ISSN: 2456-1134 www.isjcresm.com
Vol-02 Issue-01 Aug 2017

Cybercrime A Comprehensive Overview

Ajaay ,shirisha,Lakshmi

Maharaja Surajmal Institute, New Delhi, India

Abstract: Any illegal activity using a computer or network is considered a cyber crime. It is possible that the computer was either employed as a tool or the primary object of the criminal act in some instances. Viruses infect computers when users open infected files and unknowingly copy themselves to other machines' hard drives. A cyber crime is the creation and use of a computer virus. The virus has the potential to spoil data on the computer, steal disk memory, access personal information, or even send information to the personal contacts of the computer user.Emails with virus attachments are the most common vectors for computer infections. Take the case of receiving an email including an attachment as an example. Your PC becomes infected the second you open the attachment. It is not always necessary to send a virus via email for it to propagate; in certain instances, all it takes is for a computer on a system personal network, like your workplace, to open the infection. A person might create a virus and distribute it to other computers for many different reasons. It might be an attempt to steal data or funds, cause harm to that system, or take advantage of its vulnerabilities. The ability to eliminate these infections from the user's computer system varies from case to case. As a result, we can easily see how these infections result in yearly financial losses. Anyone found guilty of damaging or gaining unauthorized access to a secure computer system may face imprisonment and/or financial penalties.

***Key Words*:** Cyber Crime, Cyber Space, Cyber Security, Hacking

1. INTRODUCTION

The word Cyber crime is increasing day by day. Since the computer is developed and connected to the internet the various types of cyber crime are there in the computer world. The crime in which there is a involvement of any computer is known as cyber crime.Consumers are subject to personal identity theft, fraud and inferior simulated or pirated goods.

- Businesses risk losing cognitive property corporate secretsvalue broughtbynewinnovations, reputation and revenue through espionage and breaches.
- For a nation broader individual losses impact GDP reduce economic growth and innovation and result in a smaller tax base.
- For government's surveillance and cyber attacks threaten national security and diplomatic relations.
- Critical infrastructure that provides water, power, food supply, and healthcare are becoming more attractive career targets for attacks.

A. Cyber crime research

Cyber crime Research is one context where the solution to deal with cyber criminals is generate with the help of cyber law. Investment of time and resources requires advance strategies for research and grow transformative solution to meet critical cyber crimes involving a certain technology.

- The focus of cyber crime research is nowadays to deal with new appear threats and detecting the threats before they effect or cause good amount of damages.
- With attend number of phishing, APTs and Bitnet attacks there is lot to be worked in terms of technological advance and tracking.

ISSN: 2456-1134 www.isjcresm.com
Vol-02 Issue-01 Aug 2017

B. Secured protocol and algorithms

Research in protocols and algorithms is an important aspect for strengthening the cyber security aspect at a technical level. Protocols and algorithms define the rules for information sharing and processing over online community. In India research has also been undertaken at protocol & algorithm level such as Secure Routing Protocols,

Fig 1. Top 20 countries with cyber crime

C. Research in industry

- Next generation detection technology:

Extend perimeter crime in networks use to detect and await the attacks as early as Possible, but the sheer volume of information in the age of Big Data often makes it tough to detect anomalies that might indicate security issues. Technological research challenges consist of binary solidification, network monitoring, IDS and IPS systems, and attack analysis. Instance to detect and prevent attacks we need techniques and tools to little bit and remove duty from software and monitoring systems to boost and alarm when a system behaves in an odd manner. In order to effectively descry such advanced malware blind of the attack methods being used technology solutions are being developed which use a combination of sophisticated techniques to evaluate advance threats including checking real time emerging campaigns and known new malicious websites that are being detected across organizations and static code division looking for suspicious behavior, obfuscated scripts, malicious code snippets, and modify to other malicious sites. To add solutions based on dynamic analysis by sandboxing the target URL or attachments to simulate a real user on a machine with a goal of observing any changes made to the system are being nudged.

- Command and Control Protection:-

The campaign connected to the Internet can become a target of boot driven attack. Unlike Common attacks targeted Bitnet attacks are very stealthy in nature and are difficult to detect using traditional security solutions. However, despite their close nature, they can cause very high, sometimes irreparable damage to an organization. Research and product development sign at unique “fingerprint” detection of secret C&C traffic which can identify attackers use of accepted applications and Deep discovery custom sandbox analysis can also discover new C&C destinations of intelligent network and all customer crime protection points.

- **Malware and Malicious Infrastructure:-**

Threat of malware will remain critical for the computable future. There is already a pointed trend of increasing malwareon social networks in cloud computing and on mobile devices. In terms of research it poses an associative challenge. We need advances in technology for detail in reverse engineering, Bitnet tracking, analysis of criminal framework and classification and accumulate of malware. We need reliable methods to estimate the number of spoil machines and the effectiveness of corrective. Latest promote development of the online Bitnet Extraction and Response System a Bitnet detection and reduction tool which also integrates the online Bitnet extraction capability. Analysis engine and the signature distributor is the technology direction being supported.

