International Journal of Electrical Electronics & Computer Science Engineering
Special Issue - NCSCT-2018 | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
March, 2018 | Available Online at www.ijeecse.com

Internet of Crimes

Devshanker Banerjee[1], Ayush Bhaskar[2], Dr. Megha Gupta[3]
[1-2]UG Scholar, [3]Associate Professor, Department of CSE, Poornima Institute of Engineering & Technology, Jaipur, India
12015pietcsdevshanker@poornima.org, [2]2015pietcsayush@poornima.org, [3]Megha.gupta@poornima.org

Abstract: We will discuss the problems of cybercrime in this review paper, along with the categories. Cybercrime is increasing day by day and hence causing trouble in various Sectors. The speed of internet has give a new look to the old crimes. Thieving and fraud has become an invisible and unknown crime these days. The trouble and chaos cause by hacking and other online fraud cannot be measured in simple terms. Cybercrime can be classified into broad three categories. First the internet enable a common man to be a law breaking one without even moving from their home . The net gives a platform for unnatural behaviour. Third, the internet has become the major area for cybercrimes and online frauds. The aim of this analysis paper is to focus on the detailed analysis and some of the common terms related to cyber crime in our environment.

Keywords: Security, Network Security, Computer, Privacy, Cyber Crimes.

I. INTRODUCTION

Cybercrime is termed as the use of computer, laptops, internet , programs for activities such as frauds, kid trafficking porn and, stealing identities, or dissimulation to be somebody or one thing else. The computer will be utilized in the process of cybercrime, or it's going to be the target. Cybercrime, particularly through the net, has mature in importance because the laptop has become central to commerce, amusement, and government. These attacks generally happen on public or private body but it seems to happen over the Internet. Within the digital age and digital revolution, our virtual identities square measure essential components of everyday lifes. Crime describes the role of network web over computers in our lives, moreover because the fragility of such ostensibly solid facts as individual identity. The review paper provides a detail about these different kinds of communities. The review paper then takes United States into a discussion of policy steps to scale back and eliminate some kinds of crime.

II. DEFINING CYBER CRIME

It is the criminal activity that occurs over using of a computing system, technology, or the web for act of terrorism, pc viruses, fraud, cyberbullying.[1] The category of law-breaking is broken into many classes which will be termed as:

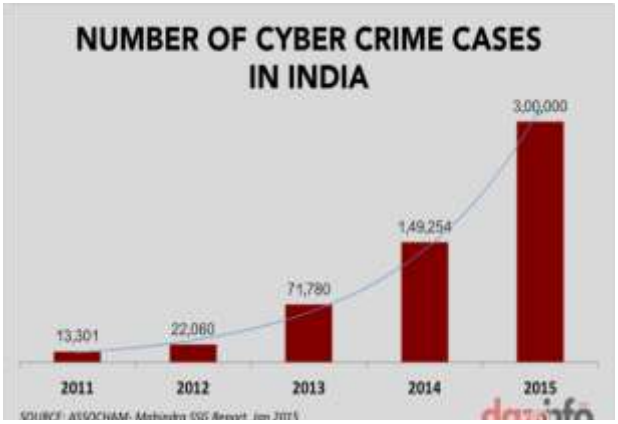
1. Identity Theft: It is termed as the stealing of some ones indentity in order to acquire some ones bank account, property or accuse someone to defame

them within the name of that person.

2. Cyberbullying: It is the process of harassing, blackmailing, embarrassing somebody over the web through the platform of social media like Facebook, Instagram etc.

3. Cyberterrorism: Cyberterrorism is the process of hurting a mass of people over the Internet. The increase in laptops and computer systems enable cyberterrorism as they makes use of well-planned attacks on government and company laptop systems.

