Analysis of the Cyber Attacks over the Past Decade

Chitra Kaul
Research Scholar
Singhania University, Rajasthan, India

Dr. B.M.K. Prasad
Principal
Dronacharya College of Engineering, Gurgaon, India

Abstract - In the last decade, the exponential growth in usage of information and communication technology had increased the extent of cyber attacks in frequent and sophisticated manner. According to a survey conducted on the basis of statistics presented from Computer Emergency Response Team Coordination Center (CERT/CC), the cyber attack incidents reported till 1999 increased significantly with the alarming rise to 1.4 lakhs in 2003. The increase in number of cyber attacks had affected the private and government sectors socially as well as financially. This paper focuses on the analysis of the cyber attacks, their classification and types, and finally their impact on the private sector business.

Keywords: cyber attacks, CERCT/CC, Cyber security

I. INTRODUCTION

With the increase in number of connected devices to internet, network and computer attacks are becoming pervasive in today's world. Any computer connected to the Internet is under threat of viruses, worms or attacks from hackers. These threats or attacks can harm home users as well as business user's security. Thus the need to combat with these computer and network attacks has turn out to be a major issue of concern. Statistics from Computer Emergency Response Team Coordination Center (CERT/CC) shows that from 1999 the cyber attack incident reported had increased significantly with the alarming rise to 1.4 lakhs in 2003. Figure 1 shows the incidents reported from 1995 to 2003.

With the emerging tendency of cyber attacks it has become very complex and sophisticated to identify them. Hence, many attacks are comparatively easy to launch and their thorough technical knowledge is no longer required. This has facilitated various clusters of attackers, known as ''script-kiddies'', who can cause huge damage even without knowing how their attack actually works. This drift is represented graphically as shown in Figure 2 [1].

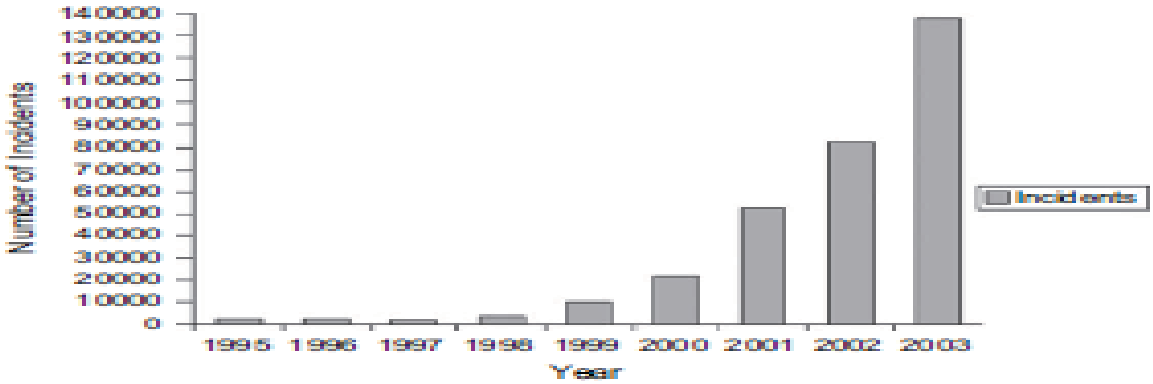

Figure 1 Security incidents reported from 1995 to 2003

II. CYBER ATTACK TYPES

In this section the various types of cyber attacks are briefly discussed [2].

Denial of Service Attacks: Denial of service (DOS) is class of attack where an attacker makes a computing or memory resource too busy or too full to handle legitimate requests, thus denying legitimate user access to a machine. One of the primary goals of DOS is to increase the response time in case of web servers.

Remote to Local (User) Attacks (R2L): It can be defined as the class of attacks where an attacker sends packets to a machine over network, and then exploits its vulnerability to illegally gain local access to that machine. It occurs when an attacker has ability to send packets to a machine over a network but does not have an account on that machine and thus it exploits some vulnerability to gain local access as a user on that machine.

User to Root Attacks (U2R): This type of attacks is defined as the class of attacks where an attacker starts with access as a normal user account on the system and is able to exploit vulnerability to gain root access to the system in which the attacker starts out with access as a normal user account on the system (perhaps gained by sniffing passwords, a dictionary attack, or social engineering) and is able to exploit some vulnerability to gain root access to the system.

Probing: "Probing is class of attacks where an attacker scans a network to gather information or find known vulnerabilities. With the help of map of machine and services that are available on a network an attacker can use this information to find the exploitation in the network [13].

