Volume 4 Issue III, March 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

An Analysis on Cyber Crime, Cyber Threats and Role of Cyber Analyst

Miss. Debalina Nandy[1], Mr. Renish J Padariya[2]
[1,2]*Assistant Professor, Computer Engineering Department*
[1]*Atmiya Institute of Technology & Science, Rajkot, Gujarat*
[2]*Om Engineering College, Junagadh, Gujarat*

Abstract - Computer crime is a general term that embraces such crimes as phishing, credit card frauds, bank robbery, illegal downloading, industrial espionage, child pornography, kidnapping children via chat rooms, scams, cyber terrorism, creation and/or distribution of viruses, Spam and so on. All such crimes are computer related and facilitated crimes. With the evolution of the Internet, along came another revolution of crime where the perpetrators commit acts of crime and wrongdoing on the World Wide Web. Internet crime takes many faces and is committed in diverse fashions. The number of users and their diversity in their makeup has exposed the Internet to everyone. Some criminals in the Internet have grown up understanding this superhighway of information, unlike the older generation of users. This is why Internet crime has now become a growing problem in the United States. Some crimes committed on the Internet have been exposed to the world and some remain a mystery up until they are perpetrated against someone or some company.
Keywords: Cyber Crime, Definition, Cyber Threat, Threat Analyst

I. INTRODUCTION

Computer fraud is any dishonest misrepresentation of fact intended to let another to do or refrain from doing something which causes loss. In this context, the fraud will result in obtaining a benefit by altering in an unauthorized way. It requires little technical expertise and is common form of theft by employees altering the data before entry or entering false data, or by entering unauthorized instructions or using unauthorized processes like altering, destroying, suppressing, or stealing output, usually to conceal unauthorized transactions. Government officials and Information Technology security specialists have documented a significant increase in Internet problems and server scans since early 2001. But there is a growing concern among federal officials that such intrusions are part of an organized effort by cyber terrorists, foreign intelligence services, or other groups to map potential security holes in critical systems. A cyber terrorist is someone who intimidates or coerces a government or organization to advance his or her political or social objectives by launching a computer-based attack against computers, networks, or the information stored on them. Cyber terrorism in general, can be defined as an act of terrorism committed through the use of cyberspace or computer resources. As such, a simple propaganda in the Internet, that there will be bomb attacks during the holidays can be considered cyber terrorism. As well there are also hacking activities directed towards individuals, families, organized by groups within networks, tending to cause fear among people, demonstrate power, collecting information relevant for ruining peoples' lives, robberies, blackmailing etc. Cyber crimes are any crimes that involve a computer and a network. In some cases, the computer may have been used in order to commit the crime, and in other cases, the computer may have been the target of the crime.

A. Changing Nature of Cyber Crime

New trends in cybercrime are emerging all the time, with estimated costs to the global economy running to billions of dollars. In the past, cybercrime was committed mainly by individuals or small groups. Today, we are seeing highly complex cybercriminal networks bring together individuals from across the globe in real time to commit crimes on an unprecedented scale. Criminal organizations turning increasingly to the Internet to facilitate their activities and maximize their profit in the shortest time. The crimes themselves are not necessarily new – such as theft, fraud, illegal gambling, and sale of fake medicines – but they are evolving in line with the opportunities presented online and therefore becoming more widespread and damaging. The different types of Internet crime vary in their design and how easily they are able to be committed. Internet crimes can be separated into two different categories. There are crimes that are only committed while being on the Internet and are created exclusively because of the World Wide Web. The typical crimes in criminal history are now being brought to a whole different level of innovation and

ingenuity. Such new crimes devoted to the Internet are email “phishing”, hijacking domain names, virus immistion, and cyber vandalism. A couple of these crimes are activities that have been exposed and introduced into the world. People have been trying to solve virus problems by installing virus protection software and other software that can protect their computers. Other crimes such as email “phishing” are not as known to the public until an individual receives one of these fraudulent emails. These emails are cover faced by the illusion that the email is from your bank or another bank. When a person reads the email he/she is informed of a problem with he/she personal account or another individual wants to send the person some of their money and deposit it directly into their account.

