has minimal skill or is learning to hack through automated means. These are persons who use the automated methods and tools to perform a hack that, in other cases of more experienced hackers, would be a manual and deliberate process. The interest within computer starts early or is introduced through another means – Script kiddies will start young and their curiosity is peaked with such devices. Desire to learn and understand is the weapon of curiosity that may be a classifying data point in terms of the beginner. The developmental phase may be through social learning theory based upon the social and or environmental factors influencing the person.

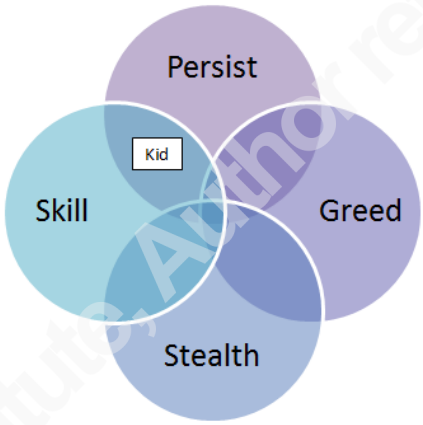


Figure 2. Skill assessment of a script kiddie.

3.2 The malicious insider:

These persons evade internal controls and access data or resources that could be used nefariously or for personal gain. The insider is characterized by intelligence and a need to either steal or perform criminal activity based upon their access or position within an organization. Here, motivational characteristics start with looking at the persons expenses compared to income. If the supplement of their income with internal resources can be achieved, the personality type inherent within a majority of persons commit these types of crime is – they are owed, they are badly treated or that they opportunity existed because the company has faulty controls within their internal systems.

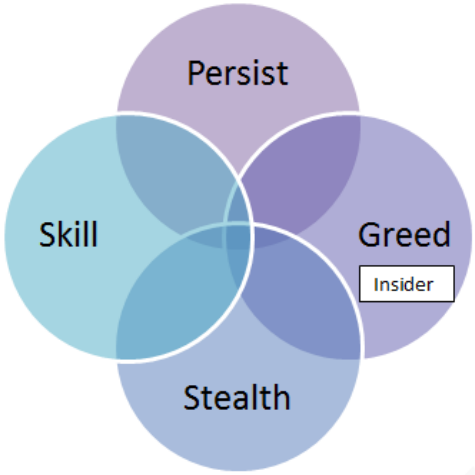


Figure 3. Skill assessment of a malicious insider.

3.3 The activist (Hacktivist):

The intent is to deny access to information, destroy reputation or provide a perspective view in to the ideals that the activist possesses. Web page defacement and denial of service to information are methods used to further the hacktivists social agenda. The Activist is a person with the means to force their ideals (social, religious, political) against those that don't hold them in the same light as the cyber activist or 'hacktivist'. The inherent need for people to understand their point of view and forcing their opinions through social media or webpages allows the vindication of such actions. In most cases the person wants to be found and appreciated for their 'insights' so the clandestine operations are not usually employed in these cases, even if the information gathered is a 'handle' or nickname the 'hacktivist' has adopted for themselves.

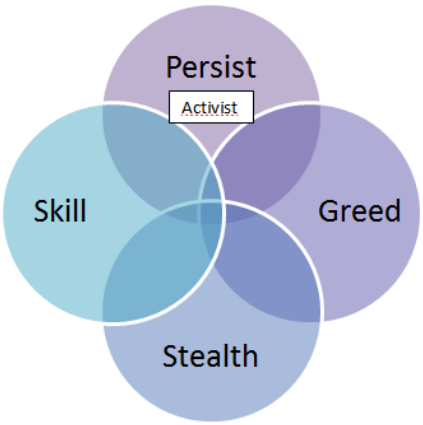


Figure 4. Skill assessment of a hacktivist.

3.4 The spy:

The corporate or government spy uses their skills to attain sensitive date and further their corporate or government's agenda. These persons have skills that allow them access to data that is very sensitive, and they use social engineering techniques to further their gain within corporate or government settings. Either corporate or government funded, the most clandestine within the classification criteria, these particular persons or groups are highly skilled and highly funded. Utilizing tried and true methods and also developing methods that are zero day exploits these individuals will use the necessary means to break into and compromise systems or ex-filtrate data from these systems for their employer's gain. Here examples can be drawn to government hackers, and a countries resources discovery and compromise.

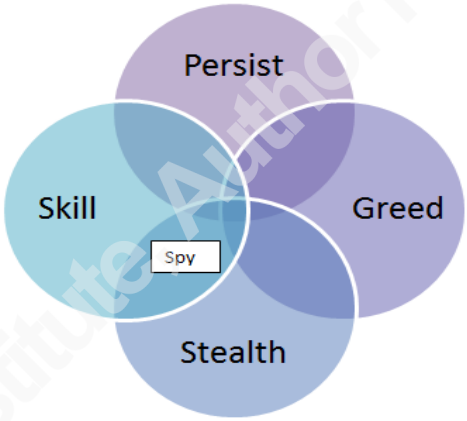


Figure 5. Skill assessment of a spy.

3.5 The criminal:

These persons are tasked with finding and using data for monetary gain or for creating chaotic situations with regards to corporations, individual persons or society as a whole. These people are easy to classify but with their increase in cybercrime and internet anonymity, the justice that should be served in most cases is limited. Utilizing techniques to bypass security protections, criminals come in different characteristics dependent upon what they are trying to steal. Financial minded criminals may choose to attack credit card accounts, banking information or organizations that collect and use this information for financial transactions. Attaining this data allows individuals to sell the data or use it for their own financial gains. Organized crime

syndicates may use persons with such skills to launder money, track persons of interest or create a digital paper trail.

Figure 6. Skill assessment of a criminal.

3.6 The terrorist:

A person or group of people with the intent to disrupt or destroy information or systems connected to computer networks. These terrorists may be nation state funded operatives or idealistic groups of people who have come together for a common cause. Or, it may be an individual with revenge or a grudge to bear that will be expressed through terrorist activities. The skills and abilities of this particular group may vary, and that is why they are identified in the diagram below to have all categories of metrics defined for the threat actors. Through sociological ideals this can be activism against a regime, a Denial of Service or complete destruction of infrastructure. Stuxnet would fall into the latter category. In order to stop a particular system, a virus was created with the intent of destroying operations. These types of infiltration and controlled attacks have been theorized and seen in practice where enemy states can take over highly sensitive infrastructure systems to shut them down or destroy them. The type of attack and review of the methodology will distinguish targeted attempts to those that are weaponized system seeking attacks.

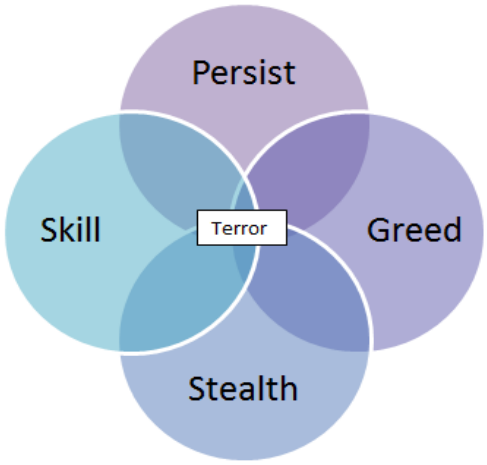


Figure 7. Skill assessment of a terrorist.

4. Psychological aspects of hackers

4.1 Empirical Psychological Research

Research has been performed into the social and psychological aspects of hackers. Bernadette Schell, in 2000, attained research data from self-reporting hackers at a security convention. When categorized and collated these results produced the following interesting facts (Shell, 2000):

Table 2 - Self-reported hacker behaviors	**Results**
Total respondents	216
Age range	14-61
Mean age	25
Mean salary /year	$56,000
Creativity score - "Highly Creative"	62%
High Depression	14%
Bipolar disorder indicators	15%
Lifestyle "monogamous heterosexual"	79%

Note: Hackers were found to have the following traits, excellent stress management, good at multitasking and are type 'B' personalities that exemplify "relaxed," "balanced" and "self-healing". Adapted from *Hacker Psychology* by B. Shell, 2000. Retrieved from http://www.happyhacker.org/gtmhh/bank5.shtml

If these results are cross-referenced with the results from a similar study the following is found (Rogers, Seigfried, Tidke, 2006):

Table 3 - Self Reported Hacker behaviors	Results
Total Respondents	77
Mean age	21
Computer Crime Index: Cronbach's alpha	0.71
Big 5 Scale:	
Extraversion	0.88
Agreeableness	0.87
Conscientiousness	0.70
Neuroticism	0.80
Openness to experience	0.85
Exploitive manipulative amoral dishonesty scale EMAD	0.90
Moral Decision Making Scale MDKS:	
Internal: 0.63	0.63
Social: 0.63	0.63
Hedonistic: 0.72	0.72

Note: The hackers in this study were mainly college students. Adapted from *Self-reported computer criminal behavior: A psychological analysis* by M Rogers, K Seigfried and K Tilde. 2006. Digital Investigation. S116-S120. Retrieved from http://www.dfrws.org/2006/proceedings/15-Rogers.pdf.

