Cyber Times International Journal of Technology & Management

Vol. 10 Issue 2, April 2017 – September 2017

TABLE OF CONTENTS

EVOLUTION AND SHIFT IN TREND OF CYBER CRIME: AN OVERVIEW

Ratikant Sadananda Mohanta
Student, Tilak Maharashtra Vidhyapeeth
ratikantmohanta@gmail.com

ABSTRACT

Cybercrime in general is any criminal activity which involves computers and networks. As technology has progressed, cost of technology has decreased thus connecting more and more people together. Though it has reduced the gap of communication it has also led to increase in Cybercrime incidents. The change in technology has brought forth a new face of Cybercrime, not just sheer increase in number of incidents. Cybercrime sums up various crimes such as Cyber Stalking, Internet frauds, Spreading Malwares, Spamming, Cyber-warfare, Identity theft, Phishing, Child Pornography, etc. Cybercrime which started as hacking activities of a few university graduates in early seventies has come a long way. With existence of market place such as Silk Road, where one can purchase various banned drugs and illegal weapons, Stuxnet a multistage malware, etc. one can say for sure that Cybercrime has evolved to an extent beyond ones belief. The main objective of this paper is to show case how Cybercrime has evolved and bring forth it's ever changing nature.

KEYWORDS: *Cybercrime, Cyber -warfare, Internet Frauds, Malware.*

I. INTRODUCTION

Cybercrime has evolved a lot from pranksters and hobbyists playing pranks and exploring the technology in the early seventies to present day exploit researcher, fraudster, hacker, etc. Cyber-attack is very common phenomenon now. Not only has it grown in frequency, but also are destructive in nature.

So what is Cybercrime? Cybercrime according to Techopedia, "Cybercrime is defined as a crime in which a computer is the object of the crime or is used as a tool to commit an offence."[5]

This is by far the most simple and easy to understand definition on Cybercrime.

With the advent of new technologies Cybercrime reaches a new peak each and every year. For instance if we look at decade long Cybercrime reporting in India, we can see that it has increased many a folds.

Figure1: Statistics of reported crime Vs arrest made in the given decade in India.

As can be seen in graph plotted on the statistics of National Crime Records Bureau, it is evident that there is a sharp rise in Cybercrime in the given country. The number of reported incident has grown from 453 in 2006 to 11592 in the year of 2015.

Why is Indian statistics important? India stands 11th in the race of most number of

Cybercrimes committed with a share of 3% globally. India along with 19 other countries constitutes in together 81% of worlds Cybercrime. [1]

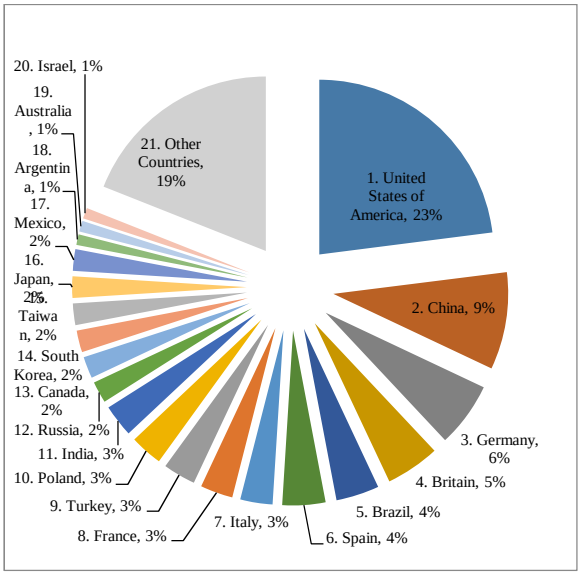

Figure 2: List of Top 20 Countries With Highest Rate of Cybercrime Sourced from BuisnessWeek/ Symantec.

The above chart shows the percentage share of countries to the Cybercrimes in the world. U.S.A leads the race with 23%, China seconds the race with 9% and Germany is at 3rd position with 6%.

So this leads to a very fundamental question, How Cyber Crime Evolved?

