Policing Cyber Terrorism

Phillip R. Neely, Jr., Saint Leo University, USA
Michelle T. Allen, Saint Leo University, USA

ABSTRACT

In order to police a crime there must be an act that is considered a crime and punishable under the law. There also must exist the capability to investigate for potential suspects and obtain physical or circumstantial evidence of the crime to be used in criminal proceedings. The act of gaining unauthorized access to a network system is a criminal act under federal law. Several key factors are presented during the course of this discussion and then built upon. Two methods of attack planning are presented. The attack planning cycle for traditional terrorist and then cyber terrorists planning used to penetrate a network system. Supervisory Control and Data Acquisition System (SCADA) are defined and presented as an important critical target within the nation's infrastructure. Examples of successful attacks are presented. A brief overview is used to present malicious software and the effects of its use against SCADA systems. The path for which data takes through a network is explained. The importance of the data path is vital in understanding the five methods of attribution which serve as methods of investigating cyber terrorism.

Keywords: Cyber; Terrorism; SCADA; Policing

INTRODUCTION

In order to understand the full scope of cyber terrorism, one must understand the cyber world. In an effort to narrow the scope of the discussion while at the same time illustrating what is meant by cyber terrorism, the author will provide a carefully guided examination on the issue of cyber terrorism. The author will give meaning to the terms of cyber, terrorism, and police. The reader will then be guided through a technical discussion of the cyber concepts, Supervisory Control and Data Acquisition (SCADA) Systems, and a very brief tutorial on malicious software. The path that data takes as it travels through the network will be explained followed by the concepts of attribution.

When cyber and terrorism are combined, the environment of the battle space changes. In the traditional sense, acts of terrorism or battle space are seen by, if no one else, the victims of the attack. The events that occurred on September 11th were viewed by millions around the world through the use of social media. In cyber terrorism, the battle space is in the virtual sense. Acts of hostility are unseen until the events have occurred. Even then they may not be discovered immediately. The initiating devices are also different. Explosive devices give way to computer worms and viruses that are used to penetrate their intended target in order to achieve the results of the more traditional understanding of terrorism.

BACKGROUND

Since the operation of the world runs through cyber space, consideration for target selection has no bounds for a terrorist. Therefore, the discussion should now focus on the planning phase of a terrorist's target selection. While there is no specific profile model for terrorists to select their targets, there are some commonalities (Habash, 2007).

The methodology for a terrorist attack is to achieve the best results with the least amount of risk. In general, terrorists will opt not to attack a target that has strong security measures. They will attack a target with whichever weapons are available to them for the task. The traditional method implements seven phases.

Phase one begins with a wide selection of targets. Collection of information is from a number of sources to include; sympathizers, media, news publications, and other terrorists. With the advent of the internet, terrorists who have a computer with a browser and a connection can sit in a quiet location and gather meaningful information to include

blueprints and other historical information pertaining to a target. Terrorists will screen information during this phase and determine the best target to support their cause. Key items of interest that factor into their selection are; the number of potential causalities, potential media attention, symbolic value, and relationship to critical infrastructure (Habash, 2007).

Phase two is the surveillance and intelligence collection phase. Terrorists observe the daily routine of the target. Are deliveries made? If so, what kind and by who? They also examine the security measures in place. Is there a guard force and do they frequently conduct drills? Does the guard force react quickly? Does the target utilize any technology such as cameras? Are there any inspection procedures in place for packages or vehicles? Is the target hardened with pop up vehicle barriers or any other security measures that would make penetration more difficult? In short, are there any vulnerabilities that can be exploited to make penetration into the target easier? If not, the target is bypassed and they move onto the analysis of another target. In 2004, targets under surveillance include the financial institutions of the New York Stock Exchange and the Prudential Building (Habash, 2007).

During phase three, each previously selected target undergoes further analysis. Specific questions must be answered. Does the target represent a symbolic value that will lend to the cause of the group? If so, will the attack result in wide spread media coverage? Will there be a high casualty count and will the resources that are applied to the target provide the best results? If the answers are yes, the group will proceed to the next phase of the planning cycle (Habash, 2007).

Phase four is the pre surveillance phase. In this phase, the target is exposed to more thorough intelligence gathering. All previous intelligence is reevaluated while paying closer attention to the vulnerabilities expected to be exploited. The actual plan of attack is developed in this phase to include; weapon selection, target breeching specifications, and plan of escape (Habash, 2007).