From the studies mentioned above, the extrapolated hypothesis would be that a computer criminal would be more introverted, open to experience, neurotic, exploitive and manipulative. The score within the social moral choice was lower than that of persons who reported no computer criminal activity within the study.

4.2 Motivation

Review of the Symantec Internet Security Report for 2014 shows data that correlates to an increase in zero day exploits, these gaps are becoming the attack vector that elite hackers will utilize to perpetrate their compromise activities. These types of exploits are of special interest to vendors as the utilization of these exploits can have harmful effectives if they are not patched. Even with patching, the knowledge of the zero day exploits allow a community of hackers to use

these particular vectors to deploy malicious software before sufficient controls can be put in place. Even within the older infrastructure new software exploits are being discovered. This demonstrates that utility software, or any software that is used within computer environments, can be targeted and used to benefit the persistent hacker.

Ransomware also became a new means to generate money, and the revenue model is adapting to create revenue streams that will allow the use of online payment methods ransomware and ransomcrypt. They will likely be prevalent and a means by which hackers can gain a foothold in a user's system.

Bragging rights are also a part of the motivation; the celebrity hack became a way to publicly humiliate celebrities and use vulnerabilities between cloud backup methods to steal and publicize pictures that the people affected would not want disclosed to the public (Gandhi, Sharma, Mahoney, Sousan, Qiuming, Laplante, 2011).

Corporate breaches also made major news headlines – such companies such as Target, Home Depot etc. have reportedly been compromised, and the loss of hundreds of millions of accounts and personal identifiable information (PII) is now in the hands of hackers, with the intent to sell the acquired data. It is not only birthdate and social security numbers that are being targeted. It is financial, medical and insurance information that is being used to create a niche market for the motivated hacker. In 2013, a total of 552 million identities have been exposed, a 493% increase above the previous year. Until major corporations and data aggregation services manage their infrastructure security more effectively the motivation and opportunity will exist for nefarious activity. Given the right opportunity, hackers will victimize those less informed and will continue to use their skills to accomplish their goals. The low rating in terms of social or moral character of a particular subset of nefarious hacker will use the 5 primary factors of victimization and apply them in their enumeration and attacking schemes.

User illiteracy

Deficient criminal cues

Limited attention

Inflated trust

Addiction potential

Given the above the persons or corporations who are victims are either not aware or don't really care about security. The digital economy has an inherent trust relationship; this again can be used against the unsuspecting or unaware average computer user. Given that people's digital lives or information is intangible the awareness that humans have built to the physical, tangible items demonstrates that the same safeguards of suspicion and protections are not inherently translated (Helfenstein & Saariluoma, 2014).

The means and the opportunity demonstrated about gives the hacker more motivation because the success rate of such attempts far exceeds the will to pursuit their goal until all of the resources or motivation has expired. Access, resources and talent have never been more prevalent as well as the social development environment allowing customization, collaboration and concealment of newer methodologies in the arsenal of hackers (Jaishankar, 2014).

In terms of motivation and based on the stereotype defined in this paper, hackers, criminals, hacktivist and tinkers all have a goal or basis in which they believe something is achievable. With any goal or objective set by oneself or by peers/leaders in a social or work environment, time and resources are required to achieve the objective. Given this ideal, achievement is a real motivator, in a social context having bragging rights is a commodity and also to be held in esteem by others is a factor in most persons psyche (Kirwan, 2011).

4. 3 Motive, Explanatory models of motives of hackers

4.3.1 Sub-culture individual theory

As hackers become part of a community of likeminded persons, there becomes a sub cultural aspect inherent within creating online relationships that allow a hacker to express themselves (Bossler & Burruss, 2010). Given the culture of the group and the intentions to hack or perform hacking related activities, the values of the below equation (1.1) will change when motivation is applied in a sub cultural group. The criminal intent may be low but the benefit value will start to exceed that of the disadvantage value given the right circumstances. Within a sub cultural group their will exist some resistance to perform nefarious activities, others with a

lower conscience of performing these acts may opt or enlist to perform them in order to increase the benefit value. i.e. ('if I am willing to perform the activity I will ingratiate myself and become part of the group').

Cost vs benefit

$$1.1\ CI = (BV * AL) – (DV * RL)$$

The equation looks at Criminal Intent (CI) equals the attained likelihood (AL) of a benefit value (BV) minus the realization likelihood (RL) for the anticipated disadvantage value (DV) (Fishbein & Ajzen, 1974).

4.3.2 Social Learning Theory

The interaction of society and environment can prevail in behavior characteristics and personal development (Hollin, 1989). Given the environment and cyber society of the web the interaction would need to be defined in terms of the original theory looking at the social and environment factors that surround the person physically. Given that the internet is not a physical construct the original paradigm becomes convoluted in terms of what socially becomes IRC and environmental become the website in which interests the computer user (Rogers, 2001).

4.3.3 Depersonalized obedience

If the victims suffering is not experienced firsthand the cognitive processes are less likely to who restraint in terms of the personal victimization (Milgram, 1963) that could be caused by the hackers actions. Given the faceless act of the computer interface and hacking in general, the level of obedience to yield to social constructs is reduced. This provides a way in which the societal influence is depersonalized and how hackers can act without regards for someone on the other side of a terminal (Bosworth, Kabay, Whyne, 2012).

4.3.4 Moral disengagement

If the agent carrying out the attacks feels as if the allowed actions of the attack are the direct results of systems inherent weaknesses (Bandura, 1990). These exploitations are deemed the fault of the system owner and not protecting their assets in ways that would have prevented the attack is culpable for the attack. The lack of understanding or failure to prevent the hacker is a depersonalization and disengagement on behalf of the hacker. The lesson they are being taught by being compromised is punishment for not securing their system (Rogers, 2001).

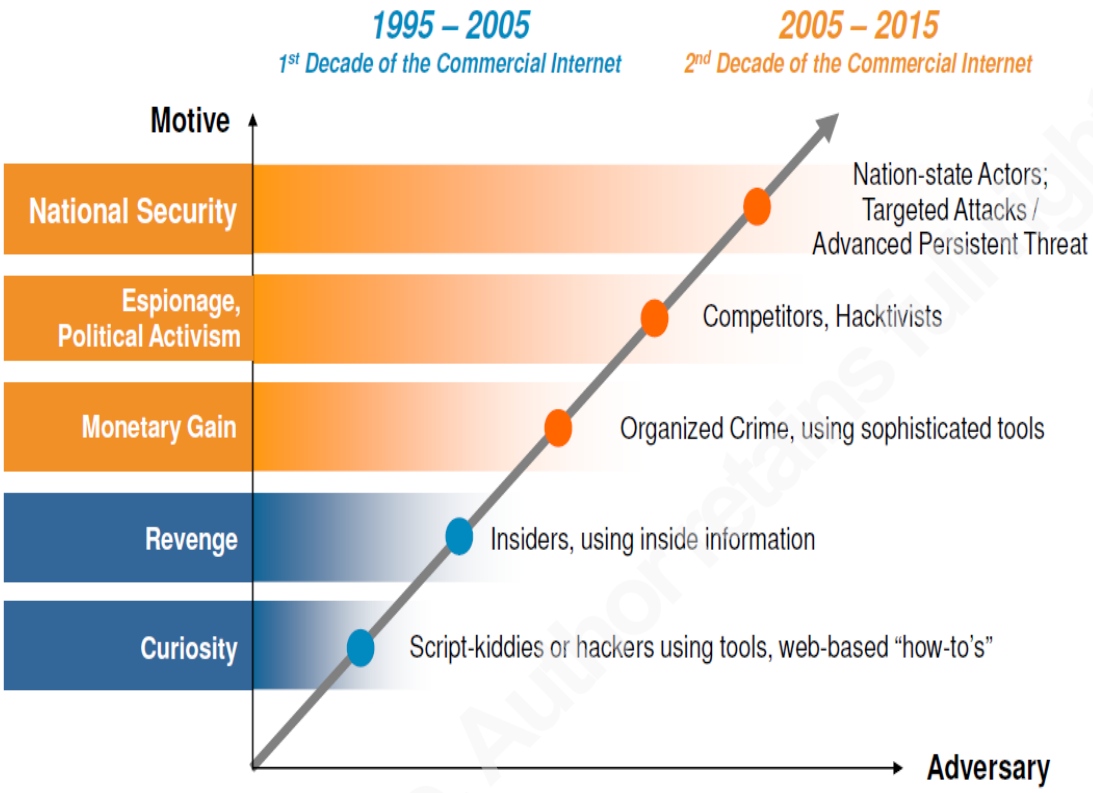


Figure 8, Hacker motive based on the type of adversary, indicates how over time the level of sophistication and intent of hackers has altered. Applying the psychological principles to attacks will start to leverage this information in more constructive and proactive responses to the adversary. Adapted from Effectively Using Security Intelligence to Detect Threats and Exceed Compliance, by C Paulin, 2012. IBM

