Top Five Cyber Frauds

Rajesh Kumar Goutam
Department of Computer Science
University of Lucknow
Lucknow

Deepak Kumar Verma
Department of Computer Science
Sama Degree College
Lucknow

ABSTRACT
In last three decades the attacks against the personal information, social information and financial information become more frequent and sophisticated. Initially, the purpose of cyber attack was the entertainment but as scenario has changed, internet is now seen as wonderful tool to conduct fraud or to grasp the information about anyone else. The paper shows how internet is important for cyber criminals and why they use it as a secure medium to conduct fraud. The major five categories of cyber crimes have been explained with their landscape. We have also presented a brief idea about the cost of stolen items in terms of information in underground cyber black market and its impact on society.

Keywords
Cyber security, Malware, Cybercrime.

1. INTRODUCTION
Cyber space is getting more attention nowadays as its coverage is continuously growing in almost every aspect of our lives. It is being a popular subject of debate for the media and various institutions from public sectors as well as private sectors. Often its disastrous impacts are highlighted in news paper and media. As almost, each person is using cyberspace and its services directly or indirectly so it becomes important and vital for each one to know its area, coverage and its disastrous impacts. Awareness among the people about the cyber security is now essential to reduce its dangerous impacts.

In reality, cyber security is now not a new concern, before a decade the same problem was available in different scenario. Cybercrime is not a technology problem instead a strategy problem, a human problem and a process problem [1]. The impacts of cyber attacks were not as dangerous as now. The volumes of cyber attack were comparatively less. Initially, cyber attacks were conducted to make a person panic. Financial gain was not behind the objective but now scenario has been changed, cyberspace has now been converted in safe tool for making forgery and conducting crimes.

Cyber space is treated on the one hand beneficial as it provides information and services in very less time with almost minimum price across the world. On the other hand, it has a disadvantage that cyber attacks may be conducted from around every corner of the world as it is borderless and shapeless in nature. It becomes not easy to arrest the cyber criminal instantly as it becomes difficult to recognize guilty due to anonymity of actor property of cyber space.

It is property of internet that allows it to grow up quickly and be sustainable. It is open equally to all for end users to access and innovators for creation and governance. These two aspects of access do not take place separately instead arise in the same virtual space. In about last two decades, cyber terrorists also enjoyed the benefits of internet and cyber space.

It may be said that in recent years of economy, one industry that has recorded double digit growth is the cyber crime. Now cyber crime has been converted in to regular profession. In early 1990s, when cyber crimes started to occur in form of hackings, were the activities of males in age group 20 to 30 years. The reason for such illegal activity was only fun. With the time, the age group, objective and scope of the cyber crime has now been dramatically changed. Today's cyber criminals can be in any age group. They have adopted it as profession. It is seen as source of their income. As a result, today's cyber attacks become more sophisticated. Another reason that has a big share in cyber crime growth is readymade malicious software. Anyone can buy this software and use it to steal credit card numbers and other personal Information.

2. MALWARE
Malware is a piece of software that is inserted into your computer to destruct the information system therein. It may harm the other attached hardware devices and group of systems. It also removes the system from their actual track and does whatever is not desired by the owner. In some cases, it satisfies the owner by completing assigned task and does some extra task that intends task for intruders. In other words, the malware infected system more often completes two kinds of task; one for the owner of system and other for intruders. In other words, the malware provides remote access to the computer to intruders. It sends the existing data on the system to the third party without user's permission and knowledge, becomes able to break the security measures and privacy of the system. The fig.1 shows the major five categories of malware. Trojan in very popular category, shares about 64% of malware [8].

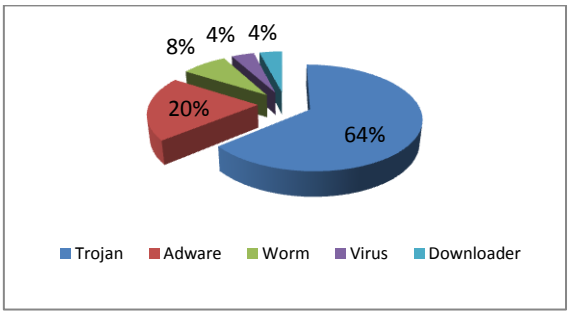

Fig 1: Top five categories of Malware

Malware becomes active because of various factors including ineffective operating systems development and existing vulnerabilities in software's installed on. Malware requires human activity to gets it installed. Internet presents an effective medium through which often intruders get success to install malicious software to a targeted system without user's permission and knowledge. As a result often users become unknown for their information theft until the theft converts into serious event.

