Impact Factor (SJIF): 4.542

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 4, Issue 3, March-2017

SCENARIO OF CYBER OFFENCES IN INDIA

Madhuri K. Shah[1], Chandresh D. Parekh[2]

[1]Cyber Security Department, Raksha-Shakti university
[2]Assistant Professor Telecommunication,
Raksha Shakti University, Ahmedabad

ABSTRACT

This paper explores the increasing number of cybercrime cases in India and examines the demographic characteristics of criminal activity. The paper is based upon data taken from the CERT, computer Emergency Response Team of India and data portal of Indian Government mainly. The paper defines cybercrime, analyses of cyber crime statistics and examines recent trend of India.one of the biggest challenges the world faces is that of cyber security. Cyber security capability building is a rising phenomenon globally and India is no exception in this. Cyber security is a complex issue, affecting many application domains and straddling many disciplines and fields. Securing the critical infrastructures requires protecting not only the physical systems but, just as important, the cyber portions of the systems on which they rely. This survey paper focuses on threats and attacks which have been seen in India that it will be helpful to the researcher to make more secure India and digitally strengthen India.

Key Words: Cyber security, cyber-crime, Cyber challenges

INTRODUCTION

Computer crime or cyber-crime refers to any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Cyber Crime is criminal activity done using computers and the Internet. This includes anything from downloading illegal music files to stealing millions of dollars. cyber Crime also includes non-monetary offences, such as creating and distributing viruses on other computers or posting confidential business information on the internet. The computer may however be a target for unlawful acts in the following cases unauthorized access to computer/ computer system/ computer networks, theft of information contained in electronic form, e-mail bombing, data diddling, salami attacks, logic bombs, Trojan attacks, internet time thefts, web jacking, theft of computer system, physically damaging the computer system. Cyber threat landscape is expanding enormously in the cyberspace

Cyber Security – A National need?

Cyber-attacks by hostile organizations, nations and criminals are on the rise, along with increase in cases of threat to governments, businesses and individuals by attempting to extract technical, financial, and national security information.

Security Incident	2015
Network Scanning/probing	3673
Virus/Malicious Code	9830
Website defacement	26244
Website Intrusion & Malware Propagation	961
Tampering with source code	15
obscenity	114
Others	8213

Recorded Cyber Crime in CERT

Cyber Challenges

Today's cyber criminals are increasingly adroit at gaining undetected access and maintaining a persistent, low-profile, long-term presence in IT environments.as the crime numbers are increasing types like network scanning/probing, virus/malicious code, website defacement, website intrusion & malware propagation tampering with source code, obscenity and many others are rising as we can see in above table. Meanwhile, many organizations may be leaving themselves vulnerable to cybercrime based on a false sense of security. Cyber criminals are generally computer professionals or computer-literate persons and are not history sheeters and mostly without previous criminal record Backbone of cyber criminals the underground black market supported by exploit kits, packaged malware and hacks is expected to continue and evolve citing tried-and-true crime ware like Black Hole, ransomware, which have been improved and refined in ways that shows the extent of professionalism and methodology for developing malwares. Cyber attackers can disrupt critical infrastructures such as financial and Government systems, producing effects that are similar to terrorist attacks in the physical space. They can also carry out identity theft and financial fraud; steal corporate information such as intellectual property; conduct espionage to steal state and military secrets; and recruit criminals and others to carry out physical terrorist activities. What makes cyberspace even more attractive to criminals including non-state actors is that attribution in cyberspace is difficult, especially given that cyberspace is borderless and cuts across jurisdictions. It allows criminals to launch attacks remotely from anywhere in the world. With this growing threat landscape, cyber-readiness of the security systems has been constantly put to test. The primary objectives for securing country's cyber space are minimize damage and recovery time from cyberattacks. Preventing cyber-attacks against the country's critical infrastructures reduce national vulnerability to cyber-attacks. actions to secure cyber space include-Forensics and attack attribution. Protection of networks and systems critical to national security early watch and warnings protection against organized attacks capable of inflicting debilitating damage to the economy research and technology development that will enable the critical infrastructure organizations to secure their IT assets.In that first step of all is to understand their attack types and trends what they do follows.Cyber Crime Includes following are the few examples of cyber-crime:

1. Cyber stalking*:* Online harassment and online abuse all comes under stalking. It generally involves harassing ort hreatening behavior that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property.Cyber stalking shares important characteristics with offline stalking; many stalkers (online or off) are motivated by a desire to control their victims. A major damaging effect of online abuse is victim avoiding his/her friends,family and social activities

2. **Intellectual Property Crimes*:*** Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offence. The common form of IPR violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code,etc.

