Future Towards Danger: The Terror of Cyber Attacks

Kanika Sharma*
Tanvi Bhalla**

Abstract

Cyber terrorism is the use of Internet attacks in terrorist activities, including acts of deliberate, large-scale disruption of computer networks, by the means of tools such as computer viruses [5]. As nation and critical infrastructure become more dependent on computer networks for their operations new vulnerabilities are created.

A hostile group could exploit these vulnerabilities to breach through a poorly secured network and disrupt or even shut down critical functions. All the data is stored on computers in the form of files and is vulnerable to be attacked and thus put ours as well as national security at risk because these files may contain confidential information about our military weapons etc. which if gone into wrong hands may lead to disastrous situations. The terrorists can change or type commands by hacking into a computer which can take over or disrupt the critical infrastructure of entire nation.

This paper covers what is cyber terrorism, what are the cyber attacks held, what the risks are and what preventive measures should be taken to prevent or handle cyber terrorism.

Keywords: Terrorism, SCADA, Denial of service (DoS), Cyber attacks.

Introduction

In today's world, a nation and critical infrastructure has become more dependent on computer networks for their operation. This growing dependency has emerged as a new threat for security which can lead to Cyber Terrorism. With the development of cyber technology, the Internet has become an important channel for terrorists to carry out their activities. Cyber terrorism is the intentional use of computers, internet in terrorist activities to cause destruction and harm for personal objectives. A poorly secured network can easily be penetrated by the hostile nation or group which could disrupt or even shut down critical functions. Many terrorist groups make use of the internet for intra group communications, recruiting people, fund-raising, for creating a feeling of terror in people's minds. They can also steal credit card numbers or valuable data to provide financial support for their operations. There can be devastating situations if the national agencies or government policies information could be breached.

Kanika Sharma*
Management Education & Research Institute
Tanvi Bhalla**
Management Education & Research Institute

Disruption via cyber attacks could be caused to a variety of communication systems including Internet, mobile phones and cables. However, if the nation's security network could be penetrated so easily so, it means that the private sector infrastructures are also vulnerable. Tele-communications networks, electricity power grids, banks could be attacked by cyber terrorists. Such attacks could cause widespread panic and even damage to the country's economy.

Terrorist attacks

(1) The Red team attack-

The first such attack was code named 'Eligible Receiver' was carried out by 35NSA computer hackers known as 'The Red Team'. They can only use software and hacking tools that can be easily downloaded from the Internet. They were authorized to break network but was not allowed to break any US laws. Their main target was the Pacific Command in Hawaii and they were easily able to breach into network and make minor changes in e-mails, disrupt telephone services and conduct denial-of-service attack and the best part was they were able to manage everything without being identified.

(2) Sri Lankan embassy attack-

In 1998, ethnic Tamil guerrillas attempted to disrupt the Sri Lankan embassies by sending large number of e-mail. The Sri Lankan embassy received around 800 e-mails a day for two-week. The messages were "We are the Internet Black Tigers and we're doing this to disrupt your communications". It was characterized as the first known attack by the terrorists.

(3) Attack on U.S. financial institutions-

In March 2013, a pattern of cyber attacks has been reported against U.S. financial institutions by The New York Times. It was believed to be instigated by Iran as well as by incidents affecting South Korean financial institutions.

(4) Attack on media companies-

In August 2013, many media companies like the New York Times, Twitter and the Huffington Post lost control of some of their websites. The hackers were supporting the Syrian government who breached the Australian Internet company that manages many major site addresses.

(5) Virus attack-

In September 2003, the 'Welchia' virus disabled the State Department's consular Lookout and Support system. This system contained records from the FBI department, State department and US immigration.[1]

(6) The attack on Iran nuclear power plant-

In July 2010, "the Stuxnet" computer worm was discovered. It is a windows based worm that spies on and subverts industrial systems. It includes a high specialized malware program that targeted Siemens Supervisory Control and Data Acquisition (SCADA) systems.

It damaged the Iran's nuclear program Siemens SCADA systems. It specifically targeted the centrifuges which are used in the production of nuclear material, making them spin so fast that they get damaged. This attacked has set back the Iranian nuclear power plant for about two years. [7]

Case of Estonia

The Baltic state of Estonia was targeted to a massive denial-of-service attack. The attack consequence was it completely rendered the country offline and the services dependent and Internet connectivity was shut down for three weeks. The infrastructure of Estonia including everything from online banking, mobile phone networks, government services and access to health care information was disabled for a time. The state was technology dependent and was in severe problem.