3. MAJOR CATEGORIES OF CYBER CRIME

As internet was not designed to track the human activity rather it was constructed to provide a common platform to researchers to share ideas and inventions [9]. As there was no provision in those days to track the internet users activity so people enjoyed its weakness and kept on using this as a tool to conduct crimes. There are few differences between manual crimes and cyber crimes. In manual crimes often criminal gets involve in crime physically and its coverage area becomes limited. In other words, the impact of manual crimes affects limited geographical area and single or a group of persons. This category of crime often does not have capability to harm a particular nation or its infrastructure. On the Other hand, the cyber crime has been newly evolved, with larger area of impact holds the capability to harm nations and their infrastructure and economy. The interesting thing is that it is very difficult to locate the origin of cyber crime. As a result, in maximum cases, the accused is not punished. On the basis of available literature, top five types of cyber crimes are as follows [2].

- Tax refund fraud
- Corporate account takeover
- Identity Theft
- Theft of sensitive data
- Theft of Intellectual Property

3.1 Tax Refund Fraud

In recent year, several new methods emerged to conduct cyber crimes, Tax refund fraud is also one newly evolved method provides financial benefits to cyber criminals.

Table 1. Cost of Products in Black Market

Product	Price
Credit Card details	From $2 to $9 per card
Physical Credit Card	From $190 to $220 Plus cost of details
Card Cloners	From $200 to $1000
Fake ATMs	Up to $3500 plus cost of details
Bank Credentials	From $80 to $700
Online Stores and Payment Platform	From $80 to $1500
Spam Rental	Starts from $15
SMTP rental	From $20 to $40 for three months
VPN rental	$20 for three Months

In this type of crime, the cyber criminals first try to attain valid information about the person preferably who is not filling tax such as name, social security number and voter ID or Adhaar number.

The information about dead persons becomes also valuable for cyber criminals. The information is generally acquired with E-mail phishing and social networking sites. The information is also can be purchased from the black market [6]. Thereafter, intruders make pressure to pay the tax in attractive schemes. In this way, customers often handover their tax payments to fraud hands. Tax refund fraud can also be conducted with readymade tool. The table 1. shows the prices of various products in black cyber market [6].

3.2 Corporate Account Takeover

In 2008, a different type of cyber crime have been identified named corporate account takeover where cyber criminals often use electronic means to conduct financial fraud or redirect money from legitimate account to their own account. Before few years, the hijacking of corporate accounts has been done with creation of new ACH files but now scenario has been changed now such type of accounts takeover is committed by manipulating the account information already submitted to banks. The manipulation in bank information becomes innocuous and difficult to notice until irreparable damage done against any organization to its finance and reputation [2]. However, it is difficult to guess total cost of corporate account takeover, about $10,000,00,000 loss was estimated by FBI in alone USA in 2011 [3]. It presents a glimpse that how this type of cyber crime is dangerous. According to Business banking survey conducted by Ponemo Institute' in 2010 that about 80 percents financial institutions are unknown about the fraud until the funds have been transferred [3].

3.3 Identity Theft

Identity theft is different kind of fraud in which a person illegally uses someone's else identity to have financial gain. Cyber criminal often use identity of some valid person, citizen or famous personality and does crime with their name. In this way, perpetrator harms two parties simultaneously; first party with which it communicates and provides wrong information about himself and another party whose identity is being used in fraud. Perpetrator can use stolen personal and financial information to access your bank accounts, opening new accounts, transferring bank balances or purchasing etc. In 2012 about 12.6 million American reported identity fraud [4]. Federal Trade commission presented a report in which major areas of cyber fraud have been explained where original identities are used as follows to conduct cyber crimes [4].

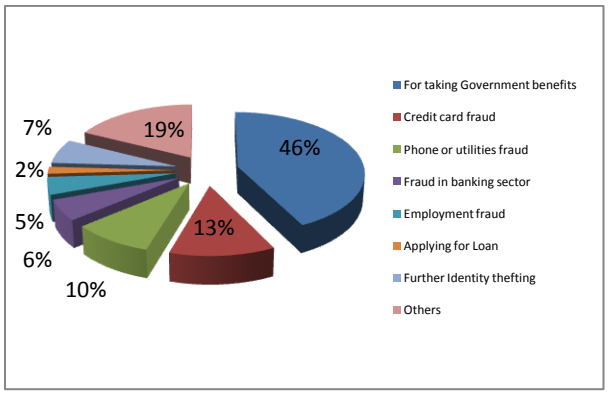

Fig 2: Various sectors for theft identities usage

3.4 Intellectual property theft

Intellectual property can be defined as any creation of mind, containing artistic and literacy work, slogan, formula, method, algorithm, logo, design and invention with an economic value and used commercially [5]. Table 2. shows the various motivating factors behind the Intellectual property theft [5].

