International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2017): 7.296

Distinct Ways to Scrutinize Cyber Security as Amalgamated Approach

Vipan Kumari[1], Sandeep Kulkarni[2]

[1]F-84, UGF Near Sai Chowk, Chhatarpur, New Delhi-110074
Himalayan University Arunachal Pradesh, Itanagar, India

[2]C/O G S Laxman, #4094/20, 1st A main, B block, 2nd stage, Rajajinagar, Banglore-560021
Himalayan University Arunachal Pradesh, Itanagar., India

Abstract: ***As technological evolution progresses of cybercrimes, continually develops new attack types, tools and techniques that allow attackers to penetrate more complex or well controlled environments, and produce increased damage and even remain untraceable. IT security experts engages in behaviour-based malware analysis in order to learn about previously unknown samples of malicious software (malware) or malware families. For this, they need to find and categorize suspicious patterns from large collections of execution traces. The factors affecting the cybercrime have different laws of treatment in different countries that often overlook aspects of the problem and investigation in the depth of the issues with different methods, are playing key role . Not only the method of fighting against the cybercrime but also the juridical issues and technical challenges involved in fighting cybercrime may not be understood. Ethical aspects are often set aside as shown by the various battles government have taken recently to address the cybercrime issues.***

Keywords: Cyber Crime, Cyber Attacks, Cyber Security, Information Technology.

1. Introduction

Cybercrime which gives an impression of an illegal activity and when it is merged with Computer creates wider and pan global issues. It is a term used mostly to describe criminal activity in which computers or computer networks are a tool, a target or a place of criminal activity. Malware (malicious software) is undoubtedly one of today's greatest threats to the Confidentiality triangle of information security. It has become a common tool in digital theft, corporate and national spam distribution and attacks on infrastructure availability. When security professionals analyse malware in a real world setting, they have large volumes of complex and heterogeneous data at their disposal. Images are preferred medium for the current steganography techniques. Content adaptability, visual resilience, and smaller size of images make them good carrier to transmit secret messages over the internet. There exists a large number of image steganography techniques which are accompanied by various attacks on the steganography systems.

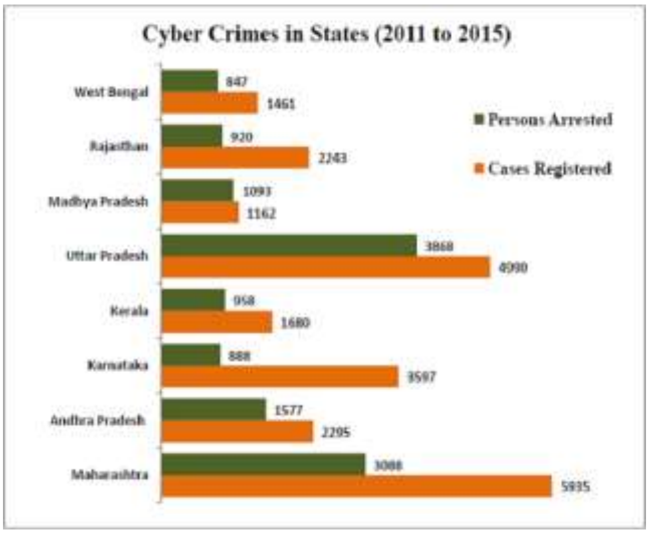
781
data breaches reported in 2015
48% of data security breaches are committed with malicious intent
211 days–
how long hackers remain undetected in corporate systems
6%–
how often Fortune 500 companies detect their own data breaches
10 FAST FACTS ON CYBERSECURITY
1 million
available cybersecurity jobs in 2016
$2.1 trillion–
the projected global cost of cyber attacks in 2019
51% of U.S. adults suffered a security incident between December 2015 and 2016
52% of data security breaches are caused by human error or system failure
1,093
data breaches reported in 2016
$6.5 million–
average cost of a U.S. data breach
THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

1.1 Crimes Related to Telecommunication

When an organization is mostly depends on Digital Information System and using that for the activities which are illegal in aspects of law come under the Telecommunication Cyber Crime. Cyber Criminals are using different front end services to hide their actual profession. The other most common example of telecommunication theft is access of PBX to obtain the services of dial in/dial out through individual or by the group of peoples. People use others telecommunication services illegally and without the knowledge of the owner. The third category of telecommunication crime is piracy of digital content. When we publish any ones personal objectionable data withoutbringing that in their knowledge comes in this category of telecommunication theft. Apart from this, financial thefts by individual or by the group of peoples like for Tax Evasion, Money Laundering, Extortion, terrorism, investment frauds, malicious fund transfers etc. are the example of these category of Cyber Crimes.

