A SURVEY ON CYBER TERRORISM

SHIVA KUMAR K
KNS Institute of Technology
Bangalore
Shivkumark94@gmail.com

ABSTRACT: Cyber terrorism is a major issue by which an individual or group of people use digitalized method to attack physically or attack on any information for their various reasons.

Recent years have seen a rapid growth in the target through cyber terrorism. Computing technology is available to the whole world. The openly available computing resources are one of the major reasons for the increase in cyber terrorism. Though the severity of the attack of terrorists depends on the situation, the countries from developing to developed in their economy are a part of the issue

Political, social and .economic changes are the motivations present in real-world terrorism. Unless steps are taken to significantly reduce the risks disaster in inevitable. Even with the best risk reduction, there are still likely to be problems. This paper brings some important issues regarding the effect of cyber terrorism.

INDEX TERMS: spoofing, hacking, vulnerabilities, phlooding.

1. INTRODUCTION

Cyber terrorism is any act of terrorism that uses information or digital technology (computer networks) as either an instrument or a target. Even the limited cyber infringement actions can disrupt the whole computer world. Cyber terrorism refers to unlawful attacks and threats of attacks against computers.

Cyber terrorism may not be a cyber-war, it can include cyber espionage. It is a back door access to information stored in digital systems. It is possible for a person to read all about a given cause and chat with proponents of the without ever leaving the safety of his or her own home. New recruits can thus become affiliated with a terrorist group, Commit to carrying out given actions, all without ever actually coming into contact with another human being.

2. WHAT THE CYBER TERRORIST CAN DO?

Terrorist groups engaging in cyber terrorism are noted for threats to commerce, public safety and national security. These threats can take any number of forms, but are generally with the computer technology against victim's computer resources.

The cyber terrorist could target the computers and computer networks of governments, individual, public utilities, private airlines and so forth. The sheer number and complexity of potential targets guarantee that terrorists can find weakness and vulnerabilities to exploit. Several studies have shown that critical infrastructures, such as electric power grids and emergency services, are vulnerable to cyber terrorist attack because the in fractures and the computer systems that run them are highly complex, making it effectively impossible to eliminate all weaknesses.

Cyber terrorists could involve destroying the actual machinery of the information infrastructure; remotely disrupting the information technology underlying the internet, government computer networks, or critical civilian systems such as financial networks or mass media.

The more general attack of cyber terrorists could be "spam" mails. These mails are sent with the viruses that cause the loss of security to the information stored on computer. Thus through sending spam mails cyber terrorists can directly attack on your information on computer. In the likely form phishing mails have taken an advanced form of spamming in which victims are forced to divulge private information like account numbers of their bank.

3. WHAT ARE THE TYPES OF CYBER TERROR TECHNIQUES?

- HACKING:
  Hacking is the abrupt way of bypassing the security systems of computer network.
- IP SPOOFING:
  An IP (internet protocol) spoofing occurs when an attacker outside the network enters pretending as if he is inside network and takes all information from network or destroying information. It could be password attacks, distribution of sensitive internal information to external sources.
- INTERNET WORMS OR VIRUSES:
  Cyber terrorists can inject victims systems with "viruses" or "worms" that can be used to shut down programs or even entire systems by hijacking email lists and address books.
- PHLOODING:

This new exploit targets businesses central authentication servers with the goal of overloading them and causing denial-of-service attacks. These simultaneous but geographically distributed attacks have targeted but are not restricted to wireless access points with login requests using multiple password combinations in what are known as dictionary attacks.

The multiple requests create a flood of authentication requests to the company's authentication server, which could slow down logins and potentially interface with broader network operations, since many different users and applications often validate themselves against the same identity management system. Phlooding could effectively block broadband VPN or firewall connections making it temporarily impossible for employees to access their corporate network.

- POCKET SNIFFERS:
  It is a package softer by which any sensitive information like accounts and passwords can be captured across a local area network.

4. WHAT MAKES CYBER TERRORIST'S MOTIVATED?

The aspects behind the act of cyber-crime may be several. The people who motivate intruders for the act of cyber threats should be punished and suitable legal actions has to be taken in order to ensure the cyber terrorist deviate from the thought to be a terror.