5. Threat Profile

Being oblivious to understanding enemy motivations, skills and reasoning is detrimental to the incident handling process. If the evolution of security is to become more efficient and effective the human element of attacks cannot be neglected. Highlighting the psychological aspects of incidents will formulate more direct plans of action against the attackers. The human element seems to have been lost in formal security education.

5.1 Actors

Decision processes and the assessment of the condition of the system after the compromise will allow a profile to be created. In similar terms the profile will be the hypothesis that defines the investigation. The perspective of the threat actor will now be illustrated utilizing figure 1 to illustrate examples of each threat and how an incident handler should respond to such a scenario and threat actor (Shinder, 2010). Also included are CSC numbers based on the SANS Institute, Critical Security Controls Version 5.

5.1.1 Script kiddie/tinkerer

Using established hacking methodologies and attack profiles to enumerate or actively scan a network. The reaction to such incidents would be through common prevention systems and monitoring of the external networks and SIEM log analysis. For example, known exploits exist and these can be used or attempted to be used to gain access to networks. It would be trivial for a well deployed firewall, intrusion detection system to stop this type of traffic and as it is a known exploit already have in place a remedy for the vulnerability. Traffic and boundary layer log analysis will show the attempts and provide evidence of a novice or tinkerer. This would be attributed to the SANS Top 20 Critical controls number 13 Boundary Defense, 14 Maintenance, Monitoring, and analysis of audit logs and 19 Secure Network Engineering. Monitoring and understand the infiltration mechanisms used by currently distributed attacks can prevent against those whose intent is not malicious but based on curiosity. Looking at some of the indications of a script kiddie or hacker using downloaded tools, indicators at the boundary defense will show the volume of network activity, a high number of failed logon attempts or the off hours utilization of resources beyond the normal correlated utilization benchmarks. See Appendix A: Script Kiddie.

5.1.2 Malicious insiders

There will be a need for greater concern, reviewing the case of a malicious insider, having the ability to describe the level of access and ability to copy/remove and maliciously distribute confidential content to the world is an asset. An internal response to such an activity would be through Data Loss Prevention (DLP) and data classification. The insiders with the rights to perform their duties are incredibly hard to detect especially at the system administration or security analysis levels. (e.g. in the case of Edward Snowden the level of access and no

monitoring controls allowed for the pilfering of sensitive documents) These are the persons in place to make sure everyone else within the organization doesn't perform these malicious activities. Internal audit and continuous monitoring should be applied to understand the weaknesses within the internal organization. It is common to see the utilization of security measures across the technology infrastructure to prevent intentional and unintentional data loss or ex-filtration. In the network arena the egress point analysis will look for sensitive data leaving the network through network traffic monitoring. Internal to a business would be the use of endpoint DLP this can also monitor internal communications. These rules, alerts and policies are only as good as the way they are implemented and the internal understanding and classification of data. See Appendix A: Malicious Insider

For example the case of Zynga (Dark Reading, 2012) an employee added a Dropbox account to his system and transferred sensitive files. 'The Data Walk Out' similar to Snowden is the removal of files in direct violation of Intellectual Property policy but in the case of some employees they feel that they have some right to the data and they 'own' it. Therefore applying a psychological profile to employees and data loss prevention should highlight sensitive work that employees have contributed, this would related to a major control that should be in place so that data doesn't walk out the door. Monitoring of the network traffic and global desktop policy for the addition of software on individuals computers would have highlighted the utilization of the software and lead analysts to perform some investigations. This would be especially important if the employee had made known his intention to leave the company; psychologically the disgruntled employee will exhibit aggressive or pessimistic undertones and will not be a contributor to the overall business strategy of the organization.

5.1.3 Activist/Hacktivist

Such teams or persons with the same political ideals can collaborate against a particular organization or political agenda to use hacking as a voice against those ideals that they believe are wrong. Such examples include the group 'Anonymous' and their attempts to protest the Church of Scientology through a protest movement called 'Project Chanology' (Wikipedia, 2008). To disrupt the Church's online activities the activists used Distributed Denial of Service and other methods. Response to these actions would be good communications with the ISP, review the logs of servers, routers and firewalls to review what infrastructure is being affected

and use this information to control the traffic that is causing the errors. Specifics in this case will provide a greater control of what is being block and what traffic is not part of the attack. It would be especially poignant to see if there were any precursory threats made against the organization. If so this could be a warning mechanism as well as a way in which to define who or what activist organization is behind the attacks. Another example would be Edward Snowden and the ability of activism to come from the inside. A contracted systems administrator with the ability to access, copy and remove information from the premises of the NSA, allowed state secrets to be revealed to the world. The aim is to highlight the methods and technologies at the NSA's disposal and the 'Big Brother' effect of their surveillance programs. See Appendix A: Activist

5.1.4 Spies

Those involved in intelligence gathering from governments and industrial secrets are Pin-pointing systems of significance in order to attain intelligence or otherwise discover vulnerabilities that would allow for access to privilege and confidential information. Such groups can be identified as nation state hacking teams such as those in the US, Britain, China and South Korea. Examples of such a surveillance tool would be Regin (Symantec, 2014). An information gathering tool used to spy on a number of international targets since 2008, the tool is a very sophisticated back door Trojan with a 5 stage infection process using multiple techniques seen in such malware as Weevil and Duqu. This level of effort shows how much development time and resources would have been used to create such a sophisticated piece of malware. See Appendix A: Spy

5.1.5 Terrorism

and acts that would disrupt or otherwise cause mass chaos are conceived in order to targets a particular system or bring an entire network of systems down. Cyberterrorism has been seen on an international stage in the compromise of Sony and issues regarding the movie 'The Interview'. The terrorists have threatened movie goers with threats of violence if they go and see the movie. The hack has been attributed to North Korea and the nation state sponsored hacking group 'Bureau 121' but responsibility was claimed by a group 'Guardians of Peace'. In terms of the psychological aspects, motivated groups that are adamantly opposed to content, product or person they will use all means necessary to remove, destroy or oppress the dissemination of the content, product or discredit the person (Robb, 2014). See Appendix A: Terrorist

5.1.6 Organized Crime

These cases allow criminals to extract information from systems in order to keep making money, so the protection and uptime of these systems are a priority. Such infiltrations would be in the form of spam, phishing, and malicious software to commit identity theft or online fraud. Dependent upon where the crime originated also determines the crime laws that are applicable and make investigation and prosecution a lot more difficult if not impossible. Internal processes and training for users to understand and not disclose personal information in an email should be employed, and review of URL's that should be blacklisted to fake websites. The psychological undertones in such attacks are based on social engineering techniques, these are harder to detect or train for as it is each person's individual response to requests for information or clicking a link in a malicious email that need to be reviewed and protected against. It is of note that cyber criminals will protect the infrastructure rather than destroying it in order to keep making money for the persons, networks that they have compromised (Aiken & Mc Mahon, 2014). See Appendix A: Organized Crime.

5.2 Targets

Situational analysis will be advantageous, understanding who the main perpetrators of particular industries are and how this can use the methods described above to protect assets, information and systems from the main threats to each individual industry. Preparing for such attacks will mitigate the main threats and those that are labelled as other can be understood and the minute changes that are required to protect against other modes of attack can be the focal point rather than trying to protect against threat actors that are targeting the specific industries mentioned in the graphic below.

