International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 8 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT183834

Cyber Crime and Security

Nisarg C Joshi[1], Jaydipsinh B Thakor[2]
[1]Assistant Professor, Physics(EC) Department, Ratnamani Science College, Becharaji, Mehshana, Gujarat, India
[2]Computer Lab Assistant, Computer Department, Ratnamani Science College, Becharaji, Mehshana, Gujarat, India

ABSTRACT
Cybercrime is becoming ever more serious. Findings from the 2002 Computer Crime and Security Survey show an upward trend that demonstrates a need for a timely review of existing approaches to fighting this new phenomenon in the information age. In this paper, we define different types of cybercrime and review previous research and current status of fighting cybercrime in different countries that rely on legal, organizational, and technological approaches. We focus on a case study of fighting cybercrime in India and discuss problems faced. Finally, we propose several recommendations to advance the work of fighting cybercrime. Cybercrime falls into three categories: (1) a computer is the target of criminal activity; (2) the computer is the tool used or is integral to the commission of the crime; and (3) the computer is only an incidental aspect of the crime. Cybercrime is a relatively new phenomenon. Services such as telecommunications, banking and finance, transportation, electrical energy, water supply, emergency services, and government operations rely completely on computers for control, management, and interaction among themselves. Cybercrime would be impossible without the Internet. Most American businesses maintain WWW sites and over half of them conduct electronic commerce on the Internet. The rise in popularity of the Internet for both private persons and businesses has resulted in a corresponding rise in the number of Internet-related crimes.

Keywords: Cyber Crime, Cyber Security

I. INTRODUCTION

Cybercrime is criminal activity done using computers and the Internet. This includes anything from downloading illegal music files to stealing millions of dollars from online bank accounts. Cybercrime also includes non-monetary offenses, such as creating and distributing viruses on other computers or posting confidential business information on the Internet.

Perhaps the most prominent form of cybercrime is identity theft, in which criminals use the Internet to steal personal information from other users. Two of the most common ways this is done is through phishing and phrasing. Both of these methods lure users to fake websites (that appear to be legitimate), where they are asked to enter personal information. This includes login information, such as usernames and passwords, phone numbers, addresses, credit card numbers, bank account numbers, and other information criminals can use to "steal" another person's identity. For this reason, it is smart to always check the URL or Web address of a site to make sure it is legitimate before entering your personal information. Because cybercrime covers such a broad scope of criminal activity, the examples above are only a few of the thousands of crimes that are considered cybercrimes. While computers and the Internet have made our lives easier in many ways, it is unfortunate that people also use these technologies

to take advantage of others. Therefore, it is smart to protect yourself by using antivirus and spyware blocking software and being careful where you enter your personal information.

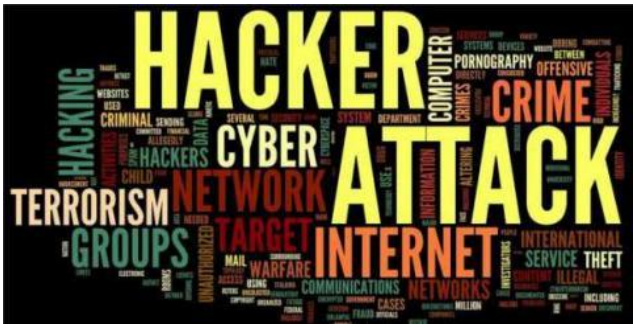

Figure 1 : Cyber Crime

II. METHODS AND DISCUSSION

Hacking

In simple words, hacking is an act committed by an intruder by accessing your computer system without your permission. Hackers (the people doing the 'hacking') are basically computer programmers, who have an advanced understanding of computers and commonly misuse this knowledge for devious reasons. They're usually technology buffs who have expert-level skills in one particular software program or language. As for motives, there could be several, but the most common are pretty simple and can be explained by a human tendency such as greed, fame, power, etc. Some people do it purely to show-off their expertise – ranging from relatively harmless activities such as modifying software (and even hardware) to carry out tasks that are outside the creator's intent, others just want to cause destruction. Greed and sometimes voyeuristic tendencies may cause a hacker to break into systems to steal personal banking information, a corporation's financial data, etc. They also try and modify systems so that they can execute tasks at their whims. Hackers displaying such destructive conduct are also called "Crackers" at times. They are also called "Black Hat" hackers On the other hand; there are those who develop an interest in computer hacking just out of intellectual curiosity. Some companies hire these computer enthusiasts to find flaws in their security systems and help fix them. Referred to as "White Hat" hackers, these guys are against the abuse of computer systems. They attempt to break into network systems purely to alert the owners of flaws. It's not always altruistic, though, because many do this for fame as well, in order to land jobs with top companies, or just to be termed as security experts. "Grey Hat" is another term used to refer to hacking activities that are a cross between black and white hacking. Some of the most famous computer geniuses were once hackers who went on to use their skills for constructive technological development. Dennis Ritchie and Ken Thompson, the creators of the UNIX operating system (Linux's predecessor), were two of them. Shawn Fanning, the developer of Napster, Mark Zuckerberg of Facebook fame, and many more are also examples. The first step towards preventing hackers from gaining access to your systems is to learn how hacking is done. Of course it is beyond the scope of this Fast Track to go into great details, but we will cover the various techniques used by hackers to get to you via the internet.