Phase five begins the refinement of the attack. Training is conducted on specific tactics, techniques, and specialized equipment. The attack is rehearsed to determine if there are any specific concerns or additional training and equipment needed to successfully complete the mission (Habash, 2007).

In phase six, final surveillance is conducted on the target. Timing of the attack and specific locations of entry are determined. The terrorists will determine if either primary or secondary diversionary measures will be used (Habash, 2007).

In the seventh and final phase, the terrorist will determine who they plan to exploit with the results of the attack. Will they have prepared statements claiming their attack? They will also conduct final planning and rehearsal of the escape plan (Habash, 2007).

LITERATURE REVIEW

Investigators should understand the five steps to a cyber-attack. Similar in nature to the traditional planning cycle of a terrorist attack, they involve a reconnaissance for information, defense penetration, setting modification, further systems infection, and paralyzing a network (Ciampa, 2009).

Reconnaissance for information or determining vulnerabilities takes place in several forms. It can include ping sweeps, port scanning, and attempts to decipher specific passwords (Ciampa, 2009). Each will be briefly addressed.

Every machine that accesses the internet has an address. Similarly, each application has a specific port for the transmission of data. To better understand this, think of the internet as an apartment building. The internet address of the computer would be the address to the building and the port number that would correspond to the individual apartment number. A socket is the internet address of the machine combined with the port number. A socket has specific numbers. Therefore, a machine or host signed onto the Internet understands that specific data entering a specific port is from a specific known process (Dean 2010).

Network Mappers is software used to identify which systems are connected to a network. An example of a very simple network is a small business that has all of its computers or nodes linked to the business network. The ping is a packet or message that is sent out to determine which systems are attached to the network. A network administrator will use this software to identify which nodes are attached to their business network. This will identify unauthorized users as well. A terrorist can use the same software to ping a network in their target selection phase (Ciampa, 2009).

A terrorist can also use software referred to as a Port Scanner. A Port Scanner will provide three pieces of information: if the port is open, closed or blocked. If the port is open, it is receiving and transmitting data. It is also a path into the machine to exploit. If closed, the opposite is true. If blocked, the host will not respond to the ping (Ciampa, 2009).

Passwords are the weakest form of protection for a computer system. In an attempt to gain access to a system, an attacker will attempt to gain access by using common passwords that are associated with specific software. The purpose of passwords is to allow the network administrator who controls and monitors the system to gain access to the system. However, it is understood that these are very easy to remember passwords such as, "Admin001" are to be changed by the administrator once the software is installed onto the system (Ciampa, 2009). If they fail to do this, their ease of access becomes the attacker's ease of access since they are common to specific systems and universally used.

After information has been gained on the system an attack is launched into the targeted system. The purpose of the attack is to penetrate the defenses of the system. This phase evaluates the targets security measures. Penetration can be made through the use of Security Administrator Tool for analyzing Networks (SATAN). SATAN evaluates the security of the SACADA system to identify vulnerabilities without damaging the system. The design of SATAN was to help network administrators expose vulnerabilities and provide a course of action to correct them. In the hands of an attacker, they have the ability to expose a weakness for further exploitation (Ciampa, 2009).

In the Modification Phase, the attacker will create a path to reenter the system. This is completed by adjusting security settings. This adjustment is performed to permit future access by the attacker (Ciampa, 2009).

In the system infection phase, the attacker may reenter the system through the information gained from the previous phase. Once entry is regained, the system may be used as a base to initiate a second attack on different systems. The tools previously identified and explained in the paragraphs above may also be used in this phase in order to gain access to a second system (Ciampa, 2009).

In the last phase, networks and systems that have surreptitiously been entered can be maliciously damaged or paralyzed through the introduction of viruses or worms (Ciampa, 2009). In this regard the attacker may steal intellectual property, destroy the computer, and change the settings on SCADA system components such as valves and sensors to paralyze or cause catastrophic damage to a system.

Police investigators must understand the types of tools an attacker has at their disposal just like they understand the tools of a check forger are the check a pen. Consider the assassination of President Kennedy. Lee Harvey Oswald's used a Mannlicher – Carcano rifle as his tool to kill President Kennedy. Oswald had training to support his marksmanship from the United States Marine Corps (Shenon, 2013).

As seen in historical events, terrorists will use many conventional methods to attack. Explosive laden boats were used in an attempt to destroy United States Naval Ships, commercial aircraft was used to fly into skyscrapers, explosives and tactics that are the equivalent to active shooters. However, in the cyber world these weapons are much different.