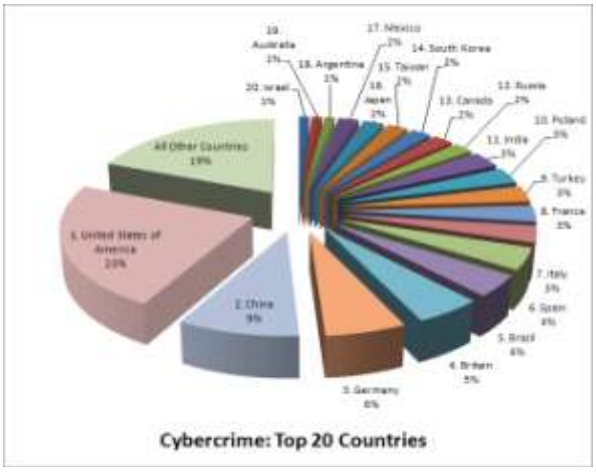
III. CYBERCRIME OVER THE YEARS



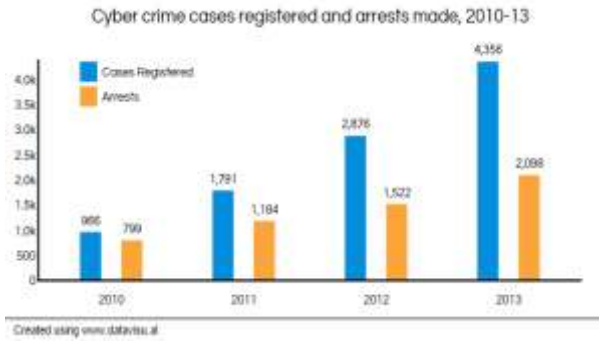
Cyber crimes reported in India rose 19 times over the last ten years (2011 to 2015)from 13,301 in 2011 to 3,00,000 in 2015, and India is now ranked third – after the US and China – as a source of "malicious activity" on the Internet and second as a source of "malicious code".[2]. Internet subscribers in India crossed the 400 million mark, and are expected to reach 462 million by June 2016.

IV. CYBERCRIMES TOP 20 COUNTRIES

Symantec has listed 20 country that faces the most cyber crimes in the world.While generating this list Symantec also got the idea how a piece of code is used for these purpose.They also study varies types of malware created and varies phising sites found on the internet.[3] They also acquired the detail about the amount of bot-infected systems that rectangular measure the ones controlled by cybercriminals, rank nations anywhere cyber attacks initiated and remember the top rate of law-breaking in countries which have quite a few get right of entry to broadband connections. These countries also got affected hugely by these activities over the years. Syria, Nigeria etc are one of the countries with most cyber crime recorded in past 5 years.



V. CASES REGISTERED VS ARRESTS



A total of 4,356 cases were registered below varied sections of IPC throughout the year two013 as compared to two,876 such cases throughout 2012, so showing an increase of fifty.6% over the previous year. 65.9% (2,870 cases) of the complete four,356 cases registered below completely totally different sections of IPC were related to cheating followed by 2.5% (109 cases out of 4,356 cases) below information crime. a whole of 1,681 cases below completely totally different sections of IPC were unfinished for investigation from previous year out of total cases for investigation (5,094 cases) throughout 2015 and 3,605 cases remained unfinished for investigation at the highest of the year. In 710 cases, charge-sheets were submitted throughout 2013. Forgery below IPC crimes shows highest pendency rate (81.0%) followed by information crime (76.5%) throughout 2013. a whole of 962 cases were unfinished for trial from the previous year, inside that a most vary of cases were reported below cheating (306 cases) followed by forgery (29 cases) throughout 2014. In fifty 3 cases trials were completed, fifteen cases diode to conviction and twelve,098 cases remained unfinished for trial at the highest of the year 2013.[5]

VI. SOME MAJOR ATTACKS

Cyberwar: The first destructive cyberattacks to hit a state happened in spring 2007 in the Baltic nation of Estonia when a group of intrusions forced the termination of government websites and disorder leading businesses.

