Spectrum of Cyber Threats and Attack Trends in Indian Scenario

Narinder Singh Rana, S. N. Panda

Abstract*— With the growth of Internet in the country the dependence of the Indian economy on ICT (Information and Communication Technology) has increased tremendously in last couple of decades, and corresponding has been growth of cyber incidents in the country. In the wake of increasing cyber incidents in India, Indian Computer Emergency Response Team (CERT-In) was constituted by government of India in 2004. In this paper the authors have studied the scope and scale of cyber incidents happening in the country. Website defacement being the most visible part of a cyber incident, have been used to study the trend of cyber attacks in India. Analysis has also been done regarding the various types of domain that have been attacked and the motivation behind these attacks, other common attacks and their growth trends have also been studied with the help of CERT-In data.

Index Terms*— CERT-In, Cyber Incident, Security, Website Defacement.

I. INTRODUCTION

The dependence of the Indian economy on the ICT has increased tremendously in last couple of decades, every business and individual is now wired to the Internet. This has definitely helped the Indian economy to grow at a fast pace but, as with any boon comes a bane, ICT also has caused unprecedented challenges and cyber attacks on the organizations using it for their day to business activities. In the initial years of the Internet boom the developed western economies like US and Europe were front runner in use of ICT and were facing threats from their cyber adversaries but during the last couple of decades the developing countries like India, Brazil, South Africa etc have seen higher growth rate of Internet penetration then their western counterpart and even these countries are striving hard to defend themselves from the cyber attacks.

Many security organizations were setup in the US and Europe to defend against the cyber adversaries, some of the most prominent once are CERT (Computer Emergency Response Team), SANS (Sysadmin, Audit, Network, Security), CIS (Center for Internet Security), ISC (Internet Strom Center) etc. Now similar cyber attacks have been taking place since many years in India and are affecting government, industrial, educational, and social organizations across the country and hence there was a need for similar security organizations in India.

Manuscript Received on March 2015.

Narinder Singh Rana, Research Scholar, Punjab Technical University, Jalandhar, Punjab, India.

Dr. S. N. Panad, Professor, RIMT-Regional Institute of Mgt & Tech., Mandi Gobindgarh, Punjab, India.

In response to this growth of Internet and associated vulnerabilities and cyber attacks in the Indian cyber space, Department of Information Technology, Ministry of Communication and Information Technology, Government of India constituted CERT-In in 2004. The primary task of CERT-In includes prevention and response to the cases of cyber incidents, analysis and dissemination of cyber attacks and associated vulnerabilities, issue advisories regarding the cyber incidents and train the network security professionals within the country and equip them with the technical expertise to handle the cyber incidents individually and collaboratively.

In this paper the author have analyzed the data from CERT-In to find the trend of cyber incidents in the Indian cyber space. The growth trend of cyber incidents in the country and around the world has constantly been positive, although the number of incidents reported to CERT-In were very low in first couple of years, primarily because of lack of awareness among the CISOs and network professionals, but now huge number of incidents are being reported regularly to the CERT-In centre.

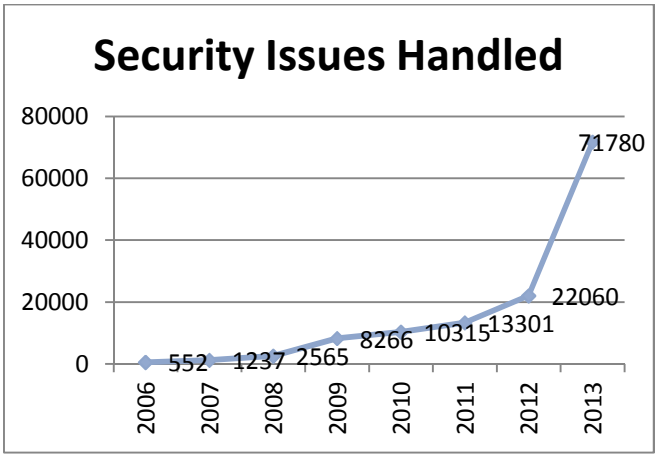
The authors have extrapolated the past data to predict the future of cyber incidents that might affect the Indian organizations in coming years. The data is also analysed from the perspective of a different types of Indian websites that have been attacked in last 8 years and the type and growth trend of various types of cyber attacks happening in India on these various organizational websites.

