Cybercrime

1

Poongodi Thangamuthu
Galgotias University, India

Anu Rathee
Maharaja Agrasen Institute of Technology, India

Suresh Palanimuthu
Galgotias University, India

Balamurugan Balusamy
Galgotias University, India

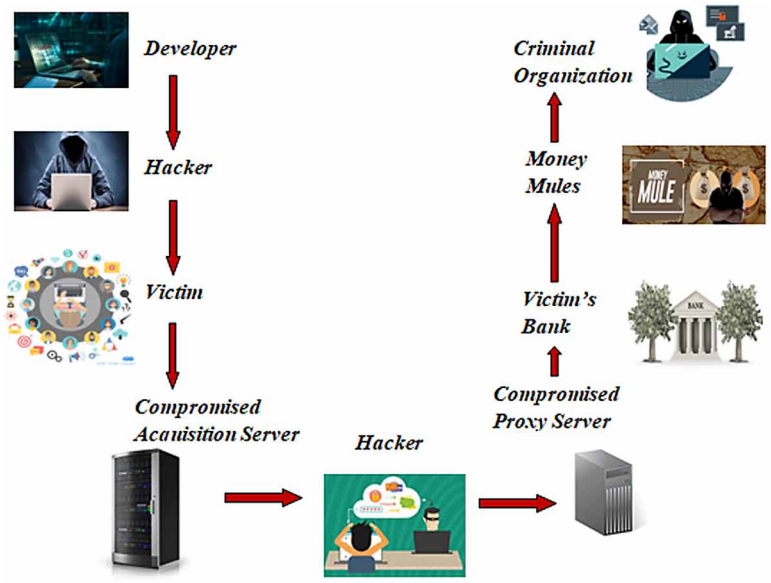
INTRODUCTION

The cybercrime prediction over the past year says about the damage cost by tracking the activities in government officials, industry experts, cybersecurity companies, universities, colleges, media outlets globally. A criminal way of doing an activity through the use of digital devices and internet by a group of people is known as cyber crime. The critical issue of cyber crime is pulling everyone's attention across the world. Due to the fast growth in e-commerce, e-governance, social networking and various other e-services cybersecurity has a growing challenge where database is easily collected and misused. Cyber attacks are more pervasive and threats to critical infrastructure and lack of security and underreporting makes industrial systems and products more vulnerable. Internationally, the most affecting problems are mass-ransomware attacks and valuable data theft much more in the last few years. Lack of electronic evidence in cybercrime and proper convergence between private, and government institutions are making difficult to seize and stop criminal financial transactions. Based on historical cybercrime statistics, there would be a dramatic increase in crime gang hacking activities and the cyber attack surface will be an order of magnitude greater in 2021 than today. According to the prediction of cybersecurity ventures, the cybercrime will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015. The estimated cyber security cost is rapidly growing to $170 billion dollars in 2020 that was only $75 billion Dollars in 2015. The European countries, making the directives used to protect the information in systems from threats, the first directive is EGDPR (European General Data Protection Regulations) and the second directive is NIS (Network Information Security).

The criminal activity of cybercrime includes the theft of intellectual property, damage and destruction of data, theft of personal data, stolen money, forensic investigation and reputational harm. Cybercrime is an online threat that can be committed by targeting the computer devices, computer networks and the automated processes performed through the use IT systems by creating and distributing malwares or viruses. Cybercrime allows attackers to penetrate in a well-controlled environment and the malicious activities remains untraceable. As it is a rapid growing area of crime, criminals exploit the convenience, speed, anonymity of the internet and committing various criminal activities by posing different threats

DOI: 10.4018/978-1-5225-9715-5.ch001

Figure 1. Cybercrime process



to victims worldwide on an unprecedented scale. The cyber crime process is explained in the following: Initially, the developer writes the malware code. Hacker uses the malware to exploit the credentials of victim's personal computer. For instance, bank account credentials are revealed to hackers from the victim's computer system and the hacker acquires the credentials of the target by compromising the server. The attacker gains the remote access to an individual's financial account in the victim's system and it is being stolen by manipulating the account from the concerned targeted bank by compromising the proxy server. The stolen fund is transferred to the money mule bank account and then it is transferred to criminal organization. The process of cybercrime is depicted in Figure 1.

Cyber attackers have the objectives for which they do cybercrime / cyber-attack (Kumar et al, 2014; Rawat et la, 2015). Significant objectives of cyber attackers are discussed below:

Entertainment

Some cyber attackers are performing criminal activities to examine their hacking abilities. Such persons are interested in getting fame in the cybercrime world. They feel proud of their successful attempts that were not achieved by any other attacker or some attackers failed to execute such kind of attack.

Hacktivists

These kinds of cybercriminals are stimulated by religious, social and political ends. Their intention is to inculcate the religious and political mottos among people and to depress them. It is an attempt of extending the religious or political popularity among the crowd. Recently, hacktivists are revealing the individuals secret affairs via social web sites.