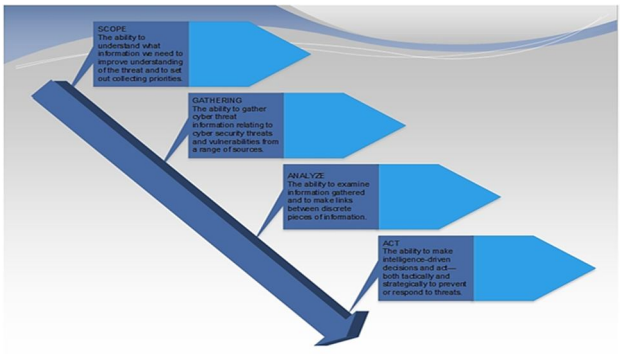
B. Statistics

The statistics that have been obtained and reported about demonstrate the seriousness Internet crimes in the world. Just the "phishing" emails mentioned in a previous paragraph produce one billion dollars for their perpetrators (Dalton 1). In a FBI survey in early 2004, 90 percent of the 500 companies surveyed reported a security breach and 80 percent of those suffered a financial loss (Fisher 22). A national statistic in 2003 stated that four billion dollars in credit card fraud are lost each year. Only two percent of credit card transactions take place over the Internet but fifty percent of the four billion, mentioned before, are from the transaction online (Burden and Palmer 5). All these finding are just an illustration of the misuse of the Internet and a reason why Internet crime has to be slowed down. The question about how to police these crimes has already been constructed, but this task is turning out to be an uphill battle. Since the first computer crime law, the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, the government has been trying to track down and stop online criminals. The FBI has tried many programs and investigations in order to deter Internet crime, like creating an online crime registry for employers (Metchik 29). The reality is that Internet criminals are rarely caught. One reason is that hackers will use one computer in one country to hack another computer in another country. Another eluding technique used is the changing of the emails, which are involved in virus attacks and “phishing” emails so that a pattern cannot be recognized. An individual can do their best to protect themselves simply by being cautious and careful. Internet users need to watch suspicious emails, use unique passwords, and run anti-virus and anti-spyware software. Do not open any email or run programs from unknown sources.

II. CYBER THREAT ANALYSIS

A threat could be anything that leads to interruption, meddling or destruction of any valuable service or item existing in the firm’s repertoire. Whether of “human” or “nonhuman” origin, the analysis must scrutinize each element that may bring about conceivable security risk. Cyber threat analysis is a process in which the knowledge of internal and external information vulnerabilities pertinent to a particular organization is matched against real-world cyber attacks. With respect to cyber security, this threat-oriented approach to combating cyber attacks represents a smooth transition from a state of reactive security to a state of proactive one. Moreover, the desired result of a threat assessment is to give best practices on how to maximize the protective instruments with respect to availability, confidentiality and integrity, without turning back to usability and functionality conditions.

A. Components of Threat Analysis as a Process



Scope gives info on what is included and what is not in the analysis. In terms of cyber security, items under consideration are those that must be protected. Although they need to be identified in the first place, the level of sensitivity of what is being guarded should be defined as well by analysis drafters.