II. GROWTH TREND OF CYBER INCIDENTS

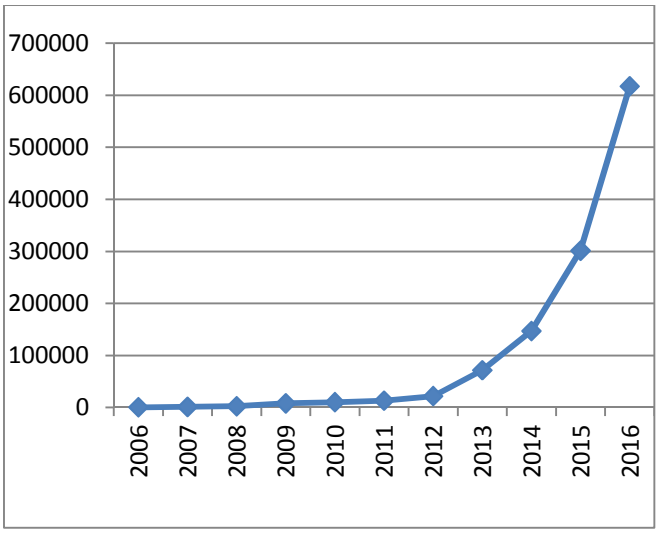
It is a well known fact that all sort of governments and increasing number of industrial and social organization face the cyber incidents across the world. As the cyber attacks are mostly anonymous and the sophisticated attacks are very difficult to be tracked by individual or even large organizations, so they often rely on some centralized agency or network security provider to respond, mitigate the effect, and prevent the reoccurrence of the attack against the organizational infrastructure or websites. The cyber attacks today are not random hack by some script kiddie rather they are strategic effort by government, industrial or even a terrorist organization to affect the economy, security, reputation of a country or organization against which the attack is launched. A disgruntled employee today does not even need to hone the computer skills to avenge the employer as the botnets today are available on rent to launch the DDoS attacks. The cyber crime enterprises are providing customised service to its clients to launch attack against any organization or individual and are openly advertising it on the web [1]. In India the CERT-In was established as the primary organization to handle the cases of cyber espionage and cyber

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

incidents. Although the data regarding the cyber incidents handed by them is available since January 2004, the data from 2006 onwards has been used to analyse the trend of cyber incidents handled in India. Exhibit 1(a) shows the graph of the actual incidents reported to and handled by CERT-In, 1(b) shows the predicted value of cyber incidents for next three years.



(a)



(b)

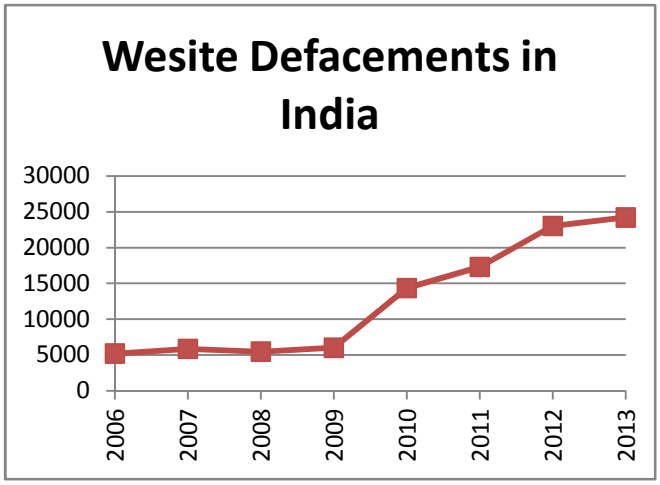
Exhibit 1
(Number of security issues handled by CER-In annually)

As the number of incidents handled did not follow a linear model so CAGR (Compounded Annual Growth Rate) has been used to predict the future incidents. The value of CAGR is 2.05, which shows that on an average the number of incidents are doubling annually. The level of awareness about cyber security and the associated threats and the monitoring of the ICT infrastructure is still very limited in India, especially the SMEs (Small and Medium Enterprises) rarely employ enough resources and technology to defend their infrastructure and consequently sometimes, the less obvious attacks are not noticed by them otherwise the numbers of security issues handled by security organizations in India would have been much higher. The situation is expected to change in future as more and more organization are now using IT security standards and frameworks and are employing penetration testers to test the robustness of their ICT infrastructure and are also willing to share this information with the security practitioners in order to fight the cyber miscreants collectively. With CERT-In slowly becoming the trusted source of analysis and defence against the cyber security incidents in India their activity is bound to increase in future.

III. INDIAN WEBSITES UNDER CONSTANT ATTACKS

The cyber attacks earlier were the manifestation of expertise by the hackers who used to hack the website of big organization just to prove that they were invincible, now the hackers are attacking the ICT infrastructure with intent to steal confidential data and sell it in the underground economy and make quick money. The method of the attacks have become much more sophisticated, and mostly the attacker would hide the tracks and often install a back door so that he can gain access to the system again without the unsuspecting target ever realizing that he was attacked. In such a situation the most obviously visible attack is the defacement of the organizational website buy posting unethical or unscrupulous images or content on the website with an intent to harm the reputation of the organization.