Table 2. Motivating factors for Intellectual property theft

Purpose	Details
Financial Gain	Selling of the stolen information becomes the primary objective in cyber black market at higher rate to attain financial gain.
Competitive advantage	To have more advantages than its competitors.
Sabotage	To damage the reputation and functioning of targeted organization.
Political	The stolen intellectual property is also used to accomplish political benefits.
Nationalistic loyality	To achieve the higher rate of success in competitiveness of business in hackers society.

If anyone else uses your intellectual property without your information and permission for profit then the person becomes guilty of stealing your intellectual property. Intellectual property is often protected and secured from thefting by using patents on new inventions or creations, copyrights on music, video, figure, logo and literacy materials and trademarks on branded devices.

3.5 Theft of Personal Sensitive data

Sensitive data includes a wide range of information such as your personal information, political opinion, religious views, personal secrets like social relations, physical and mental health information, insurance policies, property details etc [2]. In other words, for your personal information you have full rights to access and use and also have right to know how other people are doing the same. There is a difference between the personal sensitive data and identity theft. Identity theft is actually performed to acquire your identity or availability by someone else in fraud manner while personal sensitive information is acquired to know your background and behavior. Often, this information is misused to spoil your reputation in social and family environment.

4. INFORMATION AT RISK

It is not essential that your personal or social information is theft only for the revenge purpose.

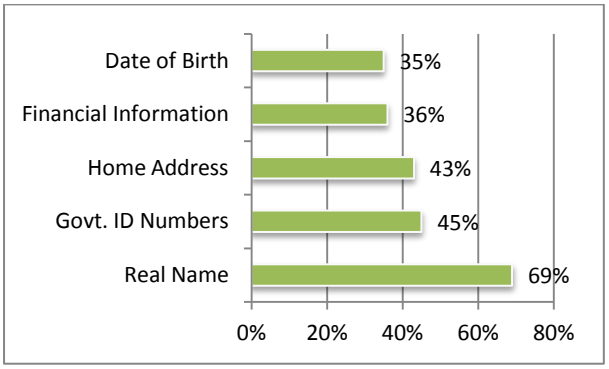

Fig 3: Top five personal information usually theft

It may be theft for selling purpose in black market. Every time and every where you are at risk in this high competitive era. As there are different methods used by different cyber criminals so there is vital need to be aware about the recent updates about cyber crimes and its methods. Almost, it is impossible to become untouched with technology, web and internet now a day. Only our awareness about the cyber crimes scenario can save us from our misuse and fraud. The Fig. 3 shows top five personal information pieces often becomes relevant for cyber criminals [7]. The real name is rated as top with 69% at risk. Cyber criminals not only concern with the personal information but also your professional information or organizational information too.

5. CONCLUSION

It is extremely difficult to be sure about the involvement of any person in a cyber crime. It is also equally difficult to locate the origin of cyber crime. Because of these few reasons, the rate of cyber crime is growing tremendously. In this paper, we have detailed about the nature of cyber space and explained why do criminals opting internet as a wonderful tool to conduct crimes? We have listed top five cyber crimes often take place in virtual cyber space. Thereafter, we have emphasized various areas where the theft identities are being misused to conduct fraud. The rates of various stolen items are described in international cyber black market. The paper also details about the various motivating factors behind the intellectual property theft and presents the top five pieces of personal information which often become target in various cyber frauds.

Note: the Data of table 1 has been taken from the report: A Report the Cyber crime Black Market: Uncovered, Panda Security, 2010

6. REFERENCES

[1] A report, Economic Impact of Trade Secret Theft: A framework for companies to safeguard trade secrets and mitigate potential threats, Centre for responsible enterprise and trade, February 2014.

[2] A Report available from Tommie Singleton, the top 5 cyber crimes, AICPA, October 2013.

[3] A Report on Corporate Account Takeover: Traditional Protection Strategies Not Enough; Multi-Dimensional, Preemptive Strategies Needed. 2011 available at http://achalert.com/uploads/Documents/WhitePaper.pdf.

[4] A Kristin Finklea, Identity Theft: Trends and Issues, CRS Report prepared for members and committees of congress, January 16, 2014.

[5] Booz, Allen and Hamilton, Cyber Theft of Corporate Intellectual Property: The Nature of the Threat, An Economist Intelligence Unit research, 2012.

[6] A Report the Cyber crime Black Market: Uncovered, Panda Security, 2010.

[7] Internet Security Treat Report (ISTR 20) From Symantec, Vol 20, April 2015.

[8] Cisco 2014 Annual Security Report available at http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.

[9] Howard F. Lipson. Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues, Carnegie Mellon Software Engineering Institute, Pittsburgh, November 2002