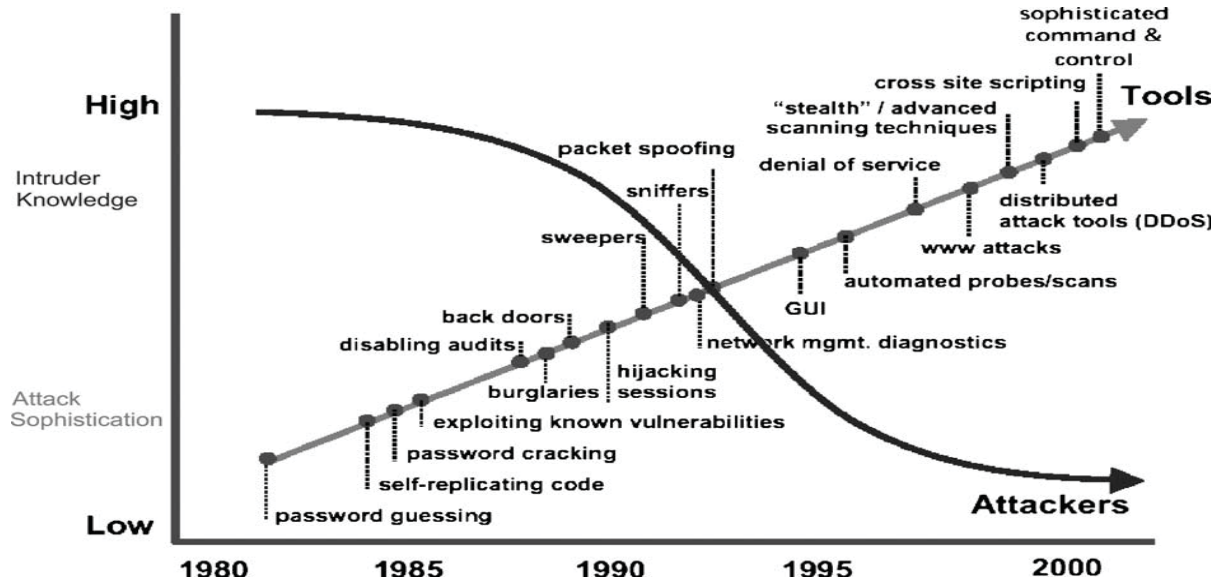

Figure 2 Attack sophistication V/S Attackers computer knowledge.

III. CLASSIFICATION OF CYBER ATTACKS

Attacking a system is not easy or a single step process, so attacker needs to wait till the system gets infected. Number of steps is required to bypass the existing security solution of the system to carry out a successful cyber attack. This attack is capable of acquiring access to resources of system and take out the important information from the system. The hackers causing cyber attack will get their result in stipulated time, in series and in a proper manner. Attacker or hacker uses a systematic approach to attack the system; this will infect the functioning of the system very easily [2]. To achieve more appropriate results attackers use planned methods of operation. This well ordered sequence of attacks generated by attacker leads to severe damage of resources of organization and will also compromise the normal operation of organization [3][4]. Cyber attacks can be broadly classified as follows:

- Reconnaissance Attacks: These types of attacks engage a mapping of unauthorized recognition system and provide facility to obtain data.
- Access Attacks: These types of attacks allow an intruder to gain access to a system to which it have no right to access. Intruder tries to make unauthorized entry to system.

- Denial of Service: This a type of intrusion attack where a intruder tries to disable the network services so that the service are not available for the authorized users. Denial of service (DOS) is category of attack where an intruder or attacker makes a computing or memory resource busy or occupied to handle the requests of legitimate users, thus denying access of legitimate users to access the system.
- Cyber crime makes use of computers and the connected network or internet to utilize clients for materialistic access.
- Cyber espionage is the act of getting benefit of others as a spy through the use of internet.
- Cyber terrorism causes large scale disturbance and demolition of life and property by using cyber space.
- Cyber war is the act of a nation with the intention of disruption of another nation's network to gain tactical and military.
- Active Attacks is type of attacks with data transmission to all parties thereby acting as a liaison enabling severe compromise.
- Passive Attacks is example of attack whose primary concern is eavesdropping without actually modifying the database content.
- Malicious Attacks is example of attack with a deliberate intent to cause harm resulting in large scale disruption [14].
- Non Malicious Attacks is the accidental attack due to mishandling or operational mistakes with minor loss of data.
- Attacks in MANET are the kind of attacks which works on stopping or narrow down the process of information transmission among the nodes.
- Attacks on WSN prevent the sensor nodes to detect or sense the information from environment and also restricts the flow of information in the network.

IV. PRICE OF THE CYBER ATTACKS

US National Security Agency (NSA) Director General Keith Alexander referred to cyber espionage as "the greatest transfer of wealth in history." Globally, the cost of cybercrime is estimated to be upwards of $385 billion [8]. The UK National Audit Office estimates cybercrime costs the UK between £18 billion ($30 billion) and £27 billion ($45 billion) a year.5 In the US that figure is estimated to be roughly $100 billion [9]. In 2013, 54% of total cyber attacks targeted the US, the most of any country, followed by Russia and India, respectively. Nearly half of all attacks originated in China followed by the US at 19% and Canada at 10% [10].