D. Recommendations

Despite our efforts cyber crime will continue. However, innovative approaches to this complex problem will enable us to predict appear threats better protect our economies and citizens and minimize the damage from cyber attacks. These advices provide guidance for designing and maintaining enterprise resilience and convert security strategies.

:Prefer cyber crime to a strategic role as it impacts the enterprise’s most valued assets.

- Consider cyber crime as a risk stave investment decision not simply a technology purchase.
- Achieve a greater level of protection by sharing data with trusted partners in industry and government, across borders.
- Allow real-time data be the driver for building
- Design operational workflows and agenda to support these decisions. Design flexible strong.
- Networks that quickly conform to new threats. Create a culture of widespread control for cyber security
- Balance privacy and protection when drafting crime scheme.

ISSN: 2456-1134 www.isjcresm.com
Vol-02 Issue-01 Aug 2017

- Real time- Threat detection and data analysis tools many tools exist today. But their level of sophisticated and widespread adoption must continue to grow to provide more comprehensive protection.
- Big Data- To effectively compile and amount large volumes of data, new technologies and algorithms will be required.
- Visualization tools – Related to big data opportunities are visualization techniques: creative visual presentations of data that quickly differentiate warning indication from normal operating behaviors.Emerging technologies- That contribute to resilience more robust protection and adscription of cyber crimes.

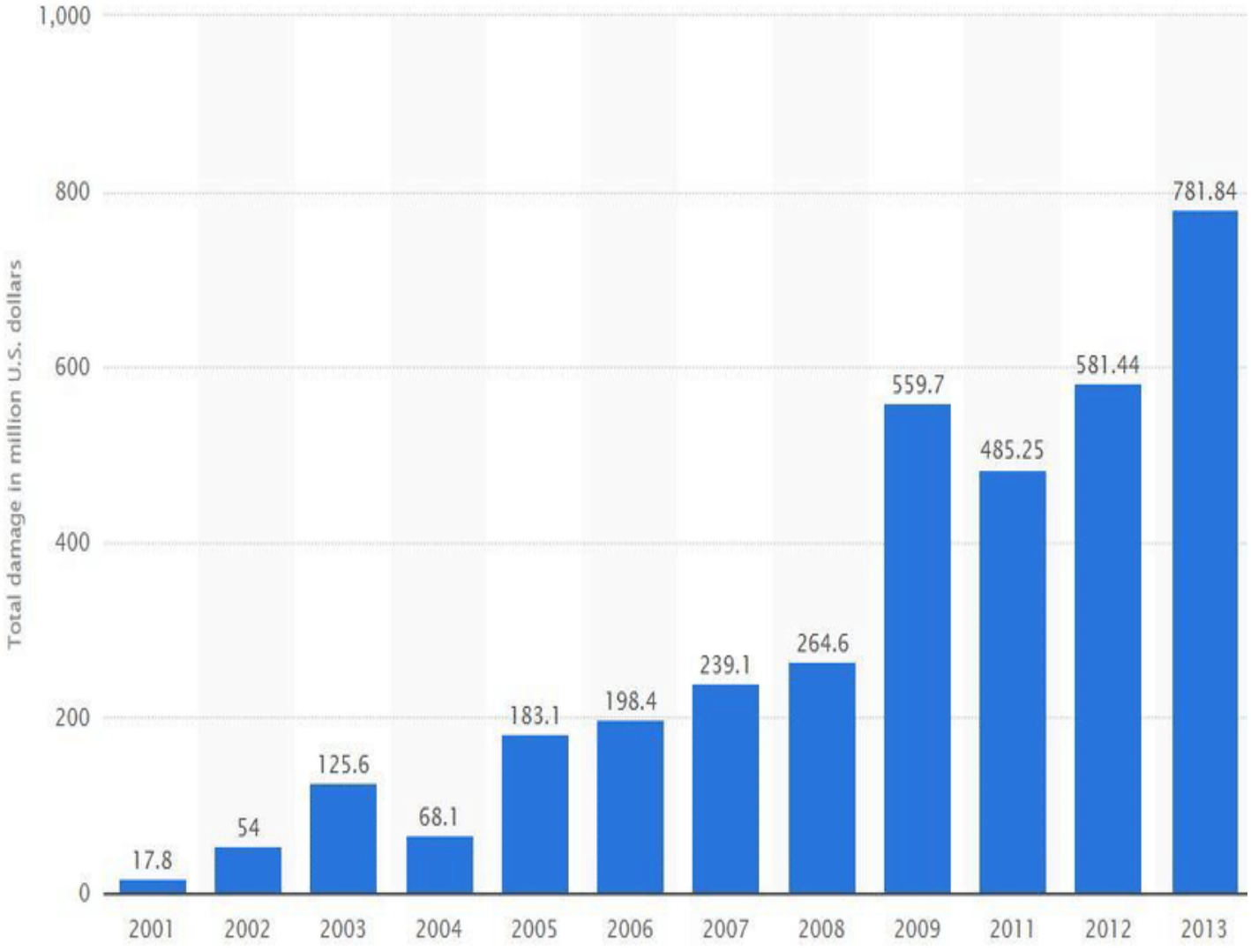

Fig 2. Amount of monetary damage caused by cyber crime from year 2001 to 2013(in million US dollar)