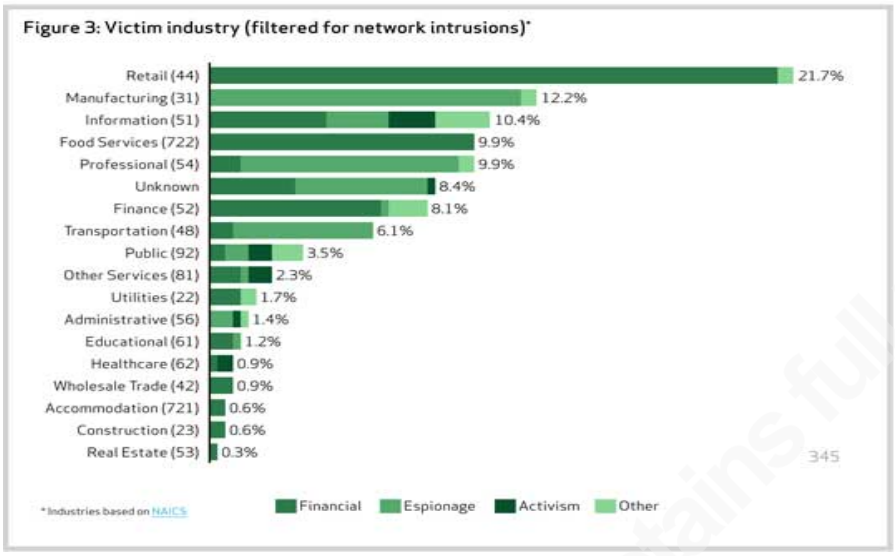


Figure 9. Victim industry categorized by target Source: Adapted from *Phishing Jumps to 29% of Cyber-attacks. Is your utility prepared for social hacking schemes?* By K Tweed, (2013).

Give the benefit of understanding the particular industry and the threats that a prevalent against each, the analysis can be utilized to understand the specific industry risks and the required controls that will mitigate the main risks to each specific industrial profile. In the analysis below four main industries are reviewed.

5.2.1 Retail, Hospitality and Food Service:

The aim for hackers in the case of the retail industry is two-fold. One is to get PCI information from Point Of Sale terminals using malware or compromised POS. When looking at the demographics of such groups, 73% were perpetrated by organized crime and 99% of the entire attacks are financially motivated. The alternate method of attack is DoS in order to overwhelm systems and remove the balance of security and availability in order to subject POS command servers to compromise.

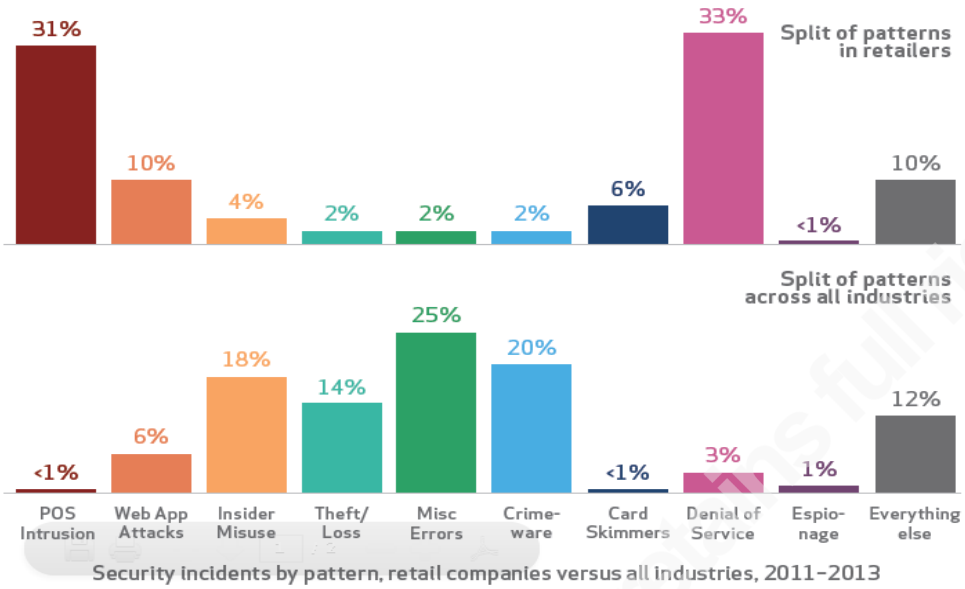
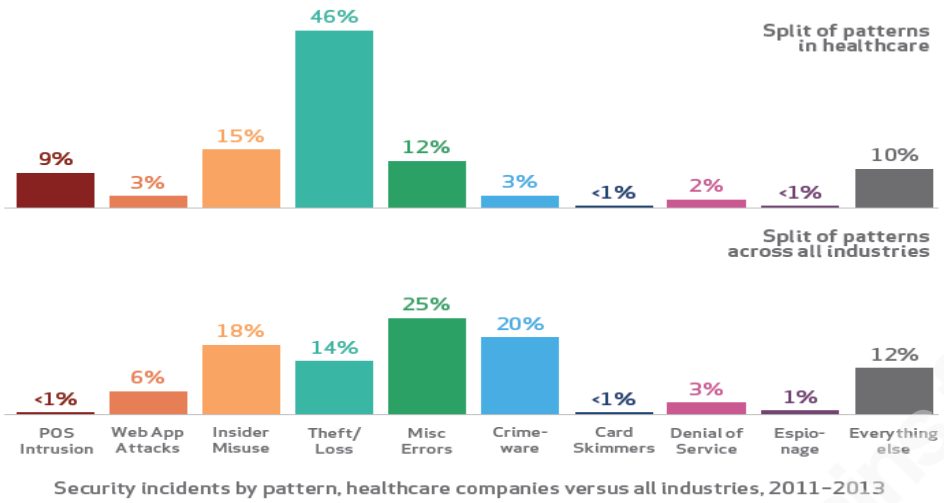


Figure 10. The retail industry compared to the attacks against all industries within the study. Adapted from *Verizon Vertical Insight (2014)*. 2014 Data Breach Investigations Report Retail.

5.2.2 Health Care:

The motivation for attack is to steal personal and healthcare data, the methods that are used include attacking POS systems to gain the PCI information and healthcare professional desktops. Methods are also used to compromise RDP sessions as the application of understanding the systems and services healthcare prof4ssional utilize allows organized crime embers to attack specific protocols and RDP services to compromise systems. Often these systems have less security controls as the ease of access to data and requirements of availability are valued over strong password requirements and factors of authentication. The internal review of these systems fails to find these compromises and attacking schemes as law enforcement detected these breaches in 84% of these cases.

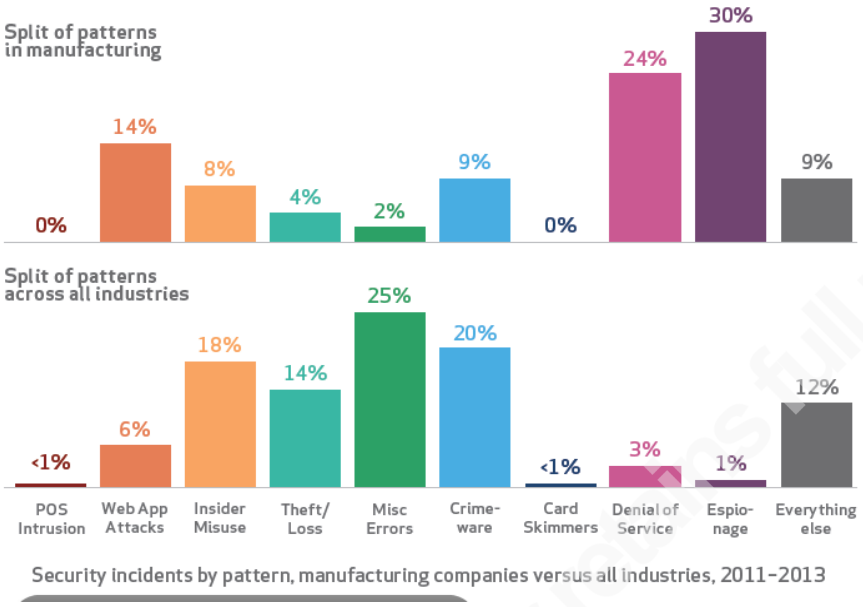


Security incidents by pattern, healthcare companies versus all industries, 2011–2013

Figure 11, the healthcare industry compared to the attacks against all industries within the study Adapted from *Verizon Vertical Insight (2014).* 2014 Data Breach Investigations Report Healthcare.