Intellectual property and business intelligence is facing a significant loss due to wide variety of cyber attacks. This can take up the cost of security, hinder workflow, and harm reputation of company. Companies reporting major attacks suffer a 1-5% drop in stock value, while some companies recover, others may lose everything. Canadian telecom giant Nortel Networks Ltd. had been infiltrated by Chinese hackers for nearly a decade before filing for bankruptcy in 2009. Investigators took several years to find the extent of damage caused to critical data by the intruders, as the intrusions were so well defined so were difficult to identify [11].

Insurance is taken as the financial protection against the inevitable threat of attacks by various companies. Cyber insurance usually includes regulatory fees and the fees to repair systems after security breaches. Number of policies has exceptions whose scope of coverage excludes loss of business intelligence and stolen intellectual property. Still, cyber insurance is a successful business. In the US insurance grew from less than $100 million in annual premiums in 2002 to $800 million in 2011 and now similar growth is occurring in Asian and European markets as the loss due to attacks continues to rise [12].

V. CONCLUSION

There is a need to reduce the vulnerabilities of private sector as the cyber attacks have grown exponentially that too in severe and complex manner. Recent studies shows that attackers are not working individually, instead they work as groups of intended criminal attacks on cyber security with huge network links and resources. The organizations which are affiliated from state present an growing intricate political limit for both public as well as private sectors. An organization that deals with current concerns can also face the mission of preparing for future ones [15]. Attacks on the healthcare and pharmaceutical industries are continuously at rise from the last few years. Attackers can steal personal information of the customers from medical records allowing hackers to commit fraud in a way such that is hard for external security agencies to identify. There is an increase of 100 % criminal attacks on network systems

between 2010 and 2013 on healthcare companies and this will continue to rise. The major reason of security threat is the shift of many companies to cloud computing environment as about three-quarters of users are employing cloud computing however less than half utilize cloud security. With the increase in content available in cloud, the risk of cyber attacks on the content is augmented and thus is the need for tools to protect and maintain the cloud data.

REFERENCES

[1] Lipson HF et al, "Tracking and tracing cyber-attacks: technical challenges and global policy issues", Technical report, CERT Coordination Center; November 2002.

[2] Jamal Raiyn, "A survey of Cyber Attack Detection Strategies", International Journal of Security and Its Applications Vol.8, No.1 (2014), pp.247-256.

[3] M. Uma et al, "A Survey on Various Cyber Attacks and their Classification", International Journal of Network Security, vol. 15, no. 6, (2013), pp. 391-397.

[4] S. Singh et al, "A Survey of Cyber Attack Detection Systems", IJCSNS International of Computer Science and Network Security, vol. 9, no. 5, (2009) May, pp. 1-10.

[5] Hold Security, LLC announces Credential Integrity Services. "*Hold Security.* 25 Feb 2014, Web, 1 Jun 2014. http://www.holdsecurity.com/#!news2013/c13i.

[6] 2013 Cost of Cybercrime Study: Global Report. "Ponemon *Institute.* Oct 2013, p. 10. Web. 9 Jun 2014. DDoS attacks are comprised of a flood of messages to a system which are intended to knock websites offline by overwhelming them with traffic.

[7] Bryan Watkins, "The Impact of Cyber Attacks on the Private Sector", Briefing Paper, Association for International Affair, August *2014.*

[8] Net Losses: Estimating the Global Cost of Cybercrime." Center for Strategic and International Studies. Jun 2014, Web, 18 Jun 2014, p.6. http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

[9] The Economic Impact of Cybercrime and Cyber Espionage." *McAfee*. 2013, p. 5.

[10] "Fourth Quarter 2014: State of the Internet." Akamai. Vol. 6, No. 4. 2014, Web, http://www.akamai.com/dl/akamai/akamai-soti-q413.pdf?WT.mc_id=soti_Q413

[11] Gorman, Siobhan. "China Hackers Suspected in Long-Term Nortel Breach." *Wall Street Journal Online.* 14 Feb 2012, Web, http://online.wsj.com/news/articles/SB10001424052970203363504577187502201577054

[12] Beck, David, L.; Siemens, Rene L. "Cyber Insurance—Mitigating Loss from Cyber Attacks." *Pillsbury Law*. 2012, Web, http://www.pillsburylaw.com/publications/cyber-insurancemitigating-loss-from-cyber-attacks

[13] Luhach, A.K.; Dwivedi, S.K.; Jha, C.K., "Applying SOA to an E-commerce system and designing a logical security framework for small and medium sized E-commerce based on SOA," in *Computational Intelligence and Computing Research (ICCIC), 2014 IEEE International Conference on* , vol., no., pp.1-6, 18-20 Dec. 2014. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7238358&isnumber=7238030

[14] Luhach, Ashish Kr, Sanjay K. Dwivedi, and C. K. Jha. "Designing and implementing the logical security framework for e-commerce based on service oriented architecture." *arXiv preprint arXiv:1407.2421* (2014).

[15] Luhach, Ashish Kr, Sanjay K. Dwivedi, and C. K. Jha. "Desiging a logical security framework for e-commerce system based on soa." *arXiv preprint arXiv:1407.2423* (2014).