3.**Bot Networks*:*** The word botnet made from the two words robot and network. A cyber-crime called 'Bot Networks', when hackers remotely take control upon computers by using malware software. Computers can be co-opted into a botnet when they execute malicious software. A botnet's originator can control the group remotely.

4. Transmitting Virus*:* Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. worm attacks plays major role in affecting the computerize system of the individuals.

5. **Hacking*:*** In general words hacking means seeking and exploiting weakness and security of a computer system or a computer network for unauthorized access. The person who do hacking is known as hacker. Hacker use computer expertise and some tool or scripts to hack any computer system.

6. Internet Time Thefts*:* Basically, Internet time theft comes under hacking. It is the use by an unauthorized person, of the Internet hours paid for by another person. The person who gets access to someone else’s ISPuser ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person’s knowledge.

7. Cracking*:* It is a dreadful feeling to know that a stranger has broken into user computer systems without user’s knowledge and consent and has tampered with precious confidential data and information. Cracker are differ with hacker because hacker are hired by companies to audit network security or test software but cracker do same work for their own profit or to harm others.

8. Phishing*:* Phishing means acquire information such as usernames, passwords, credit card details,personal details by electronic communication. Phishing commonly uses fake emails or fake messages which contain link of virus/ malware infected fake websites.These website request user to enter their personal detail.

9. Voice Phishing*:* The term is a combination of "voice" and phishing. Voice phishing is use to gain access of private, personal and financial information from the public. Voice phishing uses a landline telephone call to get information.

10. Carding: It means false ATM cards i.e. Debit and Credit cards used by criminals for their monetary benefits through withdrawing money from the victim's bank account.

11. **E-Mail/SMS Spoofing*:*** A spoofed E-mail/ SMS may be said to be one, which misrepresents its origin. It shows it's origin to be different from which actually it originates. Here an offender steals identity of another in the form of email address, mobile phone number etc and send message via internet.

12. Cross-site Scripting*:* Cross-site scripting (XSS) is a type of computer security vulnerability. By cross-site scripting attacker can bypass the predefine access permissions of website. Reflected XSS is the most frequent type of XSS attack. reflected XSS attack is also known as non-persistent XSS. Scripting languages like java script, VBScript etc are use for reflected XSS attack.

13. Cyber Squatting*:* Squatting is the act of occupying an abandoned or unoccupied space. Cyber-squatting is the act of registering a famous domain name and then selling it to needy in high cost. It means where two persons claim for the same Domain Name either by claiming that they had registered the name first on by right of using it before the other or using something similar to that previously.

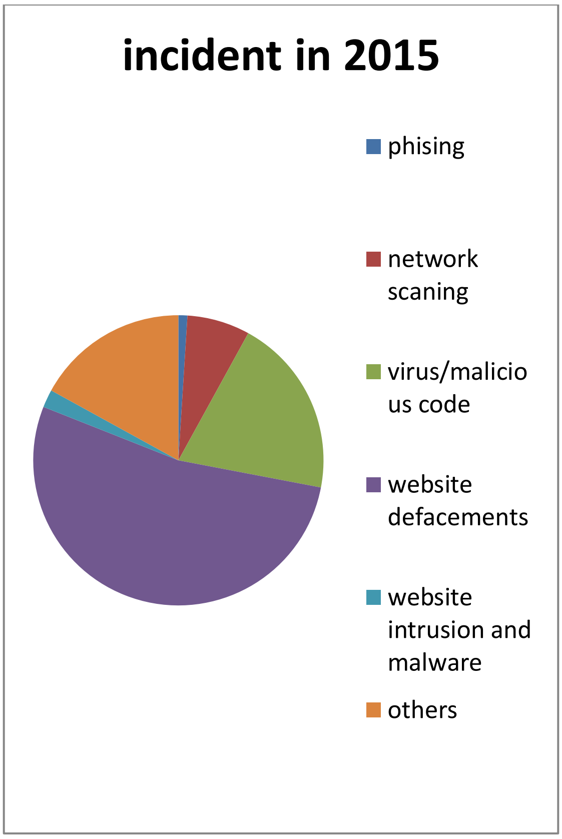
14. Child Pornography*:* It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children. Child pornography is divided into simulated direct involvement of the child (also known as child abuse images).

15. **Cyber Vandalism*:*** Vandalism means destroying or damaging property of another. Thus cyber vandalism means destroying or damaging the data when a network service is stopped or disrupted.

16. Cyber Trespass*:* It means to access someone's computer without the right authorization of the owner and does not disturb, alter, misuse, or damage data or system by using wireless internet connection.