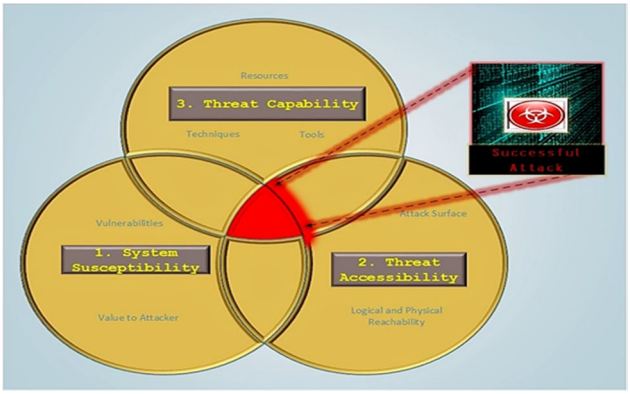
1) Data Collection In every respectable organization there are some sort of policies and procedures. Those need to be identified for

Volume 4 Issue III, March 2016
ISSN: 2321-9653

compliance purposes. In reality, almost one-fourth of the defensive capabilities corporations have in place fail to meet the minimum security standards. Amassing detailed information about real cyber incidents (e.g., URLs to malicious links, phishing email header and content, and uncovered hostile Command and Control (C2) infrastructure of domain names and IP addresses) is the first step. The focus should fall on targeted threats existing in reality, and scope settings need to filter out those perceived as such but not real, which can merely distract your attention from other ongoing security affairs. An IT analyst must have unrestricted access to data in order to transform it into intelligence. Sources of information are, for example, intrusion incidents, detection system logs, firewall logs, the reverse engineering of malware, open source Internet searches, honeypots, digital forensic analysis, etc. Of course, one source simply cannot provide all of the information needed for a thorough threat analysis, and the analyst should incorporate multiple data wells seamlessly. Once all corporate policies and procedures are collected, they should be examined to show whether they match the compliance level in the organization. Consequently, logically processing vast amounts of data and thinking critically are qualities that will form a good cyber analysis.

2) Threat/Vulnerability Analysis Of Acceptable Risks : Here we test what is being gathered to determine the level of current exposure — most of all — whether the current defenses are solid enough to neutralize information threats in terms of availability, confidentiality and integrity. This part should include as well an evaluation of whether the existing procedures, policies and security measures are adequate. Vulnerability analysis also encompasses penetration testing, which in turn seeks to acquire something valuable from the adversary's arsenal like a classified document, code or password.

3) Mitigation & Anticipation: When all previous steps are completed, a competent security analyst can use this corpus of threat data to arrange in group's activity patterns of close similarity, attribute each pattern to specific threat actors, promptly implement mitigation measures, and anticipate the emergence of similar cyber attacks in the future.



When a Cyber Attack Encircles the Rings of Protection

III. THREAT ANALYST AND ASSESSMENT ABILITIES

Based on both vulnerability and risk assessment, the analyst approaches to determine the level of risk within his organization. He further defines what security measures need to be taken or remove the ineffective ones. In addition, the analyst should be careful not to push ahead with a too overprotective security system, as it may prove unfoundedly costly to the organization. HP's Gilliland estimated that roughly 86% of security budgets available to cyber security teams are expended on warding off malicious attempts at the infiltration stage. Many organizations face the issue of avoiding false positives, an imminent occurrence in assessment of applications. The best way to mitigate the problem is to ensure that applications in question are up-to-date with latest patches and signatures. Becoming a strong technical expert is a must. Glancing through tons of practice and reading countless of security books and blogs is perhaps the right kind of bushido code to master your skills – there is no substitution for hard work. Additionally, the data in hand is often derived from intelligence products. Technical writing skills are necessary since analysts need to create security reports. Evidentially, the ability to construe security events and read off appliances are among the most important sets of skills an analyst should possess. At times this ability is not an exact science, it is more like an art where the person simply has to have a flair for it. In this line of work, making a correct analysis comes hand in hand with the analyst's technical knowledge. For instance, a security analyst who does not comprehend routing protocols and infrastructure cannot analyze what happens when a threat actor sends malformed TCP packets to a company's servers. The same can be said for a situation where the analyst cannot tell the

difference between an ineffective zero-day and a zero-day that can inflict real damage. On the other hand, other persons sometimes produce a bad analysis that can be misleading. Therefore, the analyst's ability to distinguish good from bad is critical here, even more important than creating a good product.