The assault distructed key corporate and government web services for days and knocked out the national emergency hotline for more than an hour. Estonia, which was in the heart of a diplomatic war against Russia, cursed Moscow for the attacks, which it refused.

Hacktivism: The unsnarled piracy collective Anonymous, he most dangerous hacking cluster, has targeted variety of organisations below its veil of fighting against injustices, as well as Pentagon, the Church of faith, the Islamic State cluster and Mastercard.

Anti-secrecy cluster WikiLeaks, based ten years agone by Australian full general Assange, specialises within theunleash of classified materials.

In 2016 it revealed files and communications from the political party, moving one in every of the presidential candidate mountain climber Clinton's campaign. United States of America intelligence officers disclosed the discharge was a part of a Russian plot to favour the ultimate election victor Donald Trump.

WannaCry Ransomware Attack: The WannaCry ransomware attack was a could 2017 worldwide cyberattack by the WannaCry ransomware cryptoworm, that targeted computers running the Microsoft Windows OS by encrypting knowledge and exigent ransom payments within the Bitcoin cryptocurrency. It propagated through EternalBlue, associate exploit in older Windows systems free by The Shadow Brokers many months before the attack. whereas Microsoft had free patches antecedently to shut the exploit, a– lot of of WannaCry's unfold was from organizations that had not applied these or were victimization older Windows systems that were past their end-of-life. WannaCry conjointly took advantage of putting in backdoors onto infected systems.

VII. MOST DANGEROUS HACKING GROUPS

Lizard Squad: Lizard Squad has taken the responsibility for the cyberwars on Malaysia Airlines which resulted in website visitors being directed to a page with a message "404 – aplane not found," also DDoS attack on Facebook which defamed the most popular social media network. Facebook denied it being hacked. Malaysia Airlines also posted that they had not been hacked and that their services had only been temporarily redirected elsewhere.

Anonymous: Anonymous may be a open on-line hacking cluster well-known most for its hacking and co-conspirator masks. Reports states that Anonymous consists of thousands of "hacktivists." The cluster has hacked government, spiritual and company websites. The cluster has already hacked the Pentagon, attacked Visa, MasterCard, and PayPal in 2012's Operation Payback for his or her ingonarance to method payments

to WikiLeaks, leading WikiLeaks to affix the cryptocurrency Bitcoin.

Lulzsec: Lulz Security formed as an autonomous spinoff after the HBGary Federal hack of 2011. The group declared a hack against Fox com, then Sony motionPictures . The group hacked the CIA website and turned it offline.

Syrian Electronic Army: Announcing to support the Syrian then President Bashar al-Assad, the countries Electronic Army claims to target political opposition's group. It calls itself "a group of energetic youths who could not stay silent towards the massive destruction of facts about the recent uprising in Syria".

Chaos Computer Club: This is a computer club whose mission was to expose security flaws& leaks to the world. It usually does not only depend upon illegal activities. It's the largest European hacking groups and was formed in Berlin during the early 1980s. The group made its position after stealing 133,000 Deutsch Marks from a Hamburg bank through the Bildschirmtext page to return the money the following day after completing its mission: to highlight a security leak.[6]

VIII. CONCLUSION

Every person does not face cybercrime directly still they are in great danger to be faced or accused off. Crime through the Internet has different categories rather they don't generally occur behind the computer. A recent study stated that the average age of a hacker ranger from 16 to 67 years. The increase in technology enables the criminals to stay at their home can rob any bank in the world without even moving a step outside. The have every tool the need, those tools are not guns or swords rather a program which could destruct the world.

IX. REFERENCE

[1] Ammar Yassir and Smitha Nayak:- Cybercrime: A threat to Network Security

[2]http://criminal-justice.iresearchnet.com/crime/cybercrime

[3] Social Impacts of Cyber Crime Research Paper Starter:- Enotes web portal.

[4] Hacked Web portal:- https://hacked.com/hacking