17. Cyber Trafficking*:* It may be trafficking in drugs, human beings, arms weapons etc. which affects large number of persons. trafficking in the cyberspace is also a gravest crime.

18.Cyber-crime & Social Networking*:* Cyber criminals use social media not only to commit crime online, but also for carrying out real world crime owing to "over-sharing" across these social platforms**.** The risk associated with our identities. Identity theft can happen to anyone who exposes too much personal information online on various social networking sites. Get to know the security and privacy settings, and configure them to protect from identity theft. One in five online adults (21percent) has reported of becoming a victim of either social or mobile cyber-crime and 39 percent of social network users have been victims of profile hacking, scam or fake link.

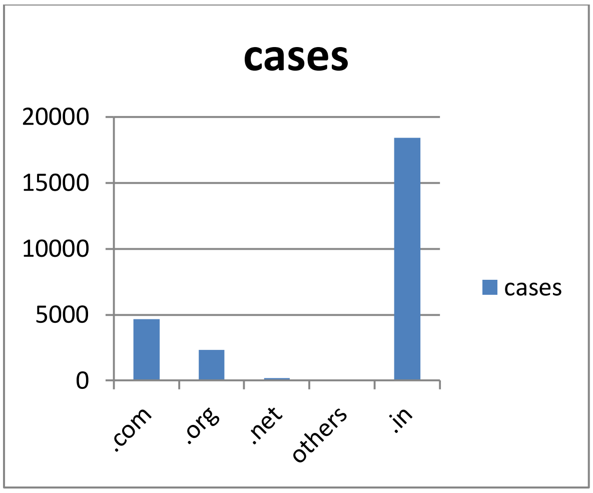


where world is going forward in being smart for cyber security it is necessary to check that where India stands. Which we can get idea from the graph of attacks done in India and mere digits the specialist for cyber security in India.

China, Cyber Specialist: 1,25,0000
US, Cyber Specialist : 91080
India, Cyber Specialist : 556
(CERN technical team :75)

State	Cases registered under cyber crime 2015	Persons arrested under cyber crime 2015
Andhra Pradesh	536	346
Arunachal Pradesh	6	4
Assam	483	457
Bihar	1567	242
Chhattisgarh	103	99
Delhi	177	53
Goa	17	8
Gujarat	242	272
Haryana	349	205
Himachal Pradesh	50	38
Jammu and Kashmir	34	12
Jharkhand	180	172
Karnataka	1447	293
Kerala	290	191
Madhya Pradesh	231	230
Maharashtra	2195	825
Manipur	6	1
Meghalaya	56	20
Mizoram	18	18
Nagaland	1	1
Odisha	386	110
Punjab	149	136
Rajasthan	949	295
Sikkim	1	1
Tamil Nadu	142	125
Telangana	687	430
Tripura	13	8
Uttar Pradesh	2203	1699
Uttarakhand	48	23
West bengal	398	287

State vise Recorded data of Cyber Crime
2015-16



Domain break up 2015-16

Conclusion

This paper represents different types of the Cyber-attacks in India with analysis of its types. There are a are so much cyber-attacks in each and every states of India and domain ".in" is largely attacked by attacker although it represents Governments sites mostly while comparing with others domain. Moreover there are so many cases of phising and regarding malicious code recorded in India during recent time. Data of cases registered and persons arrested shows the otiose progress in Cyber world. Data analysis will help researcher and developers to make a secure Digital India with these bifurcated data of India and can help to understand the trend of cyber offences in India.

Refernces

[1] http://www.cert-in.org.in/

[2]https://data.gov.in/catalog/persons-arrested-under-cyber-crime

[3] https://data.gov.in/catalog/cases-registered-under-it-act-cyber-crime

[4]http://www.ijcns.com/pdf/ijpcscvol4no22012-1.pdf

[5]http://computerera.co.in/it-minister-ravi-shankar-prasad-revealed-cyber-crime-statistics-in-india/

[6]https://factly.in/cyber-crimes-in-india-which-state-tops-the-chart/

[7]http://ptlb.in/csrdci/wp-content/uploads/2013/12/Cyber-Security-Trends-And-Developments-In-India-2013.pdf

[8]http://mha1.nic.in/par2013/par2016-pdfs/ls-010316/830.pdf

[9]http://rtinagpur.cag.gov.in/uploads/CaseStudies/CaseStudiesonCyberCrimesNOTSENT/CaseStudiesonCyberCrimes.pdf

[10]https://internetdemocracy.in/reports/cybersecurity-ig-ifp-saikat-datta/

[11]https://academic.oup.com/cybersecurity/article/doi/10.1093/cybsec/tyw001/2525524/Examining-the-costs-and-causes-of-cyber-incidents