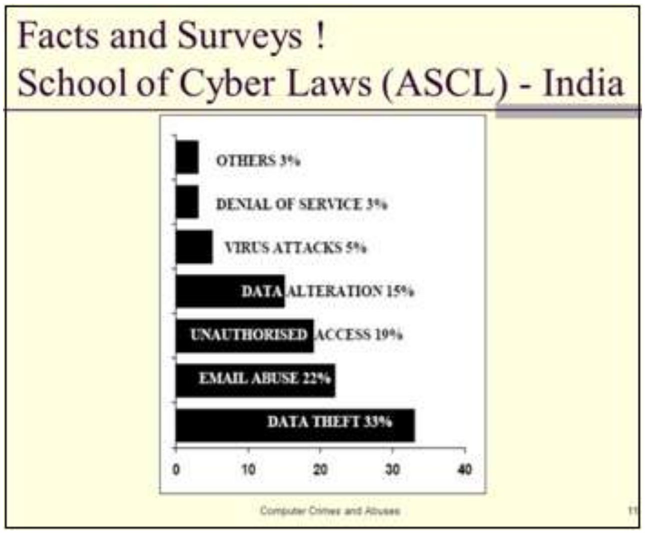
1.2 Cyber Crime against Women

Enabling the free flow of information and ideas over long distances also give rise to a worryingly high incidence of irresponsible behaviour. The vulnerability and safety of women is one of the biggest concerns of any criminal and penal law, but unfortunately women are still defenseless in cyber space. Cybercrime against women is on at alarming stage and it may pose as a major threat to the security of a person as a whole. The World Wide Web allows users to circulate content in the form of text, images, videos and sounds. The widespread circulation of such content is particularly harmful for women. In recent years, there have been numerous reports of women receiving unsolicited emails which often contains obscene and obnoxious language. India is considered as one of the very few countries to enact IT Act 2000 to combat cyber-crimes; This Act widely covers the commercial and economic crimes. Even though issues regarding women still remain untouched in this Act. Social Networking and other websites are created and updated for many useful purposes, but they are nowadays also be used to circulate offensive contents also. Individuals who post personal information about themselves on job and marriage websites or social networking websites are often at the receiving end of ‘cybercrime’. Women and minors who post their contact details become especially vulnerable. As many as 80,000 cyber-crime related complaints have been registered with police in Kerala in 2012, of which 50,000 relate to harassment of women through new hi-tech devices.



1.3 Harassment Via Email

Harassment on the Internet can take place in a number of ways. One form may include Harassment through e-mails includes blackmailing, threatening, bullying, constant sending of love letters in anonymous names or regular sending of embarrassing mails to one’s mail box. Indian Penal Code, Criminal Procedure Code and select sections of IT Act deal with the protection from cyber-crime. In general they are used to book the perpetrators along with Section 292A of the IPC for printing or publishing grossly indecent or scurrilous matter or matter intended to blackmail, and under Section 509 of the IPC for uttering any word or making any gesture intended to insult the modesty of a woman.