II. EVOLUTION OF CYBERCRIME

In the year of 1820, the first ever on records Cybercrime unfolded. Joseph Marie Jacquard a native of France crafted a loom. The device produced a set of repetitive steps to produce a specific fabric. Raising fear and suspicion among his employees for their livelihood. This led to sabotage of the device to discourage Jacquard in his quest. [7], [2]. This was a small incident in history, but major breakthroughs in Cybercrime started taking place in early seventies.

THE 70's

In the 70s PC's started becoming cheaper and direct communication of students of various universities via ARPAnet the predecessor of internet led to the beginning of new age of Cybercrime.

The emergence of "blue box" and rise in US wire frauds. John Draper discovers a giveaway whistle in Cap'n Crunch cereal boxes reproduce a 2600 Hz tone the frequency used by AT&T long lines to indicate that trunk line was available to route a call. John Draper uses this phenomenon to build blue box a device capable of reproducing other tones used by the phone company. This blue box technique was later used by many to commit wire frauds.

Creeper and Reaper, arrival of first worm and its nematode. Creeper the first worm spreads through the Arpanet and replicating itself in many computers. This worm was causing lot of havoc in the ARPAnet. Then another similar program came into picture named Reaper, the first nematode targeting creeper. Even though it was a worm it was designed to specifically attack creeper. Reaper although a nematode is also credited to be the first antivirus. A nematode is a computer virus or worm that attempts to remove another virus or worm.
So 70's not only saw the arrival of malwares and Cyber frauds but also the arrival of Reaper the first antivirus even though it was using controversial methodologies.

THE 80's

In the 80's more technology enthusiastic people came together forming groups. Young people started experimenting with the latest technology the eighties had to offer. Creating a base for the future hackers. Ian Murphy aka "Captain Zap" hacks into AT&T's Computer and changed the billing clock to turn night time rates into day time rates and vice versa. This incident caused revenue losses in several millions.

He also managed to become the first person ever to be convicted for a Cybercrime. Emergence of viruses and new kinds of malware. In 1982, Richard Skrenta writes Elk Cloner one of the oldest known viruses for Apple II. In 1986 Pakistani Brain, the oldest known virus is created under unauthorized circumstances, it infects many IBM Computers. Morris worm is launched on Arpanet over 6000 network computers are infected clogging government and university systems.

Eighties saw the first conviction in Cybercrime emergence of virus and also hacking groups such as Masters of Deception. Social Engineering started being used as a mode Cybercrime to bypass the punch card system which in today's time used to commit major Cybercrimes.

THE 90's

By 90's the perfect environment for Cybercrime had formed, many were online. People started conducting online banking and credit card transactions. With millions flowing through the system Cybercrime had a new motive. There was no legal framework and resources to prosecute Cybercrime. It was only possible because of the invention of the World Wide Web. In a single decade, the Web grew from non-existent to over 17 million web sites.

The year 1991 saw the emergence of the first cyber war, The Great Hacker War. A conflict between the Masters of Deception and Legion of Doom. Both groups were engaged in a form of Cyber Warfare trying to disrupt or take control of each other's network. This was highly published in media, but true nature of the warfare is still unknown.

Now hacking was a global phenomenon, Nashshon Even-Chaim aka Phoenix was convicted in Australia. His targets centred on defence and nuclear research networks.

Motives of hacking changed from mere pranks and small frauds to politics, money, curiosity and information.

THE 21'st CENTURY

The dawn of 21'st century an age of information, computer now is a global phenomenon. Almost every nooks and corner of the world is connected with internet via PC’s or Cell phone. Technology keeps on changing at an exponential rate. A perfect condition for already thriving Cybercrime.