Denial-of-Service Attack

A Denial-of-Service (DoS) attack is an explicit attempt by attackers to deny service to intended users of that service. It involves flooding a computer resource with more requests than it can handle consuming its available bandwidth which results in server overload. This causes the resource (e.g. a web server) to crash or slow down significantly so that no one can access it. Using this technique, the attacker can render a web site inoperable by sending massive amounts of traffic to the targeted site. A site may temporarily malfunction or crash completely, in any case resulting in inability of the system to communicate adequately. DoS attacks violate the

acceptable use policies of virtually all internet service providers. Another variation to a denial-of-service attack is known as a "Distributed Denial of Service" (DDoS) attack wherein a number of geographically widespread perpetrators flood the network traffic. Denial-of-Service attacks typically target high profile web site servers belonging to banks and credit card payment gateways. Websites of companies such as Amazon, CNN, Yahoo, Twitter and eBay! are not spared either.

Virus Dissemination

Viruses are computer programs that attach themselves to or infect a system or files, and have a tendency to circulate to other computers on a network. They disrupt the computer operation and affect the data stored – either by modifying it or by deleting it altogether. "Worms" unlike viruses don't need a host to cling on to. They merely replicate until they eat up all available memory in the system. The term "worm" is sometimes used to mean self-replicating "malware" (Malicious software). These terms are often used interchangeably in the context of the hybrid viruses/worms that dominate the current virus scenario. "Trojan horses" are different from viruses in their manner of propagation. They masquerade as a legitimate file, such as an email attachment from a supposed friend with a very believable name, and don't disseminate themselves. The user can also unknowingly install a Trojan-infected program via drive-by downloads when visiting a website, playing online games or using internet-driven applications. A Trojan horse can cause damage similar to other viruses, such as steal information or hamper/disrupt the functioning of computer systems. The Personal Area Network is shown in Figure: 2

Figure 2. Virus Dissmination

Phishing

A SAN typically supports data storage, retrieval and replication on business networks using high-end servers, multiple disk arrays and Fiber Channel interconnection technology. Storage Area Networks (SANs) technology is similar but distinct from network attached storage (NAS) technology. While SANs traditionally employ low-level network protocols for transferring disk blocks, a NAS device typically works over TCP/IP and can be integrated fairly easily into home computer networks. The term SAN can sometimes refer to system area networks instead of a storage area network. System area networks are clusters of high performance computers used for distributed processing applications requiring fast local network performance. Storage area networks, on the other, are designed specifically for data management. SANs support disk mirroring, backup and restore, archival and retrieval of archived data, data migration from one storage device to another and the sharing of data among different servers in a network. SANs can incorporate sub networks with network attached storage (NAS) systems. Simplification of Storage Administration is now possible because of Storage Area Networks cause cables and a storage device doesn't need to be moved physically. Moving data from one server into another is now a breeze. Storage area networks are great tools in recovering important data and backups. Distant location doesn't affect the storage area networks as long as the secondary storage array is working. This

enables storage replication either implemented by disk array controllers, by server software, or by specialized SAN devices. Since IP WAN's are often the least costly method of long-distance transport, the Fiber Channel over IP (FCIP) and ISCSI protocols have been developed to allow SAN extension over IP networks.

Financial Cybercrime

This crime is when you utilize your skills or third party access for the main purpose to get financial profit. Like accessing an e-bank portal in an unauthorized way and make transactions, make e-commerce payments and take goods without permission.

III. CONCLUSION

The risks of cybercrime are very real and too ominous to be ignored. Every franchisor and licensor, indeed every business owner, has to face up to their vulnerability and do something about it. At the very least, every company must conduct a professional analysis of their cyber security and cyber risk; engage in a prophylactic plan to minimize the liability; insure against losses to the greatest extent possible; and implement and promote a well-thought-out cyber policy, including crisis management in the event of a worst case scenario.

IV. REFERENCES

[1]. Prof. Briere, E. (1966). Quantity before quality in second language composition. Language Learning 16, 141-151.

[2]. Bums, H. & Culp, G. (1980, August). Stimulating invention in English composition through computer Assisted instruction. Educational Technology, 5-10.

[3]. Daedalus Integrated writing environment [Computer software). (1994). Austin, TX: The Daedalus Group, Inc.

[4]. Keirn, W. (1989). The writing-grammar battle: Adventures of a teacher/administrator. Englsh Journal, 78, 66-70.

[5]. Brewin, B., UPS to spend $127M on tri-mode wireless driver terminals. http://www.computerworld.com

[6]. Haskin, D., Motient Files for Chapter 11. http://www.internetnews.com

[7]. The switch from CDPD to GPRS. http://www.airlink.com/

[8]. ARDIS, DataTac 4000, Software Developers Reference Guide, Revision 2.0

[9]. Goldsmith, C., Wireless Local Area Networking for Device Monitoring. University Of Rochester, Rochester NY.

[10]. IEEE Std 802-2002, IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture, page 1, section 1.2: "Key Concepts", "basic technologies"

[11]. Karunakar Pothuganti and Anusha Chitneni "A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, Wi-Fi", Advance in Electronic and Electric Engineering, ISSN 2231-1297, Volume 4, Number 6 (2014), pp. 655-662

Author's Profile

Mr. Nisarg C Joshi

M.Phil, PhD (Pursuing) in Electronics and Communication, Working as Assistant Professor in Ratnamani Science College, HNGU, Shankhalpur, Becharaji, Mehsana, Gujarat, India

Mr. Jaydipsinh B Thakor

MCA from KSV University, Kadi, Mehsana, Gujarat, Working as Computer Lab Assistant in Ratnamani Science College, HNGU, Shankhalpur, Becharaji, Mehsana, Gujarat, India