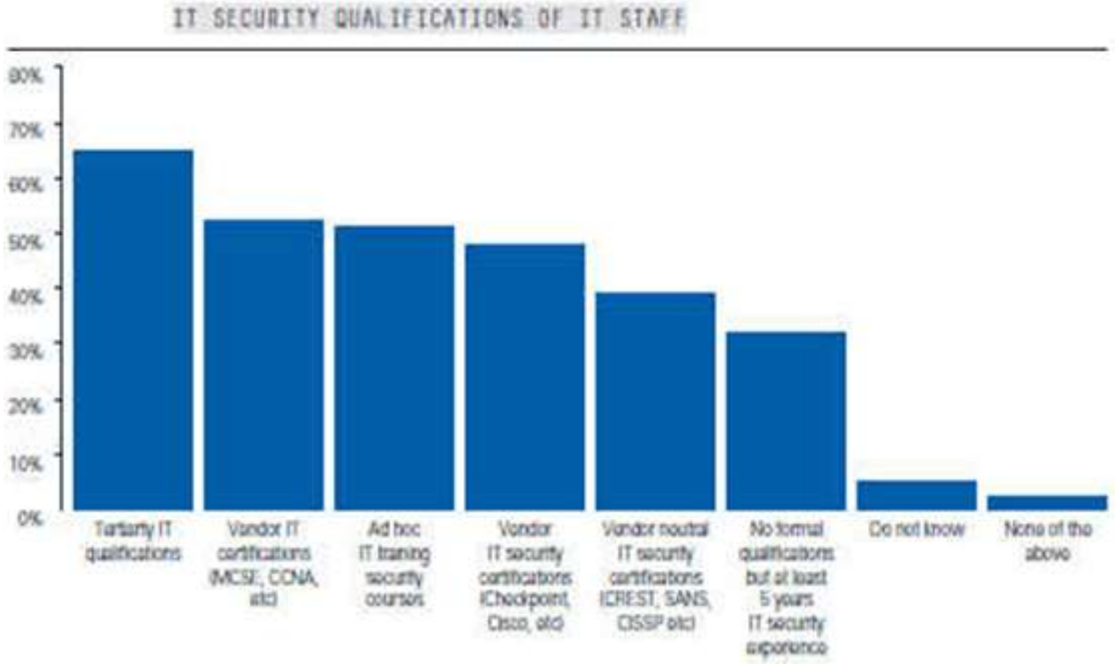

Facts and Surveys !
School of Cyber Laws (ASCL) - India

2. KAMAS

A knowledge-assisted visualization system for behaviour-based malware analysis. Malware analysis lends itself very well to visualization, because the experience of analysts plays a central role in reconstructing the obfuscated behaviour of malware. There are basically two different approaches for the detection of malicious software: the signature-based and the behaviour-based approach, since the signature-based approach can be used only for known malware, other techniques must be applied. Behavioural analysis is a promising approach for detecting and pre-classifying malware. (Behavioural analysis)Both approaches (static and dynamic analysis) yield patterns and rules, which are later used for malicious software detection and classification.

2.1 Survey based on business and what security measures they have taken

Responses indicated that 65% of participating organisations had IT security staff with tertiary level IT qualifications. More than 50% of participating organisations had IT security staff with some type of vendor based IT certifications. Almost 35% of participating organisations had IT security staff with no formal training, although most of these staff had more than five years working in the IT security industry.



2.3 Terminal safety controls

1) Proactive defence-in-depth
2) Penetration testing, ethical hacking and simulations.
3) Regulartraining exercises on social engg techniques
4) Vulnerability assessment
5) Internal and external audits
6) Data encryption
7) Counter attacks
8) Air-gapping or partial air-gapping

3. Detection and Mitigation

The ultimate objective of targeted attacks is the acquisition of sensitive data so defensive strategies need to include the identification and classification of sensitive data and appropriate access controls can be placed on such data. Developing threat intelligence based upon indicators that can be used to identify the tools, tactics and procedures of attack will help in defending against targeted attacks.The information like domain names and IP addresses used by attackers to send spear phishing emails or to host their command and control servers must be properly recorded and updated from time to time.

Detection and monitoring of suspicious behaviors that indicate targeted attacks will help in mitigation of such attacks should be based upon the following:-

Logs from endpoints, servers and network monitoring should be carefully studied and can be aggregated to provide a view of activity within an organization that can be processed for anomalous behaviors that could indicate a targeted malware attack. In order to maintain persistence, malware will make modifications to the file system and registry. Monitoring such changes can indicate the presence of malware. Security analysts with access to real-time views of the security posture of their organization should be in place to detect, analyze and remediate targeted attacks. Education and training programs combined with explicit policies and procedures that provide avenues for reporting and a clear understanding of roles and responsibilities is an essential component of defence. Sensitive information is not only stored in databases but also in the cloud and is accessible through a variety of methods including mobile devices. While securing the network layer is an important component, it is also critically important to specifically protect data as well. Identifying and classifying sensitive data allows the introduction of access controls and enhanced monitoring and logging technologies that can alert defenders of attempts to access or transport sensitive data