Cyber-attacks are considered the greatest threat to the nation's national security. These attacks are committed using malicious software or malware. The weapons used in the cyber world include viruses and worms. Once malware enters a computer system, it seeks out its intended area of a system and performs the desired act. The results can be

catastrophic to a SCADA system. A very brief explanation will be provided of viruses, worms, Trojan horses, malicious codes, and what is referred to as a blended attack.

A virus is malware that inserts into its targets files or programs. Execution of the virus is performed by the targets operating system. The virus will attach itself to the different files to include removable devices plugged into the computer through the universal serial bus (USB) ports. Other viruses attach themselves to program applications such as email once it is launched (Radack 2005).
Worms are able to self-duplicate without the assistance of the SCADA system. They can travel and infect through mass mailings. Another way is to infect the network that supports the SCADA system (Radack, 2005).

A Trojan horse is exactly like the store it represents. They appear to be harmless. Once opened, they cause a great deal of damage to a system and software (Radack, 2005).

A Mobile code is used by the attacker to penetrate the vulnerabilities of the system and expose weaknesses. A blended attack will use a combination of the above mention weapons to penetrate and expose a SCADA system (Radack, 2005). Examples will be provided to lend some credibility and evidence of the existing problem with SACADA systems.

Historical evidence is important to investigators as it provides examples to investigators with which they can build profiles of the terrorist, the act, and the methodology of the attack. Examples of this are the use of worms or a virus. Some important examples will now be provided.

In 1982, a pipeline in Siberia was infected by a Trojan horse intruder. This resulted in an explosion with the same magnitude of 3 kilotons of TNT. This was the first recorded attack on a SCADA system (Miller & Rowe, 2012).

In 1992, the Chevron plant located in Richmond, California had two satellite sites which were located in New York and San Jose, California penetrated. The attacker changed the settings on the system located in Richmond causing it to crash. The item of interest in this attack was the offices located outside the target area that were compromised. The result of the action was an unannounced release of toxins into the atmosphere with no warning to the public for a period of 10 hours (Miller & Rowe, 2012).

In 1997, an attacker penetrated a telephone company that serviced the Worchester, Massachusetts Airport. This attack resulted in the loss of all services used to operate the airport. The airport was completely paralyzed and placed the health and wellbeing of travelers and members of the immediate surrounding community in jeopardy. The denial of service attack was made by a juvenile. Denial of service attacks send countless messages to a server that controls information resulting in the network devices shutting down because it is incapable of supporting the system (Miller & Rowe, 2012).

The list of attacks grows with the 1999 Bellingham, Washington Gas Pipeline, 2000 Maroochy Water System in Queensland, Australia, 2001 California System Operator, 2003 Davis-Besse Nuclear Power Plant located in Ohio, 2003 CSX Corporation which shut down train signals, and 2007 Teham Colusa Canal Authority had unauthorized software loaded onto the SCADA system by a terminated employee (Miller & Rowe, 2012). Several more attacks have taken place since. One more interesting but deadly example is the 2010 STUXNET worm that was found in a nuclear enrichment plant in Natanz, Iran. The SCADA system was not penetrated from outside like other examples. An unidentified individual used a thumb drive and plugged it into the USB port. The worm sought out specific PLC which controlled the nuclear enrichment centrifuges. In doing so, it caused the centrifuges to speed up and slow down violently. The control room operator was not aware of the increase and decrease in speed since the information he was receiving in the booth indicated the machines were operating properly. This resulted in the damage to multiple centrifuges slowing the nuclear enrichment process for Iran (Miller & Rowe, 2012). These historical examples of attacks to SCADA systems are reason for concern. Therefore, it is the responsibility of law enforcement agencies to investigate and arrest suspects.

Consider the advantage to a terrorist who wants to inflict damage on the United States in support of their cause. All they need is a computer with a browser that has access to an Internet. As previously discussed, target planning can

be performed through the use of the Internet. If terrorists know where to look, they can find tutorials on the process. Cohen (1990) published a referenced work that gave specific details on the development of malicious software. The focus of the discussion now turns to enforcement.

CONCLUSION

Policing Cyber terrorism is possible for the following reasons. The terrorist planning methodology is understood. Cyber terrorist has a specific methodology in their quest to penetrate a system. The act of penetrating a network is a criminal act and considered a violation of Federal Law. The methods to track down suspects in traditional investigations are not as successfully in cyber terrorism. However, attribution is a possible method to investigate and locate suspects of cyber terrorism. The FBI has the jurisdiction to investigate acts of cyber terrorism. They have partnerships with other federal agencies such as the NSA to obtain information on cyber terrorist. These partnerships extend down to local law enforcement. Therefore, policing cyber terrorism is possible.