5.2.3 Manufacturing:

Intellectual property and trade secrets is the target in this industry. The exfiltration of such information allows state sponsored countries and associated governments to profit from another research and development programs. The insider threat is also a factor that allows this type of data to be stolen, this data is protected with a layered security approach and the logical method to access such data would be to compromise internal personnel who can bypass some if not all of these layered security protections. This number is reported to be 21% of all IP theft had insider assistance.

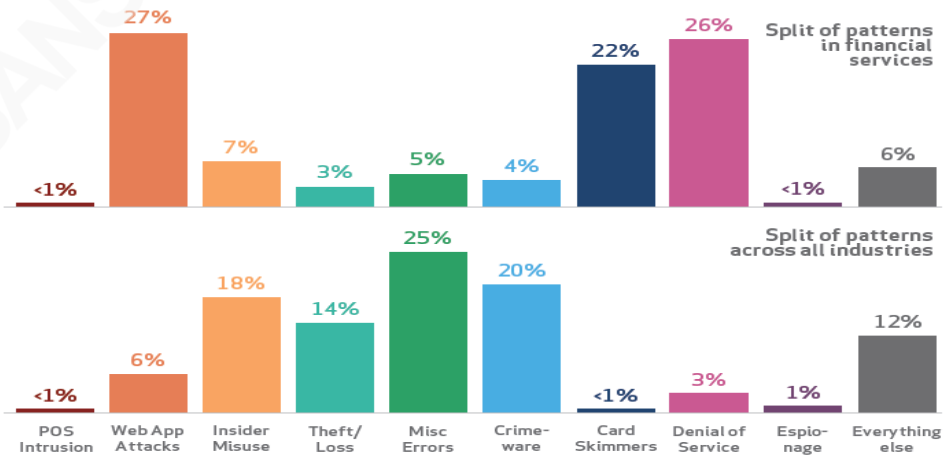


Security incidents by pattern, manufacturing companies versus all industries, 2011-2013

Figure 12, the manufacturing industry compared to the attacks against all industries within the study Adapted from *Verizon Vertical Insight (2014).* 2014 Data Breach Investigations Report Manufacturing.

5.2.4 Finance Services

The modern day bank heist is now performed over networks rather than in breaking safes. The biggest proponent of theft is through organized crime and the motivation is money even if it is in a digital format.



Security incidents by pattern, financial services companies versus all industries, 2011-2013

Figure 13, the finance industry compared to the attacks against all industries within the study Adapted from *Verizon Vertical Insight (2014)*. 2014 Data Breach Investigations Report Finance Services.

The above analysis now provides the attack vectors that are used against particular industries and how these kinds of attacks produce these types of symptoms that provide either an alert or a reactive response to the threat. See Appendix B: Symptoms and Response.

6 Incident Response

Systems with the infrastructure are monitored against a 'normal' system operational standard. In order to baseline the understanding of the operation of the system and users within those systems. This data can then be used to identify and event or threat. To get to this point of understanding within the infrastructure, asking the following questions will provide valuable information:

- Can the system be modelled to identify an event?
- Awareness that an event has occurred?

Rule based SIEM will only provide alerts that have been previously created, if an event goes unnoticed or is not considered an event or no rule exists for alert – the real time reactive response becomes nullified, and the advantage is now with the hacker. Tracking trends within the system based on the users of the system is a behavioral modelling that can be used to find out what accounts are performing within a 'normal anticipated range of activity' and which accounts are beyond their normal operating boundaries. See Appendix C: Revised Incident Response

6.1 Indicators of Compromise

If a compromise is believed to have occurred, or a more proactive approach to security controls is required, referencing the SANS Intrusion Discovery Cheat Sheets (SANS Institute) for Windows and UNIX allows an incident responder to evaluate their particular Operating Systems for indicators of compromise. The guides identify areas where a specific advantage can be

gained for identification of a breach as well as utilizing these guide to review the psychological undertones that need to be understood during an incident handling event.

6.1.1 Unusual processes:

Dependent on the processes that are running it will point to the actions of the attacker. Incident response questions to ask:

- Are the processes ex-filtrating data, removing or modifying log files?
- Based on these actions can it be determined if the hackers are looking to remain undetected?
- Is this unusual processes part of a grander hacking attempt in processes and this is a single part?

If the actions are covert or allowing activities within the system to remain covert it points to a behavior processes being applied to the system. Needing to retain access is more likely cyber-criminals 'organized crime' rather than hacktivists or attempted system destruction from a cyber-terrorism (Aiken & Mc Mahon, 2014).

6.1.2 Registry keys for malware

Looking into a registry for unusual entries may provide evident of malware that exists on the system. A review of the startup configuration will determine the level of sophistication and the intent of the malware once it has been identified (Jaishankar, 2011). If the level of sophistication is determined the following questions can be asked:

- Is this a published malware or attack, or does it point to a group or organization with sufficient resources to deploy such malware?

6.1.3 Network usage

Traffic generated for ex-filtrating data to an unknown host will indicate if data is traversing the network and with appropriate baselines will elaborate on the question 'Is this normal network usage?'

- Is the data being used for active enumeration or is it being used to detect when the nefarious channel has been exposed?

- Are backdoors present within the system for established hackers to return to retrieve data?
- Are web shells present allowing an advanced threat access to systems?

These may point to persons who are well versed in hacking techniques, based on the infrastructure that they have set up will determine their intent. Network utilization may be so 'noisy' that the skill level of the hacker may not be at the elite level. These actions could also be a ruse to enumerate a response and recovery time frame and point to the internal level of sophistication (Kirwan, 2011).

6.1.4 Start up and scheduled tasks

Suspicious task used to retrieved data, are these set to start on boot or are they managed as a scheduled task set to execute at a particular time. If the scheduled task is set to execute a log deletion it may point to a hack attempt that has already finished or is taking place right now. The covering of tracks again point to a particular profile and can identify systems that would be more vulnerable to the particular hacker profile. If the aim is to remain invisible it can point to espionage or cyber criminals that want to protect the asset they have in the methods they use to compromise the system (Kirwan, 2011).

6.1.5 Unauthorized accounts

Backdoor and level of persistence within the system provided by account creation. Account review will point to accounts with higher levels of privilege escalation, administrator level accounts, and guest accounts and also the review of orphaned files deleted by a temporary account that no longer exists. The accounts, privilege escalation and the privileges assigned to the account will direct an investigation to a profile and the intent of the account creation. What is the target for privilege escalation if events point to privileges beyond that to steal personal information; this demonstrates a requirement for higher levels of access to attain more privilege and sensitive information (Schinder, 2010). This may point to a motivation to get valuable information beyond that of which they already had access. Espionage or a specific criminal element may be utilizing such techniques until they have access to the information they want to find (Jaishankar, 2011).

6.1.6 Event viewer

Logs of event occurrences within the system should be reviewed and the following questions asked:

- Have these been altered and a person is covering their tracks?
- Can the events be reviewed to understand when manipulation occurred in order to build a timeline for the compromise?

The events of a system can be a true descriptor of a hacker's intent and actions within the system. Reviewing memory for searches and enumeration activities within the system can indicate the data or information of interest to the hacker. Specific searches can point to espionage, complete reviews of databases of PII point in another profiled direction. Another indicator of an attack and the intentions of the attack is if the log files are missing, covering the tracks through deletion of the entire log files shows the intent of being untraceable, removing specific logs and leaving the log file intact will raise much less suspicion and confirm the intent and skill of the criminal (Fitzgerald, 2013).

7 Conclusion

Profiling is limited to the extent to which it can identify hackers. Judgment will need to be applied and this is where baseline knowledge of techniques and experience can play a major part in determining who the person is and what were their intentions (Fitzgerald, 2013). The processes of incident handling allow us to view the incident landscape and look for telltale signs that a particular intruder perform actions that allowed the system to be compromised or in some way affected that wasn't the intention of the system owner. Determining the victim and hacker beyond pure incident response allows the incident handler to view the decision making perspectives of the hacker and the motivation behind such an attack (Fitch, 2004). Having ascertained that it was a hacker making a name for them, is it enough to patch the vulnerability so their mode of entry is removed, or if the attacker was part of a larger industrial espionage incident, and is a continuous high alter the norm of IT operations? The mechanisms of the attacker produce psychological responses from the system administrators and information security personnel who are put in charge of network and system protection. The technical skills that are attributed to both side of the attack can also be applied to the psychological resiliency of

the personnel on both sides of the attack. A battle of wits will ensue and being prepared with a psychological understanding of opponents will allow incident handler to make better informed decisions.