During the review of literature it has been observed that globally website defacement is one type of attack which is most promptly reported by the attacked organization or individual as there is no point of hiding the attack as it is already visible to the visitors of the websites. Therefore the authors have analyzed the growth trend of website defacement attacks reported to CERT-In to predict the future growth pattern of the attacks that are likely to happen in India. Exhibit 2 shows the actual attack pattern of website defacements for eight years since 2006.



It is common for an attacker to compromise websites to facilitate other cyber attacks. The compromises are often not noticed by the end users, but they are a big security threat to anyone visiting the website, and obviously to the organization whose website has been compromised. For example, an attacker may infect a website with some Trojan horse code, which would download and install automatically when the user visits a website page, this Trojan might record keystrokes on the user's computer and send it to its command and control centre. The attacker can then extract the confidential information such as user name and passwords, card numbers, passwords for email and financial accounts etc, from the data. It is the responsibility of the organization to keep the website clean of such malwares, however all

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

organizations are not equipped with the technical expertise to keep their websites protected from these kind of cyber attacks. During the analysis it was found that the maximum number of defacement of the Indian websites have been done by anonymous group called "AIC (Anti India Crew)", followed by "Silver Lords" and "GForce Pakistan" groups which have caused second and third highest number of defacement to the Indian websites[2]. Out of total website defacements of Indian organization almost 53% defacements were done by these three groups and rest 133 such anonymous groups were responsible for rest of the 47% website defacement in the country. It is quite evident from the above statistics that certain groups are specifically targeting Indian websites but attribution is difficult. The organizations may think that an attack may have come from some particular geographical location but actually the attack may not be from that geographical location as command and control centre of botnets are mostly located far from the bots which are actually used to execute such cyber attacks.

IV. Attacked Domain Statistics

As a major number of website defacement were done by a selected group, so the data has been further analysed to see what kind of domains are being targeted the most. For all instances of website defacement the data for four different domains have been consistently tracked since 2006 these are .com, .in, .org and .net, data for some other domains such as .edu, .info have been tracked in some years when the number of defacement of these types of website was large, but for the purpose of analysis all other domains have been considered as "others". As expected, the maximum number of the website defacement attacks targeted the Indian website which had the country specific domain .in, the second most attacked domain was the .com domain as this domain correspond to the commercial organizations and the miscreant tend to extort money and gain financial mileage by attacking these websites. These two domains were targeted in more than 91% website defacements incidents and rest all other domains including .net, .org and others constituted for remaining 9% of cases. The Exhibit 3 below shows graphically the number of attack against these domains as reported to CERT-In in last eight years since 2006.

The largest number of .in websites being targeted by the miscreants is definitely a specific attack on the Indian cyber infrastructure by the adversaries to malign the reputation and hinder the growth of the Indian economy by attacking various e-commerce and other social and government interaction websites. Numerous attacks on .com websites might be because a competitor might be seeking competitive advantage through theft of intellectual property. In some instances the competitor might want to malign the reputation of a company by defacing it website or it might be that some disgruntled employee is trying to steal the confidential information from the company's Intranet website and then sell it off to the competitor or underground economy for making some quick money.

The largest number of .in websites being targeted by the miscreants is definitely a specific attack on the Indian cyber infrastructure by the adversaries to malign the reputation and hinder the growth of the Indian economy by attacking various e-commerce and other social and government interaction websites. Numerous attacks on .com websites might be because a competitor might be seeking competitive advantage through theft of intellectual property. In some instances a competitor might want to malign the reputation of a company by defacing its website or it might be that some disgruntled employee is trying to steal the confidential information from the company's Intranet website and then sell it off to the competitor or underground economy for making some quick money.

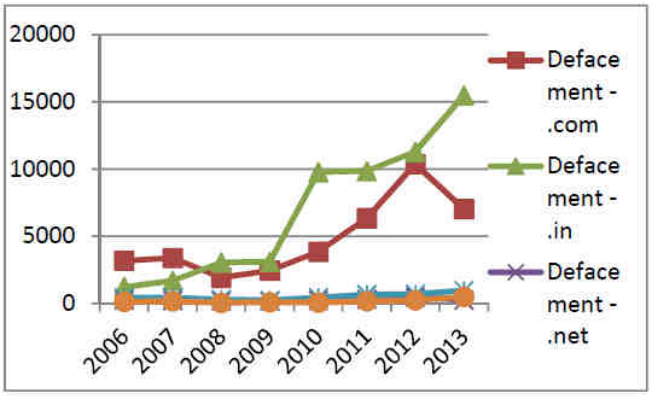


Exhibit 3
(Domain specific website defacement statistics since 2006)

V. Other Attacks Statistics

Individual and organization report numerous security incidents to the Indian CERT centre which handles these varied attacks to analyze and protect the Indian individuals and organizations from the malicious effect of these attacks. Apart from the website defacement incidents other types of attack that have been handled by the Indian CERT centre are shown in table 1.