As a result, for security reasons Estonia joined NATO in 2004. NATO carefully monitored its member state's response to the attack and worried both about escalation and the possibility of cascading effects beyond Estonia's border to other NATO members. In 2008, as a result of the increasing attacks, NATO opened a new center of excellence on cyber defense to conduct research and training on cyber warfare in Tallinn.[5][9]

Types of Cyber Attacks

Different types of cyber terrorism attacks-

1. Incursion-:

   The attacks which are carried out with the purpose of gaining access or penetrating into computer system or network in order to get or modify information. The computer systems and network are very insecure, terrorist take advantage to modify important information which can cause damages to the organization or individual.

2. Destruction-:

   In this method, the attack is used to intrude into computer system and networks with purpose of inflicting severe damage or destroy them. These attacks are very disastrous to an organization as this costs them very heavy to get their operations up and running again.

3. Disinformation-:

   This type of attack spreads fake information that can have severe impact to a particular target. These attacks create uncontrollable situation throughout the nation or in the organization.

4. Denial of Service-:

   The objective of Denial of Service attacks is to disable or disrupt the network by flooding the target server with huge number of packets which ultimately lead the server being unable to handle

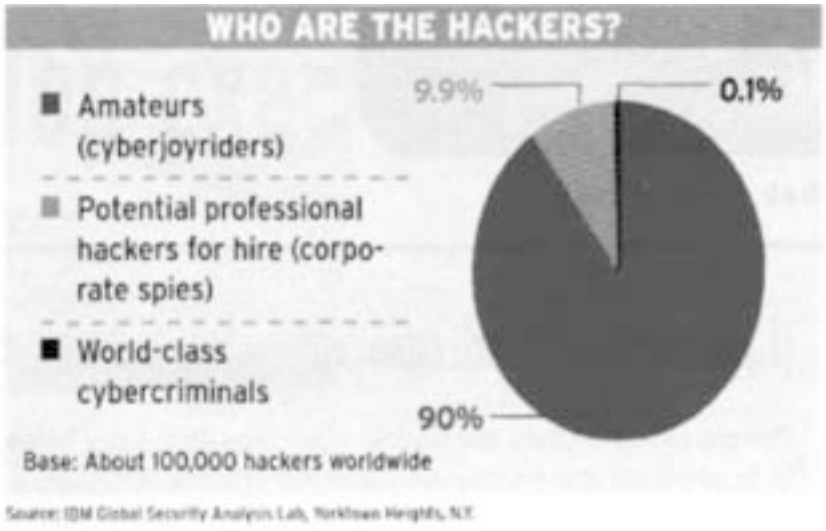

Figure 1. Distribution of cyber hackers

normal service request from legitimate users. This causes organizations to suffer massive loss.

5. Defacement of websites-:

   These attacks focus in defacing the websites of the victims. The website is changed to include cyber terrorist message or to re-direct the users to other websites. [4]

Preventive measures taken by the world

In May 2011, The Chinese Defense Military confirmed that it has an online defense unit known as "Blue Army". It has 30 elite Internet specialists who are engaged in cyber defense operations.

On November 2, 2006, the Secretary of the Air Force announced the creation of the 'Air Force Cyber Command', whose task is to monitor and defend American interest in cyberspace. But later this plan was replaced by the creation of 'Twenty-Fourth Air Force' which became active in August 2009 and is a component of the planned United States Cyber Command.

Another security method is known as 'sniffing'. It is the process of searching social websites, suspected terrorist web pages and even e-mails to detect terrorist activities or threats. A sniffer is a software program which is programmed to search Internet traffic for specific keywords. A sniffer can be authorized or unauthorized. An unauthorized sniffer can be a threat because it can be inserted anywhere without permissions.

The US was one of the first countries that considered cyber terrorism to be a big problem in 2006 in terms of economy and national security.

Cyber Terrorism in India

In March 2013, some Chinese hackers breached the computers of the Defense Research and Development organization, which is India's top most military organization. It was a classical case of cyber war attack. Hackers from Algeria also carried out an attack on websites run by the DRDO, the Prime Minister's Office and various other government departments were attacked by them. A group called 'Pakistan Cyber Army' had also hacked into several Indian websites.

Experts believe that India's cyber security is not enough compatible to combat cyber attacks. Experts say that the country spends a small amount of money on cyber security. The budget allocation towards cyber security was Rs.42.2crore ($7.76 million) for 2012-13. In comparison, the US spends several billion dollars through the National Security Agency, $658 million through the Department of Homeland Security and $93 million through US-CERT in 2013.[4]

Prevention against cyber attacks in India

1. Indian government must collaborate with private sector to create an organization which is developed

mainly to detect and fight against cyber terrorism. Like, in Malaysia they established an International Multilateral Partnership against cyber terrorism (IMPACT), an effort to coax the world's govt.'s into collaboration on cyber security. Some of the major Indian organizations are not a member of IMPACT.