> "To know your Enemy, you must become your Enemy." (Griffith, 1971)

A famous quote that would in this aspect is reworded:

> "To know your enemy, you must understand the actions of your enemy"

I am a student of forensic psychology, but my day job is in the realm of information security risk management and the views that are expressed are my personal opinion through the research I have conducted. In order for the process of psychological incident handling to become a reality, communities of those who are experts in psychology, law and incident response are needed to bring a fundamental change in the methods and ways in which the information security industry thinks about incident response. I ask those who have ideas to contribute towards an integration of this papers premise as a service to the overall understanding of the human side of hacking and as a public service to protect systems from these threats.

Sean Atkinson, Seanwatkinson5@gmail.com

References

Aiken, M.P., & Mc Mahon, C. (2014). *The CyberPsychology of Internet Facilitated Organised Crime, Europol Organised Crime Threat Assessment Report (iOCTA).* Retrieved October 5 from https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta

Bandura, A. (1990). *Selective Activation and Disengagement of Moral Control*. Journal of Social Issues, Vol. 46, No. 1, pp. 27-46.

Bossler, A. & Burruss, G. (2010). *The general theory of crime and computer hacking: Low self-control hackers?* Idea Group Inc. (IGI)

Bosworth, S., Kabay, M., Whyne, E. (2012) Computer Security Handbook. 5th Edition. Wiley & Sons.

Cook, C. (2000). *An Introduction to Incident Handling*. Symantec. Retrieved from http://www.symantec.com/connect/articles/introduction-incident-handling

Dark Reading. (2012). *Five Significant Insider Attacks of 2012*. Information Week: Dark Reading. http://www.darkreading.com/vulnerabilities---threats/five-significant-insider-attacks-of-2012/d/d-id/1138865?

Fishbein, M., Ajzen, I. (1974). *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research*, Addison-Wesley. Reading, MA

Fitch, C. (2004). *Crime and Punishment: The Psychology of Hacking in the New Millennium*. SANS White paper. Retrieved from http://www.giac.org/paper/gsec/3560/crime-punishment-psychology-hacking-millennium/105795

Fitzgerald, M. (2013). *Behavior Analysis: New Weapon To Fight Hackers*. Information Week: Dark Reading. Retrieved from http://www.darkreading.com/security-monitoring/behavior-analysis-new-weapon-to-fight-hackers/d/d-id/1113797

Fotinger, C., & Ziegler, W. (2004). *Understanding a Hacker's Mind–A psychological insight into the hijacking of identities*. Krems, Austria: Donau-Universität Krems.

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

Griffith, S. (1971). Sun Tzu. The Art of War. Oxford University Press.

Sean Atkinson, Seanwatkinson5@gmail.com

Helfenstein, S. & Saariluoma, P. (2014). *How Cyber Breeds Crime and Criminals*. University of Jyvaskyla, Finland. Retrieved from http://sdiwc.net/digital-library/web-admin/upload-pdf/00001120.pdf.

Hollin, C. (1989). *Psychology and crime: An introduction to criminological psychology,* Routledge. New York

Jaishankar, K. (2011) *Cyber criminology: exploring internet crimes and criminal behavior*. CRC Press.

Kirwan G (2011). *The Psychology of Cyber Crime: Concepts and Principles*. IGI Global.

Long, L.(2012). *Profiling Hackers*. SANS Institute. Retrieved from http://www.sans.org/reading-room/whitepapers/hackers/profiling-hackers-33864

Milgram, S. (1963*). Behavioral study of obedience.* Journal of Abnormal and Social Psychology (67): 371–378.

Poulin, C. (2012). *Effectively Using Security Intelligence to Detect Threats and Exceed Compliance*. IBM- Reboot Conference 2012 Retrieved from https://www.rebootcommunications.com/wp-content/uploads/2012/10/ChrisPoulin205_IBMSecuritySystems.pdf

Robb, D. (2014). *Sony Hack: A Timeline*. Deadline.com Retrieved from http://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501/#

Rogers, M (2001). *A social learning theory and moral disengagement analysis of criminal computer behavior: An exploratory study*. University of Manitoba. Retrieved from https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/rogers_01.pdf

Rogers, M., Seigfried, K. Tidke, K. (2006). *Self-reported computer criminal behavior: A psychological analysis*. Digital Investigation S116-S120. Retrieved from http://www.dfrws.org/2006/proceedings/15-Rogers.pdf.

SANS Institute. *Critical Security Controls*. Version 5. Retrieved from https://www.sans.org/critical-security-controls/

SANS Institute. *SANS Intrusion Discovery Cheat Sheets*. SANS Institute. Retrieved from https://www.sans.org/media/score/checklists/ID-Windows.pdf

Schinder, D (2010). *Profiling and categorizing cybercriminals*. Tech Republic Retrieved from http://www.techrepublic.com/blog/it-security/profiling-and-categorizing-cybercriminals/

Shell, B. (2000). *Hacker Psychology*. Retrieved from http://www.happyhacker.org/gtmhh/bank5.shtml

Symantec (2014). *2014 Internet Security Threat Report*, Symantec. Vol. 19. Retrieved from http://www.symantec.com/security_response/publications/threatreport.jsp

Symantec (2014). *Regin: Top-tier espionage tool enables stealthy surveillance*. Symantec. Retrieved from http://www.symantec.com/connect/blogs/regin-top-tier-espionage-tool-enables-stealthy-surveillance

Tweed, K. (2013). *Phishing Jumps to 29% of Cyberattacks. Is your utility prepared for social hacking schemes?* Retrieved from http://www.greentechmedia.com/articles/read/phishing-jumps-to-29-of-cyber-attacks

Verizon Vertical Insight (2014). *2014 Data Breach Investigations Report Financial Services*. Retrieved from http://www.verizonenterprise.com/resources/factsheets/fs_2014-dbir-industries-financial-services-threat-landscape_en_xg.pdf

Verizon Vertical Insight (2014). *2014 Data Breach Investigations Report Manufacturing*. Retrieved from http://www.verizonenterprise.com/resources/factsheets/fs_2014-dbir-industries-financial-services-threat-landscape_en_xg.pdf

Verizon Vertical Insight (2014). *2014 Data Breach Investigations Report Healthcare*. Retrieved from http://www.verizonenterprise.com/resources/factsheets/fs_2014-dbir-industries-healthcare-services-threat-landscape_en_xg.pdf

Verizon Vertical Insight (2014). *2014 Data Breach Investigations Report Retail*. Retrieved from http://www.verizonenterprise.com/resources/factsheets/fs_2014-dbir-industries-retail-services-threat-landscape_en_xg.pdf

Verizon Research Report (2013). *Threat Landscape RETAIL, ACCOMMODATION AND FOOD SERVICES.* Retrieved from http://www.verizonenterprise.com/resources/factsheets/fs_dbir-industries-retail-threat-landscape_en_xg.pdf

Verizon Research Report (2013). *Threat Landscape HEALTHCARE*. Retrieved From http://www.verizonenterprise.com/resources/factsheets/fs_dbir-industries-healthcare-threat-landscape_en_xg.pdf

Verizon Research Report (2013). *Threat Landscape FINANCIAL SERVICES.* Retrieved

From http://www.verizonenterprise.com/resources/factsheets/fs_dbir-industries-financial-services-threat-landscape_en_xg.pdf

Verizon Research Report (2013). *Threat Landscape MANUFACTURING, SERVICES AND TECHNOLOGY*. Retrieved From http://www.verizonenterprise.com/resources/factsheets/fs_dbir-industries-manufacturing-services-technology-threat-landscape_en_xg.pdf

Wikipedia (2008). *Project Chanology*. Retrieved from http://en.wikipedia.org/wiki/Project_Chanology

Sean Atkinson, Seanwatkinson5@gmail.com

Appendix A: Profile analysis

Script Kiddie:

Threat Profile:	
Type:	Script kiddie/tinkerer
Industry targeted:	Any – usually based on the specific interests of the threat actor
Modes of attack:	Hacking tools and web "how to's"
Attributes:	Persistence and building skill
Identification:	Common forms of attack methods and creating a lot of noise in terms of perimeter and boundary intrusion detection alerts.
Remedy – reactive:	SIEM analysis and boundary defense to disrupt common threats and hacking enumeration and scanning techniques. CSC 14, 18
Proactive incident response:	Protecting against known or freely distributed enumeration and attack methods. Maintaining a comprehensive knowledge and understanding of newly found exploits and managing access controls appropriately across firewalls and internal network infrastructure. Which applications should be hardened against the OWASP top 10 threats as these methods that are widely known become the initial steps for hacking attempts. CSC 4, 9, 10, 11, 13, 19, 20
Psychological model:	Sub-cultural individual theory would apply in this case. Looking for meaning beyond common social constructs allows persons to find or seek methods that will allow them to ingratiate themselves into a sub cultural group.