Silk Road was the first modern darknet market, an online black market to sell illegal drugs under Tor hidden service in such a way that users were browsing anonymously. It was taken down by FBI on October 2013. Later a mirror site emerged as Silk Road 2.0 which was shut down by FBI and Europol on 6th November 2014. Silk Road 3.0 is online and is yet to be downed until March 2017. With existence of market place such as Silk Road, where one can purchase various banned drugs and illegal weapons, one can say for sure that Cybercrime has evolved to an extent beyond ones belief. With the introduction of BitCoins(BTC) a cryptocurrency , it becomes even more difficult to track these transaction. Giving criminal elements operating such websites like Silk Road an edge and anonymous safe havens for their illegal trade.[6]

Stuxnet a well-designed sophisticated multistage malware is found in the wild. It was specifically targeted towards Iran's nuclear program. It had three modules, a worm that executes all the routines related to payload, link file which propagates the worm and a root kit which hides the Stuxnet. Typically introduced through USB. This gives us an example how far malwares have evolved. [3] Ghostnet a term coined by Information Warfare Monitor for a large scale cyber spying, originating mainly from People's Republic of China.

It has managed to infiltrate high valued targets such as computer systems belonging to embassies, foreign ministries, etc in 103 countries. The extent of this spy network is commendable. [4]

Hactivism a new form of hacking emerged done to disrupt services and bring forth attention to a political or social cause. Anonymous a group came in forefront orchestrating various hacks for Social and Political reasons. WikiLeaks an international organization that leaks classified information gathered from various anonymous sources changed the face Hactivism and Cyber Journalism.

Cyber terrorism defined as "unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives" (Michael Knetzger, 2008). The internet which started as a tool to connect people together now became a training and recruiting ground for terrorist. A place to propagate their false beliefs and radicalize people for their own gains. The 21'st century saw many changes in Cybercrime, be it Silk Road, Hacktivism, Cyber terrorism, Extortion etc. The face of cyber-crime kept on changing. The Cybercriminal who was once a programmer is now just an ordinary end user of the technology.

THE CYBERCRIMES OF FUTURE

In the coming future, Cybercrimes will see further more rises, as technology advances. The nature of Cybercrime may not be same as today but they will evolve from same tool and techniques used by Cyber Criminals of today. As time passes tailor made techniques will come up and keep on evolving assisting Cybercrimes of the future.

III. CONCLUSION

Cybercrime has a changing nature i.e. it evolves very rapidly with time. With the spread of technology Cybercrime which was once a domain of technical people has reached to the non-technical users of the technology. Evolving nature of cybercrime is a reason because of which, even after so many years of struggle experts are yet to curtail it and cybercrime keeps on increasing.

REFERENCES

[1] Dr. P. N. Vijaya Kumar , 2016, "*Growing Cyber Crimes in India: A Survey*", Data Mining and Advanced Computing (SAPIENCE), International Conference, Available at: <http://ieeexplore.ieee.org/document/7684146/>, [Accessed 30 March 2017].

[2] Infosec Institute, "*Evolution in the world of cybercrime"*, Available at: <http://resources. infosecinstitute.com/evolution-in-the-world-of-cyber-crime/#gref>[Accessed 16 March 2017]

[3] Kushner, David, "*The Real Story of Stuxnet*". ieee.org. IEEE Spectrum , Available at: <http://spectrum.ieee. org/telecom/security/the-real-story-of-stuxnet>[Accessed 30 March 2017].

[4] Scribid, "*Tracking Ghostnet*", Available at: <https://www.scribd.com/ doc/ 13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network>, [Accessed 19 March 2017].

[5] Technopedia, "*C*ybercrime", Available at: <https://www.techopedia.com/definition/2387/cybercrime>, [Accessed 19 March 2017].

[6] The New York Times, "*Man Behind Silk Road Website Is Convicted on All Counts"*, Available at: <https://www.nytimes.com/ 2015/02/05/ nyregion/man-behind-silk-road-website-is-convi-cted-on-all-counts.html?hp&action=click& pgt-ype=Homepage&module=first-column-region & region=top-news&WT.nav=top-news&_r=1>, [Accessed 18 March 2017].

[7] Vinit Kumar Gunjan, 2014 ,"*Present & Future Paradigms of Cyber Crime & Security Majors - Growth & Rising Trends*", Artificial Intelligence with Applications in Engineering and Technology (ICAIET), 2014 4th International Conference, Available at: <http://ieeexplore. ieee.org/document/7351818/>, [Accessed 30 March 2017].