A. Thread Metrics

A decent threat measurement can facilitate analysis through improved understanding of how trends and anomalies occur. It can also underscore the imminence of certain types of vulnerabilities and connect missing dots between threats and potential consequences. In other words, a qualitative threat measurement can yield accurate results concerning risk management. Unfortunately, defining and applying threat measures of proper quality is a practice that lacks maturity and consistence.

The notion "metric" denotes a unit of measure, while 'measure' stands for a given hallmark of performance. If we measure some event in a consistent way—using a good metric that is unambiguous and clear as well—the analyst will most likely improve his ability to understand that event (threat in our case), control, affect and defend against it to a certain extent. And if the nebulosity is not so dark, decision-making based on correct interpretation will be much simpler. An example of a good quantitative portrayal in cyberspace would be the number of attacks per month. Measured for a long stretch of time, the count of cyber attacks can reveal the adversary's capability and intent, allowing analysts in turn to calculate properly the risk and allocate needful resources to cope with it.

B. Threat Models

A stand-alone metric is oftentimes insufficient to encapsulate behavioral characteristics of complex systems/actors. A combination of metrics, the so-called "measurement framework", might do the job. A threat (in addition to the definition given at the beginning) is "a malevolent actor, whether an organization or an individual, with a specific political, social, or personal goal and some level of capability and intention to oppose an established government, a private organization, or an accepted social norm. Uniform threat models promote consistency, and on the other hand, they reduce the negative effects of preconceived notions and personal bias. Furthermore, the index of success rate intensifies as the time goes by. For that reason, inter alia, the analyst is advised to store threat reports in a continuous manner in order to build up a reference database that can be used by other experts.

IV. CONCLUSION

In April 2014, the U.S. DOJ Antitrust Division and the FTC released a joint statement on creating a uniform policy for mutual threat information exchange. This policy has the potential to enhance "the security, availability, integrity, and efficiency of the nation's information systems" without raising antitrust concerns because "the sharing of cyber security information is highly unlikely to lead to a reduction in competition and, consequently, would not be likely to raise antitrust concerns." So exchanging threat information has been looked upon with a favorable eye, but that should be generally accepted practice for all entities in a particular field. Most of all, organizations should remember that not performing a threat and risk analysis will leave them open to cyber pests that can damage their business for good. Nothing is more detrimental in the world of cyber security than the feeling of invulnerability or trusting that your lucky star will extend by all means its reach to magically patch up the holes in your system through which threats are waiting to get in.

REFEENCES

[1] Lance J. Hoffman, Daniel Ragsdale: Exploring a National Cyber Security Exercise for Colleges and Universities, IEEE Security and Privacy, Volume 3, Issue 5 (September 2005).
[2] Wayne Schepens, Daniel Ragsdale, John Surdu, the Cyber Defence Exercise: An Evaluation of the Effectiveness of Information Assurance Education, the Journal of Information Security, Volume 1, Number 2. July, 2002.
[3] Susan W. Brenner, Cybercrime: Criminal Threats from Cyberspace, ABC-CLIO, 2010.
[4] Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.
[5] Frincke, D., Wespi, A., Zamboni, and D: From Intrusion Detection to Self-Protection, Computer Networks 51, 1233--1238 (2007).
[6] Karat, J., Karat, C.-M., Brodie, C., Feng, J.J.: Privacy in Information Technology: Designing to Enable Privacy Policy Management in Organizations Int. J. Human.-Computational Studies, 63, 153--174 (2005)
[7] Axelsson, S the base-rate fallacy and the difficulty of intrusion detection. ACM Trans. Information and System Security, 3(3):186–205, 2000.
[8] Rao, A.S., Georgeff, M.P.: BDI Agents: From Theory to Practice. In: First International Conference on Multi-Agent Systems (ICMAS-95) pp. 312—319, AAAI Press, Menlo Park, CA, USA (1995).