Malicious Insider:

Threat Profile:	
Type:	Malicious Insider
Industry targeted:	Systems that dare freely available to them inside a corporate network
Modes of attack:	Depending on their position within the company, sys admins will have access to all systems under their responsibility (Snowden). Others will seek data that is not protected but should be PII or access to confidential information that can be sold to competitors
Attributes:	Greed
Identification:	Data Loss prevention will enumerate access to data at rest, in transit or in use. Do the persons accessing the information have a 'need to know'? Data classification and information owners should determine those who have a 'need to know' – although these person who exfiltate this data who have legitimate access is harder to detect but not impossible.
Remedy – reactive:	Understanding what has been taken and making sure that backup of the data exists if it has been deleted or

Sean Atkinson, Seanwatkinson5@gmail.com

	altered. Reviewing the actions that the person took will allow a timeline and forensic investigation to be pursued to capture all files and information accessed. CSC 8, 15, 17
Proactive incident response:	Managing user rights and privilege accounts will allow for a controlled review of who has access to what specific items and what can they do with it. Controlling and monitoring of user accounts will enable a view into data access across the enterprise and make sure the 'need to know' does exist and is required. Log management and analysis will be a first hand indicator of nefarious actions are being employed with denials to specific folder or files or unauthorized devices are connected to the system to remove data or via file sharing software. CSC 1, 2, 9, 12, 14, 15, 16, 17
Psychological model:	Moral disengagement, by giving me access or by not controlling access to data you have allowed me the opportunity to take what I feel entitled to or what I need to make more money.

Activist:

Threat Profile:	
Type:	Activist
Industry targeted:	Information and social media
Modes of attack:	Dependent upon the reasoning, denial of service attacks or administrative compromised in order to alter web pages and alter messages. Also the use of internal information to protest the use or manipulation of data.
Attributes:	Persistence
Identification:	Compromised systems and accounts will come to someone's attention after the message or systems are not operational. Alerts and identification of such events should be captured before a site or systems are completely compromised.
Remedy – reactive:	Understanding the threat and how a system was compromised will allow incident response to review specific traffic cause DoS or a service provider to lock down access to compromised accounts and return from a backup or erase and activist propaganda from sites, tweets or pages. CSC 8, 17, 18
Proactive incident response:	Traffic filtering and baseline reviews of network traffic will allow DoS to be predicted with enough time to filter the traffic based on the attackers IP. Information or data should be backed up that can be used to restore services, systems and pages to their original content before attacks occurred. CSC 3, 9, 10, 11, 13, 14, 16, 17,19
Psychological model:	Depersonalized disobedience: victimization and promotion of an ideal allows the attacker(s) to think of promoting a message rather than accept the structure of social constructs. These social niceties are removed

Sean Atkinson, Seanwatkinson5@gmail.com

	and the end goal is to promote or disrupt in order to project a message of fear or ideal.

Spy:

Threat Profile:	
Type:	Spy
Industry targeted:	Manufacturing and Professional
Modes of attack:	Internal or external compromise. Spy will use any system or social engineering attack available to accomplish their task.
Attributes:	Stealth and skill
Identification:	Information leakage and the industrial espionage ecosystem provide channels that are not easily infiltrated, this would mean that in order to find out a compromise exists, the information or data that was compromised has been used for its intent by a nation state or competitor to its full advantage will be released or found during anti-competitive practice engagements. In some cases the exfiltration may never be known.
Remedy – reactive:	Once an exfiltration has been discovered the response it to review if any other data has been compromised, how the attackers got that information and trace the activities within the system to provide patches, updates or hardening to prevent the event form occurring again. CSC 4, 8, 11, 13, 14, 18
Proactive incident response:	The management of security systems and a defense in depth approach is only as strong as the weakest systematic link; one of the most important proactive skills is that of training and end user awareness. It may be a clandestine act of social engineering that compromises a system in the first place so starting with people and working through the layers of defense is the best approach to combating espionage. CSC 1, 2, 3, 4, 5, 7, 9, 10, 11, 13, 14, 16, 17, 18, 19, 20
Psychological model:	Moral disengagement and a contained social learning theory environment. Morally compromising and stealing information has its own connotations within the moral disengagement; although this may be to benefit a nation state or company it still requires disengagement for social constructs of ownership and proprietary property rights. Internal to the espionage actors the group affiliations and social learning will promote such activities and will determine the need for a person to become ingratiated into a group through the ability to compromise and attain specific data.

Terrorist:

Threat Profile:	
Type:	Terrorism
Industry targeted:	Public, finance and information
Modes of attack:	All modes of attack can be part of a terrorist plot or

Sean Atkinson, Seanwatkinson5@gmail.com

	event. Attacks can be based on enumeration, espionage to find weaknesses and testing critical security infrastructure and until a significant weakness is found the infiltration and scanning of networks, people and system will continue.
Attributes:	Greed, skill, stealth and/or persistence
Identification:	The critical security controls should be used to identify all 20 areas where controls for detection, automation and testing are needed. Each method of prevention needs to be addressed when talking about those who want to find the weaknesses and have a moral, political, social or religious agenda to fulfil.
Remedy – reactive:	Once an attack has taken place the initial assessment will determine the reaction. Data protection, business continuity/ Disaster recovery will be required to manage the incident response process. CSC 4, 5, 8, 13, 14, 17, 18
Proactive incident response:	Prevention of such attacks and event will require a complete security infrastructure with specific target testing, automation, alerting and personnel that are equipped and trained to manage systems that are susceptible to attack. CSC: all controls
Psychological model:	Moral Disengagement and depersonalized disobedience are the constituent psychological profiles that exist for terrorists; morally being able to perform such acts that could cause mass hysteria requires a specific mindset. The depersonalized engagement allows the objective and specific need to perform the act to go beyond thinking of human lives or the disruption of services to those persons within the attack landscape.

Organized Crime:

Threat Profile:	
Type:	Organized Crime
Industry targeted:	Retail, food services and financial
Modes of attack:	Phishing, malware or infiltration of networks through unauthorized access or devices.
Attributes:	Persistence and greed
Identification:	Data exfiltration and financial losses should indicate a compromise exists, based on the need to keep such communication channels open, the compromise should be seen in the current infrastructure as the mentality is to keep getting this valuable information from the compromised system.
Remedy – reactive:	Incident response should be to close the network connection and open ports to disrupt the kill chain. Forensic review of such channel and data accessed during the compromise should be reviewed. One the important facts in similar cases are that an external party identifies the compromise rather than it being detected internally.

Sean Atkinson, Seanwatkinson5@gmail.com

	CSC: 1, 5, 7, 8, 13, 14, 17, 18
Proactive incident response:	Management of protected system though a layered security approach that provides comprehensive coverage and continually review will allow a mature security proactive response to being compromised. A big part of this again is the human element that through psychological manipulation can compromise system with data exchange or file execution that initiates such events to occur. CSC: 1, 2, 3, 4, 5, 10, 11, 13, 14, 16, 17, 18, 19, 20
Psychological model:	Moral Disengagement in that the financial gains are put ahead of the crime and effect that it will have on the persons, businesses or government that the attack is being performed against. Unlike a physical crime, the crime itself is a transfer of data and no person is physically injured or out in harm's way in that a face to face confrontation is avoided so reduces the social context of not performing crimes against another.

Sean Atkinson, Seanwatkinson5@gmail.com

Appendix B: Symptoms and response.