2. Perform required software updates for your operating system and web browser.
3. Install a firewall on your computer.
4. Change your passwords often on a weekly basis. So, that it will be difficult for the hackers to hack the e-mail accounts.
5. Purchase or download any anti-virus software which will detect any virus that can harm your data. It also provides browser security.
6. Install anti-spyware/adware programs onto your system.
7. Delete e-mails from unknown users. [6]

Our recommendation

In this paper we will like to propose our ideas for future implementation.

1. During creation of an e-mail account, generally the e-mail websites provide only 1 question for the recovery of passwords or for authentication. Our idea is that we must provide some 5 uncommon personal questions during account creation. The user must answer to all the 5 questions. Whenever the user login, during sign in, a random question out of the 5 question appears on the screen must be answered by the user. This ensures that the user is the legitimate user. For further security, a message would be send to the user whenever he or she login.
2. To tackle the most common Denial of Service attack we are proposing following methodology-

   DoS is the attack which makes a machine or network resource unavailable to its intended users so they are unable to serve them. To tackle this, every organization or a government department must have a "unique secret code" allotted to them. Whenever the sender sends the packet it must attach the secret code with the header of the outgoing packet. The recipient router must check the header of the incoming packet for the "unique secret code". If the code is present in the header, it indicates that the packet is send from the legitimate user then it is accepted otherwise it is discarded. This prevents Denial of Service attack.

Table 1.

Unique Secret Code	S.A.	D.A.	Data

Where, S.A. is source address and D.A. is destination address

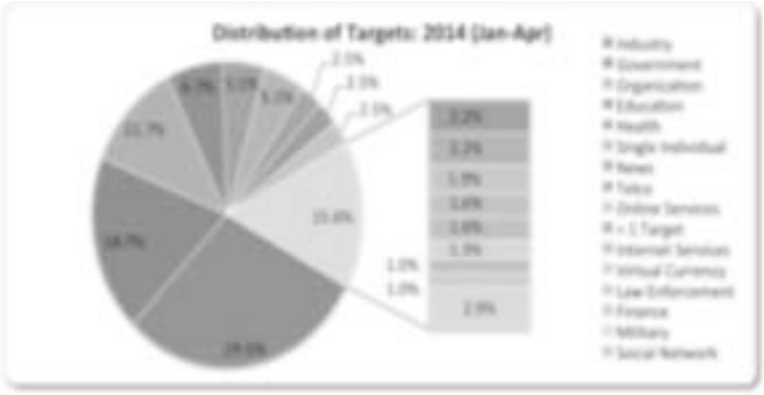

Figure 2. Distribution of Targets

3. The improper and violent data and videos uploaded by the terrorists should not be displayed by sites like you tube etc. The websites should first check the data content that the user is going to upload and if it is violent and can hurt the sentiments of people then that content should be removed. Now-a –days terrorist groups are using social media like face book and twitter to engage and recruit youth into terrorist activities.

Conclusion and Future Scope

Cyber terrorism is increasing day by day. It is very difficult to detect and prevent these attacks. We need to be more attentive and proactive towards cyber security. Legal Policies against Cyber crime have to be established and implemented for nation's security. More cyber laws firms should be engaged in action towards cyber crime. More funds should be raised in this direction to fight against cyber security.

Government and private sector must collaborate with each other to work together as one hand in this direction. They must recruit ethical hackers and professional programmers to combat cyber security. The idea of "unique secret code "should be applied to reduce denial of service attack. We are still further working on this direction so that we can detect and punish cyber terrorist.

References

1. http://cyberterrorismpaper.blogspot.in/
2. http://www.thehindu.com/scitech/technology/towardscyberdefence/article4974205.ece
3. http://gadgets.ndtv.com/internet/news/india-must-wake-up-to-cyber-terrorism-349274
4. Shamsuddin Abdul Jalil , Countering Cyber Terrorism Effectively: Are We Ready To Rumble?, June 2003, GIAC Security Essentials Certification (GSEC) Practical Assignment Version 1.4b Option 1
5. http://en.wikipedia.org/wiki/Cyberterrorism
6. http://www.wikihow.com/Prevent-Hacking
7. By keith Giacobozzi, Cyber terrorism, 27 feb, 2011, http://cyber-terrorismpaper.blogspot.in/
8. http://hackmageddon.com/tag/cyber-crime/
9. http://www.infosecurity magazine.com/magazine-features/cyberterrorism-a-look-into-the-future/