ISSN: 2456-1134 www.isjcresm.com
Vol-02 Issue-01 Aug 2017

E. Privacy and government role

Several broader policy issues that govern our collective approach to cyber security have large conclusion for the future:

- The right to privacy by the individual and the activity.
- The act government should play in cyber security.
- Reporting claim for security breaches.

F. The challenge

No matter what strategy is embrace breaches will occur. It is nearly impossible to take advantage of our association without being artist. Technologies such as firewalls, passwords, encryption, physical barriers and authentication. Their value as stand-alone security measures will be of limited use in fighting increasingly artificial, innovative, and well-funded cyber criminals. The emerging challenge is to find more augur

methods of identifying threats, relieve their impact and managing an active cyber security operation that will both cooperatively and effectively maintain protection. In accept that challenge. It is important to know that:-

It is not productive to protect every piece of data and every

CONCLUSIONS

Cyber crime is one of the biggest problem facing by the society in technological world which makes people fearful to perform financial transactions over internet. Recently .

Lack of consistency in laws and claim between nations and severity of penalties.

These are complex and sometimes doubtable policy issues but purpose established by new policies may have far reaching impact on the level of protection and the approaches we can take to protecting individuals, campaign and state from cyber crime of the future.

asset to the same matter.

- A balance between the rights to separation with the need to protect nations.
- Enterprises and individuals from interference must be negotiated.
- Acknowledgment and severe amends for cyber crime must be more uniformly realized within the multi- national communities.
- The challenge is great and desire fresh ways to blend people, processes, technology and shared data to protect societies from appear threats to security.

creation of cybercops, cybercourts and cyberjudges may eventually required to overcome the significant jurisdictional issues

REFERENCES

[1].
The forensic difficulties of electronic crime, by B. Etter, Australasian Centre for Policing Research, Adelaide, 2001, Current Commentary No. 3.
[2] Etter B. (2002), given at the Netsafe: Society, Safety and the Internet Conference in Auckland, New Zealand, discussed the difficulties of policing cyberspace. Cyber Crimes: A Practical Approach to the Application of Federal Computer Laws, edited by William P. Reilly and Eric J. Sinrod, published in 2000 by Santa Clara University Press, Volume 16, Number 2.
[4] Gengler, B. (2001), The Australian, 11 September p.36, virus cost $20 billion.
section 5 of the Information Technology Act of 2000.
www.indianchild.com, "Cyberstalking India," [6]. [7]. Criminal Bureau of Investigation faces fresh cybercrime threat, www.rediff.com, March 12, 2003 12:27 IST.

Viruses, Worms, and Other Destructive Forces, by Richard Raysman and Peter Brown (1999), page 8. Judge N. Y. L.
In 2000, Kabay published a work with the same title. Studies and Surveys of Computer Crime, Focus.
[10]. New Strategies for Managing the Risks of Exploitation in E-Commerce and Cyber Crime, USA: KPMG (2000).
[11] An article titled "Hackers Hit Government Sites" was published in Computer World on January 29, 2001. Cyber Criminals on Trial, by Russell G. Smith, Peter Grabosky, and Grgor Urbas, published by Cambridge University Press, ISBN 0521840473 [12].
The article "An Extended Model of Cybercrime Investigations" by Seamus O. Clardhuanin appeared in the summer 2004 issue of the International Journal of Digital Evidence, volume 3, issue 1.
cited as [14]. Global Terrorism and Criminal Acts, cybercrime-en.asp.
http://www.dfaitmaeci.gc.ca/internationalcrime/cybercrime-en.asp.

ISSN: 2456-1134 www.isjcresm.com
Vol-02 Issue-01 Aug 2017

The Times of India reports that there is a cybercrime in India every ten minutes. July 22, 2017, in The Times of India.
[16]"Only 34 convictions in Maharashtra between 2012 and 2017 out of 10,000 cybercrime cases," writes J. S. Naidu. on August 21, 2017, at http://www.hindustantimes.com.
[17]V. Nanjappa, "The Reasons Behind the 0.5% Conviction Rate in Cyber Crime,"
"Why not? India and the Budapest Convention?" (A. Seger, 18) Oh my.
7. Convolutional Budapest En.pdf [19]
Article 32 of the T-CY Guidance Notes addresses cross-border data access. "Inda and the Budapest Convention" by D. A. Kovacs [21].
"T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime," [22] European Council, Strasbourg, .