3.2 The Gompertz Model

The modified Gompertz model used by Pitcher assumes that the probable causes forthe outbreak of such incidents are imitative as well as inhibitive in nature. This model's Theoretical background is strong and is based on a social conflict theory. The imitative aspect is based on incident news spread via the Internet and by word-of-mouth; the inhibitive aspects can also be spread via Internet/Web sites and related stories. However, people only engage in, Security attacks when they feel threatened or are motivated by some economic or other gain and observed the success of earlier attackers. Traditionally, the challenge or threat to such attackers was mostly an intellectual one: to break a system. To quote a hacker expert, Of course, other types of challenges come, for instance, from making money or taking economic or political advantage. The more successful the earlier attackers are, the more aggressive the behaviour of the present attacker becomes. Each such incident is an imitation of previous behaviour and a behavioural model for others to imitate. On the other hand, the increase of security activities and success stories about preventing such attacks could reduce the number of attacks. Thus, a combination of imitation and inhibition as assumed by the asymmetric model could provide a realistic background in modelling such incidents. The model can be expressed as, The parameter **c** denotes the net rate of instigation to attacks
q denotes the rate of inhibition in such attacks.

$$\frac{dN(t)}{dt} = c \cdot e^{-qt} \cdot N(t)$$

where t = time,

N (t) = cumulative number of attack incidents at time t

c, q are parameters of the models.

4. Conclusion

As the Cyber Crime is growing in wide scale and becoming a global issue. Regardless of regional and national boundaries researchers are working together to find out all possible solutions. Various legislative acts are enforced and implement. Organizations are instructed to abide and follow the safety measures. To fight with Cyber Crime, Cross-Domain Solutions are becoming popular to resolve issues. Fraud prevention approaches now require solutions which can extend to mobile and cloud environments, make greater use of behavioural analytics, and take advantage of integrated threat intelligence capabilities to protect users and data. Even if attacks can’t be stopped completely, it is possible to change how we detect and respond to an attack to minimize the potential for loss or damage. Several key factors to help increase the security awareness among users were also presented. The defensive strategies can be greatly improved by understanding how targeted attacks work and their trends and the tools, tactics and procedures that they use. The defensive strategies can be greatly improved by understanding how targeted attacks work and their trends and the tools, tactics and procedures that they use. As these attacks focus on the acquisition of sensitive data, so defense should focus on protecting the data itself, wherever it resides. By effectively using threat intelligence derived from external and internal sources combined with context aware data protection and security tools that empower and inform human analysts, organizations are better are better positioned to detect and mitigate targeted attacks.

References

[1] Akhgar, S., Yates, B., 2013. Strategic Intelligence Management, 1st Edition, Butterworth-Heinemann

[2] H. Choi, H. Lee, H. Lee, and H. Kim (2007) "Botnet Detection by Monitoring Group Activities in DNS Traffic," in Proc. 7th IEEE International Conference on Computer and Information Technology.

[3] Kshetri, Nir "Pattern of global cyber war and crime: A conceptual framework, " Journal of International Management, Elsevier.

[4] Kshetri, Nir (2005) "Information and communications technologies, strategic asymmetry and national security, " Journal of International Management.

[5] Michael Massourakis & Farahmand Rezvani & Tadashi Yamada "Occupation, Race, Unemployment and Crime In a Dynamic System, " NBER

[6] Panu Poutvaara & Mikael Priks "Violent Groups and Police Tactics: Should Tear Gas Make Crime Preventers Cry”

[7] Cyber Crime – A Threat to Persons, Property, Government and Societies by Er. Harpreet Singh Dalla, Ms. Geeta ,2013

[8] Cyber Crime and Corporate Liability.Author(s) : RohasNagpal

[9] Cyber Crime and Cyber Security: A White Paper for Franchisors, Licensors, and Others by Bruce S. Schaeffer, Henfree Chan,Henry Chan and Susan Ogulnick

[10] Cyber Crime and Research paper 2013

[11] Cyber Crime and Security Survey Report 2012

[12] Cyber Crime Criminal Threats fromCyberspace:Susan W Brenner

[13] " ETHICAL ISSUES IN CYBERAGE ", Rajeev Kumara, R.K. Mittal, Delhi Business Review Vol. 3, No. 1, January - June 2002

[14] Software Vulnerabilities, Banking Threats, Botnets and Malware Self-Protection Technologies by Wajeb Gharibi1, Abdulrahman Mirza, 2011

[15] Halder, D & Jaishankar, K “Cyber Crimes against Women in India: Problems, Perspectives and Solutions” TMC Academic Journal Volume 3, Issue 1.