- PERSONAL FINANCIAL GAIN:
  In order to attain financial growth, an individual may be involved in a cyber-crime. The people who want to attain financial growth can involve in cyber threats like blackmail through internet and divert valuable assets.
- REVENGE:
  This could be a personal issue related to the intruder and the terrorist. Example for this kind of act is potentially disgruntled employee.
- CURIOSITY AND THRILL SEEKING:
  This can be a non-malicious hacker, how does it work reasons. This kind of terrorists may be aware that actions are illegal and punishable.
- POLITICAL AND ECONOMIC INTELLIGENCE:
  This kind of terrorists may want to gain information on individuals, obtain research and other valuable technical information that would be too expensive to develop by oneself or in failing economies.
- MILITARY AND NATIONAL INTELLIGENCE:
  National disputes or national competition may be the reason on any way of the cyber-crime act.
  The severity of this reason always impacts on larger destroy to the security systems.
- IGNORANCE:
  Intruders may be unaware that actions are illegal and punishable.

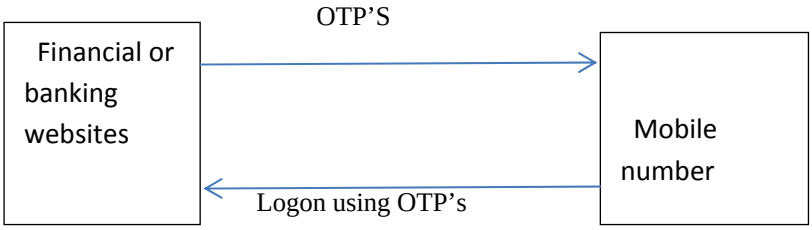
5. WHAT COULD BE DONE TO AVOID CYBER TERRORISM?

There are many ways by which an individual can overcome the act of cyber terrorism:

- By not responding to any of the spam mails especially mails which come with fake lottery information's
- .By not providing any personal details in any of their social networking sites unauthorized access to any network has to be denied by cyber systems by knowing the network they are accessing.
- A cyber security board has to be established in order to ensure security towards cyber terrorism, in every part of the country. A board through which faster actions has to be taken to any cyber-crime complaints.
- Government can use their coercive capacity to make terrorism too costly for those who seek to use it. This could be made military strikes against terror bases.
- Information assurance which means providing right information to the right people at the right time .
- Raise awareness among people about the risks that involve in the act of cyber-crime and misleading the information.
- Create a general frame of references that will help individuals understand security issues and respect ethical values in the development and implementation of coherent policies, practices, measures and procedures for the security of information systems and networks.
- Recognizing the interconnectivity of information systems and networks and the potential for rapid and widespread damage, participants should address security incidents and share information about threats and vulnerabilities and implement procedures for rapid and effective cooperation to prevent ,detect and respond to security incidents
- Legal safeguards can act as deterrent to attackers and therefore can be considered as a safeguard. Certain data protection rights accrue to those who use computer systems and one who violates these rights may be subjected to civil and perhaps criminal proceedings.

6. METHODOLOGY

People who use online banking or any other financial related websites to access, a better way to implement the security is by the use of OTP's (one time passwords). By which a single use password is sent to their provided mobile number to log on to the websites to access the information or to provide any details.



But the process is time consuming and leads to complexity in case of any disturbance to access .

7. CONCLUSION

Computers can play enormous role in terrorism. At the same time they can provide perhaps our biggest defense against terrorism if used to our advantage. However, just like as we need to understand the integration of computers with terrorism, we must examine how computers can assist in defense broadly. This begins with the reexamination of cyber terrorism which must take place at all levels of any institution or organization to ensure security system.

Information at each levelof analysis must be shared, collated, and redistributed across federal, state and local government boundaries, as well as amongst industry and academia, and in some cases, the private citizenry.

Aside from the role of computers in defense, we must attempt to re-educate the policy makers, defusing the latent danger of vertical cyber terrorism defenses and replacing them with a well-rounded, integrated approach to a problem that is extremely broad.

The lack of understanding of cyber terrorism and overall insecurity among computer users has allowed a situation to develop which is not in the best interest of the country or computer users.

8. REFRENCES

[1] A summery on cyber terrorism. www.itworld.com
[2] Terrorism Questions and Answers, Council on Foreign Relations, http://www.terrorismanswers.org/terrorism/cyberterrorism.html
[3] Data Interchange Standards Association-Test conditions and Results from when the workgroups test transactions proposed for HIPAA
www.disa.org
[4] http://netsecurity.about.com/cs/cyberterrorism/
[5] http://www.itworld.com/security/255094/cyberterrorism-threat-shouldnt-be-underestimated-some-security-experts-say
[6] http://www.cfr.org/homeland-security/targets-terrorism-information-infrastructure/p10212