AUTHORS INFORMATION

Dr. Phillip Neely is the recipient of the Doctor of Philosophy in Public Policy and Administration from Walden University and the Masters of Science in Public Administration from Central Michigan University. He is an Associate Professor at Saint Leo University in Duluth, Georgia. Dr. Neely's expertise comes in the field of criminal justice and public policy. E-mail: Phillip.neely@saintleo.edu

Michelle Allen is the recipient of the Masters of Science in Criminal Justice, Critical Incident Management from Saint Leo University and the Bachelors of Arts in Sociology from Saint Leo University. She is an Instructor of Criminal Justice at Saint Leo University in Atlanta, Georgia. Instructor Allen's expertise comes in the field of criminal justice and public policy. E-mail: Michelle.allen@saintleo.edu

REFERENCES

18 U.S.C. § 2331 Retrieved from http://www.gpo.gov/fdsys/pkg/USCODE-2011-title18/pdf/USCODE-2011-title18-partI-chap113B-sec2331.pdf

Albanese, J. S., (2013). Criminal Justice 5th Ed Pearson. ISBN:13978-0-13-277034-7

Chien, E (2011). W32.Stuxnet Dossier. Retrieved from http://www.symantec.com/connect/blogs/w32stuxnet-dossier

Cohen, F. B., (1990). A short course on computer viruses. Pittsburg, PA. ISBN: 1-878109-01-4

Ciampa, M. (2009). Security + guide to network security fundamentals (3rd ed). Boston: Course Technology, Cengage Learning

Dean, T. (2010). CIS 175: Network + guide to networks: 2009 custom edition (5th ed). Boston: Course Technology, Cengage Learning

Department of Homeland Security (2009). *National Infrastructure Protection Plan*. Retrieved from http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

Federal Bureau of Investigation (n.d.). Frequently Asked Questions. Retrieved from http://www.fbi.gov/about-us/faqs

Habash, G., (2007). Terrorist Planning Cycle. U. S. Army Training and Doctrine Command. Retrieved from http://www.au.af.mil/au/awc/awcgate/army/guidterr/

Kerrigan, A. (2013) Russian Federation: The Snowden Decision Cornell international Law Journal. Retrieved from: http://webcache.googleusercontent.com/search?q=cache:gBP8UerMZUEJ:cornellilj.org/wp-content/uploads/2013/10/Kerrigan-The-Snowden-Decision.pdf+&cd=1&hl=en&ct=clnk&gl=us

Koh, H. H. (2012). International Law in Cyberspace. U.S. Department of State. Retrieved from http://www.state.gov/s/l/releases/remarks/197924.htm

Lynn, W., J. (2010). *Defending a New Domain*. Retrieved from http://www.defense.gov/home/features/2010/0410_cybersec/lynn-article1.aspx

Miller, B. & Rowe, D. C. (2012). A Survey of SCADA and Critical Infrastructure Incidents. Retrieved from http://www.slideshare.net/fullscreen/daniel_bilar/scada-attack-summary-2-12/6

Mueller, R. S., (2012). RSA Cyber Security Conference. Retrieved from http://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies

National Security Agency (2013). The National Security Agency: Missions, Authorities, Oversight and Partnership. Retrieved from http://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf

Nicholson, A., Janicke, H. & Watson, T. (2013). An Initial Investigation into Attribution in SCADA Systems. Retrieved from http://ewic.bcs.org/content/ConWebDoc/51169

Radack, S. (205). Preventing and handling malware incidents: how to protect information technology systems from malicious code and software. National Institute of Standards and Technology. Retrieved from http://www.itl.nist.gov/lab/bulletns/bltndec05.htm

Shenon, P. (2013). A CRUEL AND SHOCKING ACT. (1ST ed). New York, ISBN: 978-0-8050-9420-6

Snow, G., M. (2011). Statement Before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism. Retrieved from http://www.fbi.gov/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism

Stallings, W. (2009). Business Data Communications. Upper Saddle River New Jersey ISBN: 13: 978-0-558-09810-0

Tafoya, W. L. (2011). Cyber Terror. FBI Law Enforcement Bulletin. Retrieved from http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/november-/cyber-terror

NOTES