Threat	Symptoms	Current Response
POS Intrusion	PCI data compromised, poor configuration controls on new hardware and deployed systems. Compromises are found through law enforcement or fraud related agencies (Banks, etc.)	90% of attacks take weeks or more to discover, the targets are smaller business that lack the security infrastructure or know how to prevent these crimes or provide a means into larger stores infrastructure.
Web Application	Using website for the exfiltration and access to user accounts, organized crime is utilizing malware to install spyware/keystroke loggers to gain the credentials to access accounts.	Given the monetary motivation, 15% of online customers were a first responder to such crimes using web applications. Noticing money missing from accounts or mysterious charges has prompted customer recognition of insecurity within the current web application infrastructure. Two factor authentications is a prime example of securing authorizations. OWASP and the top 10 application security risks for web applications have increased a awareness for secure software development lifecycle to thwart SQL injection and cross-site scripting attacks.
Insider Misuse	Having an inside source of information or a person inside the wall with access to critical systems a provide challenges in detection especially when such personnel have a need for access to sensitive systems.	Background checks and pre-employment interviews seem to be the steps taken currently to diagnose if a person is trustworthy.
Theft/Loss	Insider assistance in order to gain access through intentional or by use error. IP theft is harder to discover as response times are based on months and years of knowledge of an intrusion or theft.	Add more systems of security and make sure that IP is protected at all costs, but from an external perspective.
Errors	Clicking a compromised file or failing victim to a phishing attack will allow malware to be executed against network assets.	A onetime awareness training and reliance upon spam filters and IT teams to control what makes it into a network and what policies are in place to consider what acceptable use is.
Crimeware	The exfiltration of credentials, funds or confidential information from a network surreptitiously.	Checking for web application vulnerabilities and the services enabled within an enterprise reduces some of the delivery vectors that can be utilized. Vulnerability scanning and system hardening exist to control the prevalence of such malware.
Card Skimmers	POS tampering allows card readers to be installed and allows the transfer of PCI data to an external device.	Considered inevitable and uncontrollable the use of external readers attached to POS systems and ATMs. The response is reactive rather than being proactive for such fraud.
DoS- Denial of Service	Systems are disabled or do not function as	As a reactive process utilizing

Sean Atkinson, Seanwatkinson5@gmail.com

	the system or service is compromised in terms of requests for content/ access, thus crashing the system's ability to provided content or service.	upstream filtering to circumvent the attack vector, IPS can be used to stop the attempts, rate limiting and black holing malicious traffic are methods to react and response to such a threat.
Espionage	IP will be the target of industrial espionage or sponsored attacks.	Current methods are to control access to such data and engage added protection mechanisms such as defined security groupings, two factor authentication and 'need to know' level of least privilege.

Sean Atkinson, Seanwatkinson5@gmail.com

Appendix C: Revised Incident Response

Threat	Revised incident response
POS Intrusion	Knowing the vulnerabilities the retailers can prevent system compromise through routine activities, POS strong password and authentication, malware detection and intrusion reviews to eliminate POS command server and the POS systems from tampering. This will be a good offensive strategy to close the gaps in security. Understanding that PCI data is the target the data loss prevention strategy would be to build controls around systems that store, transport or use this data. Any system within this infrastructure should be reviewed for security controls as well as PCI-DSS compliance.
Web Application	The attack vector is used for fraud and misappropriation of money or products from compromised websites or stolen credentials. The appropriate monitoring of systems and logging of events are essential elements of incident response. Vulnerability management will eliminate common threats against a web infrastructure and those anomalies should be detected through malicious input and breaks in web access trends.
Insider Misuse	Behavioral analysis and system account auditing events through an integrated SIEM and DLP infrastructure will determine illicit events originating from the internal population. Access monitoring to 'Crown Jewels' information will highlight those who should have access and those that have access but no reason to view or query such information – such as system administrators.
Theft/Loss	Similar to insider misuse the audit and review of access levels need to be revised continually and augmented against insider movement or termination – providing sufficient motive to steal information that they believe to have some possession against. A psychological profile or risk flag should be highlighted against anyone leave or coming into an organization from a competitor.
Errors	Internal use and errors within the authorized population is a common occurrence within any electronic infrastructure. Spotting these anomalies lies with behavioral analysis of system use as well as applications and network component operating baselines. The first line of defense is a properly configured SIEM that promotes and categorizes the behavioral analysis of users and internal systems.
Crimeware	Knowing the target and knowing the common vectors for attack. Combining the IPS and vulnerability management into a training program that focuses on social engineering and indicators of attack for simple system users to system administrators, can prevent malicious entry.
Card Skimmers	A conscious review of terminals, POS and ATM's will highlight added periphery or unusual card reading devices.
DoS- Denial of Service	Incident response and understanding common DoS threats to similar organizations will allow for IPS automation and black holing specific traffic will enable a understanding of what attacks vectors will be used as well as understanding who would be attempting such attacks i.e. depending on the type of industry, attacks may be prevalent in hacktivist attacks or IP theft.
Espionage	Determining the aim of espionage is to gain IP or CI, organizations need to have a method to define data classification. Knowing what needs to be protected and that extremely skilled personnel will target or system to gain access to this coveted prize. Systems of access controls, authentication mechanisms, internal network sensors and protection mechanisms should be employed to match the financial contribution such information has within the enterprise.

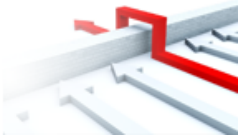
Sean Atkinson, Seanwatkinson5@gmail.com

Last Updated: December 13th, 2019

Upcoming SANS Penetration Testing

SANS PENETRATION TESTING

Click Here to {Get Registered!}



Community SANS Portland SEC542	Portland, OR	Dec 16, 2019 - Dec 21, 2019	Community SANS
SANS Austin Winter 2020	Austin, TX	Jan 06, 2020 - Jan 11, 2020	Live Event
Mentor Session - SEC504	Minneapolis, MN	Jan 08, 2020 - Feb 19, 2020	Mentor
Mentor Session - SEC504	Colorado Springs, CO	Jan 10, 2020 - Jan 31, 2020	Mentor
Miami 2020 - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	Miami, FL	Jan 13, 2020 - Jan 18, 2020	vLive
SANS Threat Hunting & IR Europe Summit & Training 2020	London, United Kingdom	Jan 13, 2020 - Jan 19, 2020	Live Event
SANS Miami 2020	Miami, FL	Jan 13, 2020 - Jan 18, 2020	Live Event
Community SANS Columbia SEC542 @UKI	Columbia, MD	Jan 20, 2020 - Jan 25, 2020	Community SANS
SANS Amsterdam January 2020	Amsterdam, Netherlands	Jan 20, 2020 - Jan 25, 2020	Live Event
SANS Anaheim 2020	Anaheim, CA	Jan 20, 2020 - Jan 25, 2020	Live Event
Cyber Threat Intelligence Summit & Training 2020	Arlington, VA	Jan 20, 2020 - Jan 27, 2020	Live Event
SANS Vienna January 2020	Vienna, Austria	Jan 27, 2020 - Feb 01, 2020	Live Event
SANS Las Vegas 2020	Las Vegas, NV	Jan 27, 2020 - Feb 01, 2020	Live Event
SANS San Francisco East Bay 2020	Emeryville, CA	Jan 27, 2020 - Feb 01, 2020	Live Event
Community SANS Quantico SEC504	Quantico, VA	Jan 27, 2020 - Feb 01, 2020	Community SANS
Mentor Session - SEC504	Online, TX	Jan 29, 2020 - Apr 01, 2020	Mentor
SANS Security East 2020	New Orleans, LA	Feb 01, 2020 - Feb 08, 2020	Live Event
Security East 2020 - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	New Orleans, LA	Feb 03, 2020 - Feb 08, 2020	vLive
Security East 2020 - SEC560: Network Penetration Testing and Ethical Hacking	New Orleans, LA	Feb 03, 2020 - Feb 08, 2020	vLive
Community SANS Seattle SEC504	Seattle, WA	Feb 03, 2020 - Feb 08, 2020	Community SANS
Mentor Session - SEC504	Seattle, WA	Feb 04, 2020 - Mar 24, 2020	Mentor
SANS vLive - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	SEC504 - 202002,	Feb 04, 2020 - Mar 12, 2020	vLive
SANS Northern VA - Fairfax 2020	Fairfax, VA	Feb 10, 2020 - Feb 15, 2020	Live Event
SANS New York City Winter 2020	New York City, NY	Feb 10, 2020 - Feb 15, 2020	Live Event
SANS London February 2020	London, United Kingdom	Feb 10, 2020 - Feb 15, 2020	Live Event
Mentor Session - SEC504	Ann Arbor, MI	Feb 12, 2020 - Apr 22, 2020	Mentor
SANS Dubai February 2020	Dubai, United Arab Emirates	Feb 15, 2020 - Feb 20, 2020	Live Event
SANS San Diego 2020	San Diego, CA	Feb 17, 2020 - Feb 22, 2020	Live Event
SANS Brussels February 2020	Brussels, Belgium	Feb 17, 2020 - Feb 22, 2020	Live Event
SANS Scottsdale 2020	Scottsdale, AZ	Feb 17, 2020 - Feb 22, 2020	Live Event
Community SANS Omaha SEC504	Omaha, NE	Feb 17, 2020 - Feb 22, 2020	Community SANS