Table 1 (Number/type of security incidents handled)

Security Incidents	2006	2007	2008	2009	2010	2011	2012	2013
Phishing Attacks	339	392	604	374	508	674	887	955
Network Scanning	177	223	265	303	277	1748	2866	3239
Virus & Malicious Code	19	358	408	596	2817	2765	3149	4160
Spam and Email Spoofing	-	-	305	285	181	2480	8150	54677
Website Malware Propagation	-	-	835	6548	6344	4394	4591	5265
Others	17	264	148	160	188	1240	2417	3484
Total	**552**	**1237**	**2565**	**8266**	**10315**	**13301**	**22060**	**71780**

The table shows that Indian cyber space is constantly being targeted by attacks such as phishing attacks, virus and malware propagation and exploits, network scanning which is used to identify the possible vulnerabilities and exploits, and email spoofing. Since the inception of CERT centre all types of attacks and reporting of such attacks is on rise and in year 2013 more than seventy thousand incidents were handled by CERT-In.

The CERT centre is also tracking the systems in the country which might be part of a larger botnet which has

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

command and control centre within or outside the country, these system are proactively monitored by the centre and the individual and organization to whom the bots belong are notified through their respective internet service provider and they are advised and technical support is provided to these cyber crime victims to clean and protect their systems. It was astonishing to note that as many as 7.5 [4] million such bots were identified by the CERT centre in year 2013 and these activities have shown constant growth is last many years[4][10]. The CERT-In is being supported by many Indian ISPs and security vendors such as RedHat, Cisco, Microsoft, eBay, McAfee, Trend Micro and Symantec in protecting the India cyber space.

VI. CONCLUSION

The analysis done by the authors in the paper proves beyond doubt that the Indian cyber space is constantly being attacked through various types of cyber attacks. The huge number of these attacks are originating from other hostile geographic location and are attacking certain specific domains, knowing the imminent consequences of these threats government of India had constituted the CERT-In centre to mitigate and respond to these cyber incidents. Although the CERT centre has been handling numerous and varied type of cyber incidents, the increasing scope and scale of the incidents is going to be a reality and is going to accelerate in future. The country would need to further strengthen the cyber defense mechanism to protect the critical infrastructure and economy of the country.

REFERENCES

[1] Kamluk V, "The Botnet Business", Securelist (May 13, 2008), https://www.securelist.com/en/analysis/204792003/The_botnet_business?print_mode=1

[2] Srijith K. N, "Analysis of Defacement of Indian Web Sites", First Monday Journal, 7(12)

[3] Cyber Crime & Security Survey Report 2013, CERT-Australia

[4] Indian Computer Emergency Response Team CERT-In, Annual reports 2006-13

[5] Baker Y S, Bhattacharya S, "Analyzing security threats as reported by the United States Computer Emergency Readiness Team (US-CERT)", IEEE conference on Intelligence and Security informatics, 2013, pp 10-12

[6] Arce I, "More bang for the bug: An account of 2003's attack trends", IEEE Security & Privacy, 2004, 2(1), pp 66-68

[7] *Stiawan D , Idris Y, AbdullahA H*, "Attack and Vulnerability Penetration Testing: FreeBSD", TELKOMNIKA Telecommunication, Computing, Electronics and Control, 11(2)

[8] Ransbotham S, Mitra S, "The Impact of Immediate Disclosure on Attack Diffusion and Volume", Economics of Information Security and Privacy, 2013, pp 1-12

[9] Common cyber attacks: reducing the impact – CERT UK, Director GCHQ, http://goo.gl/2RaCGD

[10] Eeten M V, Bauer J M, "The Role of Internet Service Providers in Botnet Mitigation An Empirical Analysis Based on Spam Data", Social Science Research Network, 2011

Narinder Singh Rana, is currently an Assistant Professor in Department of Computer Applications at Tilak Raj Chadha Institute of Management and Technology, Yamuna Nagar, Haryana. He has a master degree in computer application from Kurukshetra University, and is a research scholar at Punjab Technical University. He has five national and international research publications. His area of interest includes network security, sustainable uses of information and communication technology and open source technologies.

Dr. S. N. Panda, is currently Director Research at Chitkara University. He has more than 20 research publication in national and international journals and two patents to his credit. He has a master degree in computer application from Kurukshetra University. He completed his doctorate degree in computer science from Kurukshetra University in 2008 and has worked as principal for 8 years in Regional Institute of Management and Technology, Mandi Gobindgarh, Punjab. His area of interest includes network security, cryptography and big data analytics.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.