ISSN: 2321-7782 (Online)

Volume 3, Issue 9, September 2015

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Cyber Terrorism

Neeru Ahuja
Sirsa, India

Abstract: Internet technology has grown enormously. It is really a matter of pride but there is another side of coin that is causing serious concern is the rapid raise in cyber terrorism. Cyber terrorism is also known as 'Electronic terrorism' or 'Information war' or 'Cyber war'. It is criminal activity who uses computer technology and internet, especially to cause fear and distruption. This paper attempts to brief cyber terrorism and also highlights sophistication of cyber terrorism. It also include major tools of cyber terrorism which reported as viruses, spyware, worms, Trojan etc. Last but not least it not precautious measures to combat cyber terrorism.

Keywords: Cyber terrorism, Internet, Stalking, Data, Information.

I. Introduction

The internet has revolutionized the computer and communication world like nothing before. The internet today is widespread information infrastructure. Internet technology refers to the creation , gathering ,processing, storage, presentation of information and also the processes and devices that enable all this to be done. It is affecting us as individual and as society. It has exposed the user to have data bank of information. But this is only one facet of information technology, today the other facets are challenges for whole world like cyber terrorism. Today computer play important role in every cyber terrorist activity. There is a lot of misinterpretation in the definition cyber –terrorism .Here cyber is common word and terrorism is difficult to define. The word cyber terrorism is used because terrorist use technology as a weapon. A simple definition would be "unlawful attacks against computer network"

Tomorrow terrorist may be able to do more damage with a keyboard than a bomb-National research council.

Cyber terrorism means intentional use of computer network tools to harm or shut sown critical national infrastructure1.

II. Sophistication of Cyber Terrorism

1. *Simple-Unstructured*: The capability to conduct basic hacks against individual systems using tools created by someone else. The organization possesses little target analysis, command and control, or learning capability.

2. *Advanced-Structured*: The capability to conduct more sophisticated attacks against multiple systems or networks and possibly, to modify or create basic hacking tools. The organization possesses an elementary target analysis, command and control, and learning capability.

3. *Complex-Coordinated*: The capability for a coordinated attack capable of causing mass-disruption against integrated, heterogeneous defenses (including cryptography). Ability to create sophisticated hacking tools. Highly capable target analysis, command and control, and organization learning capability

III. Tools Of Cyber Terrorism

1.*Viruses/Worms* :Infections are projects that connect themselves to a PC or a record and afterward circle themselves to different documents and to different PCs on a system. They more often than not influence the information on a PC, either by changing or erasing it. Worms, not at all like infections needn't bother with the host to join themselves to. They only make useful duplicates of themselves and do this more than once till they gobble up all the accessible space on a PC's memory.

2.*Cyber Stalking*: Digital stalking includes a man taking after a man's development over the web by posting message on release bord frequented by casualty ,entering the visit room frequented by casualties, continually assaulting the casualty with messages and so on.

3.*Email spoofing*: A parodied email is one that seems to start from one source however really has been sent from another source. e.g. Rama has an email address rama@yahoo.org. His adversary, Ravana parodies his email and sends disgusting messages to every one of her colleagues. Since the messages seem to have begun from Rama, his companions could take offense and connections could be ruined forever.

4.*Denail of service Network* : This includes flooding a PC asset with a greater number of solicitations than it can deal with. This causes the asset (e.g. a web server) to crash consequently denying approved clients the administration offered by the asset. Another variety to a regular disavowal of administration assault is known as a Distributed Denial of Service (DDoS) assault wherein the culprits are numerous and are geologically across the board. It is extremely hard to control such assaults. The assault is started by sending over the top requests to the casualty's computer(s), surpassing the farthest point that the casualty's servers can bolster and making the server's accident.

5.*Phishing* : Phishing is a demonstration of sending an email to client erroneously asserting to be a set up authentic business trying to trick the client into surrendering private data that will be utilized for character theft.The email guides the client to visit a site where he or she is requested that overhaul individual data, for example, passwords and Mastercard, standardized savings, and financial balance numbers, that the true blue association as of now has issued. The Web website, be that as it may, is false and set up just to take the client's data.

6.*Cyber defamation*: Digital maligning is only criticism happens with the assistance of PCs as well as the Internet. e.g. somebody distributes defamatory matter about somebody on a site or sends messages containing defamatory data to the greater part of that individual's companions.

7.*Web jacking*: Compelling cracking so as to take of the control of a site the secret word, is termed as 'web jacking'. For this situation, genuine proprietor of the site does not have any more control over what shows up on that site.

IV. Prevention Of Cyber Terrorism

“Prevention is better than cure” is not only meant for human health but for computers as well. It is always better to take necessary steps to prevent cyber crimes. The following are some of the useful tips to prevent cyber terrorism to some extent.

Dos

» Ensure using a security program that gives you controls over cookies that send information back to Web sites.

» If your Web site serves up dynamic content from a database, consider putting that database behind a second interface on your firewall, with tighter access rules than the interface to your server.

» Make sure web servers running your public site are physically separate and individually protected from your internal corporate network.

» Put in a firewall and develop your content off line.

» Send credit card information only to secure web sites

» Thoroughly check out the site you are doing business regularly.

- Use the latest anti-virus software, operating systems, Web browsers and email programs

DON'T

- Allow your children to download files or software without your permission
- Allow your children to have face-to-face meetings or send their photographs online
- Forget to protect your databases.
- Forget to put in a firewall and develop your content off line.
- Let all cookies in without monitoring them
- Send credit card information to unknown sites
- Share your password with other people
- Use obsolete / pirated anti-virus software, operating systems, Web browsers and email programs.
- Post / host inappropriate content
- Respond to inappropriate messages or emails

V. CONCLUSION

Cyber terrorism are slowly evolving from simple e-mail crime to more serious crimes. It is a known fact that given the unrestricted number of free Web sites, the Internet is undeniably open to exploitation. The problem is that people are not aware about cyber terrorism and lack of knowledge about cyber security. The IT Act 2000 was undoubtedly a welcome step at a time when there was no legislation on this specialized field. Therefore proper measure should be implemented to aware people about the variety of cyber crimes taking place across the globe and they should be prepared to combat such crimes.

References

1. Gabriel(2005) :Cyber Terrorism :The sum of all fears ?
2. Raghav: Cyber security in india's counter terrorism strategy
3. Cyber Crimes and Real World Society by Lalitha Sridhar.
4. www.legalserviceindia.com/cyber-crimes.
5. www.crime-research.org/library/cyber-terrorism